FAUSTINI FRANK NICOLINI

FAUSTINI FRANK NICOLINI

Via Giulio Alberoni, 49, 29121, Piacenza
Tel. e Fax: 0523.321659 – e-mail: pcmm00300g@istruzione.it – PEC: pcmm00300g@pec.istruzione.it
Codice Fiscale/Partita IVA: 80010270330

Agli atti
Piattaforma MePA
Spett.le Ditta TECNOLOGICA s.r.l. Unipersonale

PNRR – Missione 4: Istruzione e ricerca – Componente 1 – Investimento 3.2: Scuola 4.0 – Azione 1 – Next generation classroom – Ambienti di apprendimento innovativi, Codice: M4C1I3.2-2022-961-P-12250

OGGETTO: Affidamento diretto ai sensi del disposto combinato dell'art. 50 comma 1, lettera b), del D.Lgs n. 36/2023 e delle disposizioni di cui al decreto-legge. N. 77 del 2021, convertito con modificazioni dalla legge n. 108 del 2021, al decreto-legge 24 febbraio 2023 n. 13, mediante Trattativa Diretta sul Mercato elettronico della Pubblica Amministrazione (MePA) per un importo contrattuale di €. 126.547,13,00(oltre IVA) pari a €. 154.387,49 (IVATO).

Codice avviso: M4C1I3.2-2022-961
Codice progetto: M4C1I3.2-2022-961-P-12250
CUP: J34D22005050006

PRESTAZIONI: Prodotti e servizi per dotazioni digitali (attrezzature, contenuti digitali, app e software, arredi, interventi edilizi, ecc).

CAPITOLATO TECNICO

Il presente progetto descrive gli aspetti tecnici relativi alla fornitura di prodotti e servizi per la realizzazione di ambienti didattici innovativi nell'ambito del potenziamento dell'offerta dei servizi di istruzione: dagli asili nido alle Università Investimento 3.2: Scuola 4.1 Azione 1 - Next generation classroom.

Il sottoscritto ing. Giovanni Fiorillo, in qualità di Progettista del progetto in epigrafe, con la presente, sottopone all'attenzione di codesto spett.le Istituto, relazione Tecnica, capitolato e layout grafici degli ambienti oggetto di intervento , relativamente al progetto indicato in oggetto. Si precisa che sono state esperite tutte le operazioni necessarie in risposta alle richieste pervenute, con effettuazione di sopralluoghi e rilievo dati degli apparati ed infrastruttura esistente, di tutti i plessi dell'Istituto interessati dalla realizzazione del progetto in conformità del **target minimo richiesto pari a 23**.

Pertanto, quanto di seguito descritto, è stato redatto, in conformità alle richieste dell'Istituto e sulla base delle esigenze emerse e delle verifiche effettuate durante il sopralluogo tecnico ed in considerazione della proposta progettuale inoltrata.

La presente relazione è articolata nelle seguenti sezioni e sottosezioni:

1 – PREMESSA

L'Istituto ha aderito al progetto PNRR – Missione 4: Istruzione e ricerca – Componente 1 – Investimento 3.2: Scuola 4.0 – Azione 1 – Next generation classroom – Ambienti di apprendimento innovativi che ha l'obiettivo di trasformare almeno 100.000 aule delle scuole primarie, secondarie di primo grado e secondarie di secondo grado, in ambienti innovativi di apprendimento. Ciascuna istituzione scolastica ha la possibilità di trasformare la metà delle attuali classi/aule grazie ai finanziamenti del PNRR. L'istituzione scolastica potrà curare la trasformazione di tali aule sulla base del proprio curricolo, secondo una comune matrice metodologica che segue principi e orientamenti omogenei a livello nazionale, in coerenza con gli obiettivi e i modelli promossi dalle istituzioni e dalla ricerca europea e internazionale.

2 - DESCRIZIONE DEL PROGETTO

Il progetto prevede il potenziamento degli ambienti di apprendimento relativi al target previsto potenziando l'infrastruttura tecnologica delle classi e degli spazi condivisi, utilizzando un modello ibrido. Il progetto favorirà un apprendimento cooperativo con metodologie di insegnamento/apprendimento di tipo action research. I nuovi ambienti pertanto consentiranno una migliore integrazione della comunicazione orizzontale e verticale, anche di tipo virtuale, favorendo l'interazione non solo con il territorio circostante, ma anche oltre i normali confini territoriali. Il Progetto prevede in particolare l'implementazione di almeno un grande ambiente che sia di stimolo per le competenze computazionali e linguistiche. A tale scopo il design degli ambienti sarà caratterizzato da attrezzature versatili (schermo di proiezione, dispositivi digitali mobili e/o integrati (ad es. OPS) per lo studio delle STEM, sistemi per la videoconferenza.

3 - ANALISI PRELIMINARE E RICOGNIZIONE DEGLI SPAZI E DELLE DOTAZIONI ESISTENTI

Dalla ricognizione effettuata si evince la necessità del completamento della digitalizzazione delle classi e degli ambienti comuni con monitor interattivi, attrezzature/arredi che consentano di realizzare gli obiettivi previsti. In alcune aule sono presenti LIM obsolete che andranno pertanto sostituite con più moderni monitor touch.

4 - CAPITOLATO E SPECIFICHE TECNICHE

Il presente Capitolato Speciale definisce e disciplina la fornitura e le specifiche tecniche, funzionali e prestazionali per la realizzazione del progetto la cui corrispondente rimodulazione presenta la

seguente stima relativa al **piano finanziario**:

PIANO FINANZIARIO PROGETTO	Importo oltre iva in euro	Importo ivato in euro
Spese per acquisto di dotazioni digitali per i laboratori (attrezzature, contenuti digitali, app e software, etc.)	113.548,50	138.529,17
spese per acquisto di arredi innovativi	8.726,11	10.645,85
spese per piccoli interventi di carattere edilizio strettamente funzionali all'intervento	4.272,52	5.212,47

Di seguito per ogni plesso e per ogni aula sono rappresentate le caratteristiche tecnico funzionali dei beni.

I riferimenti Aula (Aula 1, Aula 2 ecc. sono riportati nelle planimetrie allegate). Per ogni Aula è allegata la planimetria di dettaglio e la disposizione dei beni.

Art. 1

Elenco analitico dei prodotti e dei servizi necessari per dotazioni digitali (attrezzature, contenuti digitali, app e software, etc.)

Arredi e piccoli adattamenti edilizi

A supporto di tutti gli ambienti
Fornitura di una Piattaforma specificatamente progettata e pensata per la ricerca, la creazione e la condivisione di materiali ed attività didattiche con licenza istituto per un periodo minimo di 3 anni. La licenza deve consentire l'utilizzo ad un numero illimitato di utenti. Tale piattaforma consente al docente e allo studente di cercare, scegliere e aggregare contenuti per realizzare "costruzioni didattiche" multimediali personalizzate "Bricks Unit" La piattaforma deve consentire di: • Creare e gestire classi e gruppi classe • Cercare e scegliere contenuti didattici e di approfondimento • Aggregare e integrare con contenuti propri in modo da costruire Bricks Unit personalizzate • Arricchire le lezioni con test e verifiche interattive • Assegnare le Bricks Unit alla classe, ai gruppi o al singolo studente • Può essere utilizzata con qualsiasi device (computer,display interattivo,tablet,smartphone) Basta avere un collegamento a internet. • Condividere e ricercare le lezioni all'interno della Community • Commentare le lezioni e attivare dinamiche di social learning

• La piattaforma deve poter offrire qualsiasi tipo di contenuto (Video, audio, testi, presentazioni, mappe, immagini, oggetti interattivi, animazioni, test, corsi, percorsi, webinar)
• permettere l'accesso ad un archivio digitale di contenuti didattici realizzati da importanti editori del settore scolastico e da altre realtà che producono contenuti di valore educativo, come ad esempio Hub Scuola, Mondadori Education, Rizzoli Education, Pearson, Sanoma, Editrice La Scuola, SEI, etc.

Anna Frank
aula 1
Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime: • Area Attiva 65" • Tecnologia Pannello Ips • Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K • Contrasto 1200:1 • Color Depth 10bit, 1.07Bilion colors • Surface Treatment(Haze) Anti Glare, 7H(Mohs) • Tempo di risposta 8ms (G to G) • 20 Tocchi simultanei in ambiente Windows • Casse integrate minimo 10W • Connettività Hdmi – Usb – Wifi-Lan • Sistema operativo Integrato Android 8.0 • Cavo Usb 5 Mt • Cavo Hdmi 3 Mt • Staffa di supporto omologata inclusa • Garanzia 36 Mesi Casamadre • Certificazione Radio Equipment Directive 2014/53/EU • Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021 • Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863) • FCC (Regulatory) Class "A" • Ce (Regulatory) Saranno a carico della ditta i seguenti servizi: • Consegna e installazione on site • Montaggio a parete mediante staffa di supporto omologata • Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria • Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.

• Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

aula 2, 3
Fornitura e installazione di n.02 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime: • Area Attiva 65” • Tecnologia Pannello Ips • Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K • Contrasto 1200:1 • Color Depth 10bit, 1.07Bilion colors • Surface Treatment(Haze) Anti Glare, 7H(Mohs) • Tempo di risposta 8ms (G to G) • 20 Tocchi simultanei in ambiente Windows • Casse integrate minimo 10W • Connettività Hdmi – Usb – Wifi-Lan • Sistema operativo Integrato Android 8.0 • Cavo Usb 5 Mt • Cavo Hdmi 3 Mt • Staffa di supporto omologata inclusa • Garanzia 36 Mesi Casamadre • Certificazione Radio Equipment Directive 2014/53/EU • Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021 • Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863) • FCC (Regulatory) Class“A” • Ce (Regulatory) Saranno a carico della ditta i seguenti servizi: • Consegna e installazione on site • Montaggio a parete mediante staffa di supporto omologata • Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria • Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe. • Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

aula 4 stem
Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime: • Area Attiva 65” • Tecnologia Pannello Ips • Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K • Contrasto 1200:1 • Color Depth 10bit, 1.07Bilion colors • Surface Treatment(Haze) Anti Glare, 7H(Mohs) • Tempo di risposta 8ms (G to G) • 20 Tocchi simultanei in ambiente Windows • Casse integrate minimo 10W • Connettività Hdmi – Usb – Wifi-Lan • Sistema operativo Integrato Android 8.0 • Cavo Usb 5 Mt • Cavo Hdmi 3 Mt • Staffa di supporto omologata inclusa • Garanzia 36 Mesi Casamadre • Certificazione Radio Equipment Directive 2014/53/EU • Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021 • Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863) • FCC (Regulatory) Class “A” • Ce (Regulatory) Saranno a carico della ditta i seguenti servizi: • Consegna e installazione on site • Montaggio a parete mediante staffa di supporto omologata • Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria • Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe. • Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore
Fornitura e Installazione di n.01 Workstation di primaria marca internazionale avente le seguenti caratteristiche tecniche minime : • Processore I9-13900HX • Ram 16 Gb • SSD PCI EXPRESS 1000 GB • Display 16” WQXGA Ips

- GeForce RTX 4060 8 Gb -GDDR6
- Connettività Wifi 6-Bluetooth 5.0
- Sistema Operativo Windows 11 Home
- Servizio di consegna e Installazione on site
- Breve Corso di Formazione al corretto utilizzo del prodotto

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi

client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset, che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows. L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti. Sicurezza con i sistemi Windows Anti-malware avanzato Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore. • DeepGuard Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale. • Patch management Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc. • Protezione web Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing. • Exchange, SharePoint, Citrix, Linux Componenti di sicurezza dedicate disponibili per piattaforme differenti.
Fornitura e Installazione di n.01 Visore avente le seguenti caratteristiche tecniche minime: • Tecnologia 6DoF, il visore effettua il tracking dei movimenti di testa e corpo per poi tradurli in VR con precisione realistica • Controller Touch ergonomici con appoggio per il pollice • Cinturino Morbido con regolazione • Display LCD a commutazione rapida Risoluzione di 1832x1920 per occhio ,Supporto per frequenza di aggiornamento a 60, 72 e 90 Hz • Audio posizionale 3D integrato direttamente nel visore • SPAZIO DI ARCHIVIAZIONE 128 GB • Cavo ottico attivo USB completo. USB 3.2 Gen 1 Type-C della lunghezza di 5 mt • Configurazione e installazione on site secondo le indicazioni del progettista • Assistenza nella creazione degli account necessari per il collegamento del visore • Corso di formazione della durata di 4 ore al corretto utilizzo del prodotto • Schermo: 1.832 x .1920 pixel per occhio, Fast-switch LCD, 72 Hz • Processore: Qualcomm Snapdragon XR2 • RAM: 6 GB • Audio: 3D positional speaker, jack 3,5 mm • Servizio di Installazione e configurazione son site secondo le indicazioni del progetista •Assistenza alla creazione degli account necessari per il corretto utilizzo del prodotto •Corso di formazione della durata di 4 ore al corretto utilizzo del Visore.

Fornitura e installazione di n.01 LABORATORIO MOBILE SCIENTIFICO TIPO SCIENCEBUS COMPLETO DI 95 ESPERIMENTI IN
AMBITO DI FISICA, CHIMICA, BIOLOGIA E FISIOLOGIA (ALLEGARE DEPLIANT PENA ESCLUSIONE)
Il laboratorio scientifico mobile dovrà permettere l'osservazione di fenomeni scientifici e l'esecuzione di
esperienze nella scuola primaria e secondaria.
Il laboratorio dovrà integrare lateralmente un vano porta strumenti, permettere di custodire in sicurezza
una serie di collezioni scientifiche e di apparecchiature scientifiche necessarie all'esecuzione di esperienze di base in ambito scientifico, di fisica, chimica, biologia e fisiologia.
La struttura dovrà essere robusta, in alluminio e acciaio con angoli arrotondati; il piano di lavoro dovrà
essere in materiale fenolico (spessore almeno 2cm), resistente agli acidi, agli urti e al calore e dovrà essere dotato di 3 aste telescopiche di supporto utili all'esecuzione delle esperienze.
Dovrà essere dotato di maniglioni ergonomici per facilitare trasporto e movimentazione dello stesso.
Il laboratorio mobile scientifico dovrà essere dotato di tre diversi moduli sotto specificati:
- il Modulo lavello dovrà essere dotato di sistema idraulico di carico e scarico acqua (due serbatoi di 10 litri ciascuno); di alimentatore regolabile 0-15 Volt DC con corrente regolabile da 0 a 40 Ampere (max. 600W), fi un indicatore display con Voltmetro e Amperometro digitali, cavo auto -avvolgente di
alimentazione e sul pannello anteriore 2 prese 220V. Il modulo lavello dovràessere dotato di 4 ruote piroettanti con freno
- Modulo centrale dovrà essere dotato di ante trasparenti con chiusura a chiave per contenere i vassoi-collezione incluse con il banco. Porta posteriore a battente con chiusura a chiave per contenimento di eventuali ulteriori oggetti in dotazione. Il modulo centrale dovràessere dotato di 4 ruote piroettanti con freno.
- Modulo laterale dovrà essere dotato di ante trasparenti con serratura a chiave per contenere i vassoi
di raccolta inclusi nel banco. Porta posteriore a battente con chiusura a chiave per contenimento di eventuali ulteriori oggetti in dotazione. Il modulo laterale dovràessere dotato di 4 ruote piroettanti con freno.
Il carrello mobile dovrà essere fornito (di serie) con le seguenti collezioni scientifiche di base: Chimica, Biologia, Fisiologia, Fisica (meccanica, elettricità, magnetismo, ottica, acustica, termologia, elettrostatica) per l'esecuzione di circa un centinaio esperienze in vari ambiti.

√ KIT ACUSTICA (INCLUSO NEL BANCO AUTONOMO SCIENTIFICO SOPRA INDICATO)
Gli studenti dovranno poter analizzare ed osservare da vicino i principi fondamentali dell'Acustica grazie
allo studio dei fenomeni di propagazione delle onde meccaniche nell'aria e la loro influenza su corpi ravvicinati.
In dotazione nel kit dovrà essere fornita tutta la strumentazione necessaria insieme ad un manuale applicativo illustrato utile ad eseguire diversi esperimenti che trattano argomenti come:
- La propagazione delle onde meccaniche nell'aria;

- Generatore di onde meccaniche: il Diapason;
- La Frequenza di un'onda meccanica;
- Il fenomeno della Risonanza;
- Il fenomeno del Battimento acustico.

Lo svolgimento degli esperimenti proposti dovrà essere semplice e guidato in ogni fase di esecuzione
grazie al manuale in italiano.
Il singolo esperimento dovrà essere completato con la descrizione teorica dei principi dimostrati, formule
matematiche e raccolta dei dati sperimentali

√ KIT ELETTRICITA' (INCLUSO NEL BANCO AUTONOMO SCIENTIFICO SOPRA INDICATO)

Gli studenti dovranno poter analizzare, osservare e sperimentare con mano alcuni dei principi fondamentali dell'Elettricità attraverso la costruzione di circuiti con resistenze in serie ed in parallelo, la
conoscenza dei componenti elettronici di base, la misura tramite multimetro di corrente e tens ione in un
circuito elettrico e tanto altro.
In dotazione nel kit dovrà essere fornita tutta la strumentazione necessaria insieme ad un manuale applicativo illustrato utile ad eseguire diversi esperimenti che trattano argomenti come:

- Componenti base di un circuito elettrico;
- Circuiti in serie ed in parallelo;
- Partitori di corrente e di tensione;
- Misura di corrente e di tensione di un circuito elettrico.

Lo svolgimento degli esperimenti proposti dovrà essere semplice e guidato in ogni fase di esecuzione
grazie al manuale in italiano.
Il singolo esperimento dovrà essere completato con la descrizione teorica dei principi dimostrati, formule
matematiche e raccolta dei dati sperimentali

√ KIT TERMODINAMICA (INCLUSO NEL BANCO AUTONOMO SCIENTIFICO SOPRA INDICATO)

Gli studenti dovranno poter analizzare ed osservare da vicino molti dei principi fondamentali della Termodinamica grazie allo studio dei fenomeni di dilatazione dei diversi materiali presenti in natura, oltre alla valutazione della conducibilitàtermica e tanto altro ancora.
In dotazione nel kit dovrà essere fornita tutta la strumentazione necessaria insieme ad un manuale applicativo illustrato utile ad eseguire diversi esperimenti che trattano argomenti come:

- Trasmissione del Calore;
- Isolamento termico;
- Equilibrio termico dei liquidi eterogenei;
- Il Calore specifico dei solidi;
- Misura della Costante di tempo di un termometro.

Lo svolgimento degli esperimenti proposti dovrà essere semplice e guidato in ogni fase di

esecuzione
grazie al manuale in italiano.
Il singolo esperimento dovrà essere completato con la descrizione teorica dei principi dimostrati, formule
matematiche e raccolta dei dati sperimentali

√ KIT OTTICA (INCLUSO NEL BANCO AUTONOMO SCIENTIFICO SOPRA INDICATO)
Gli studenti dovranno poter analizzare ed osservare da vicino molti dei principi fondamentali alla base
dell'Ottica geometrica grazie allo studio dei fenomeni di riflessione e rifrazione della radiazione luminosa, il comportamento delle lenti e tanto altro ancora.
In dotazione nel kit dovrà essere fornita tutta la strumentazione necessaria insieme ad un manuale applicativo illustrato utile ad eseguire diversi esperimenti che trattano argomenti come:
- La Distanza Focale;
- Le Equazioni delle Lenti Sottili;
- L'Ingrandimento;
- Miscelazione radiazioni luminose;
- Sistemi ottici: Microscopio e Telescopio;
- Il Prisma: composizione della luce;
- Ombra e Penombra.
Lo svolgimento degli esperimenti proposti dovrà essere semplice e guidato in ogni fase di esecuzione
grazie al manuale in italiano.
Il singolo esperimento dovrà essere completato con la descrizione teorica dei principi dimostrati, formule
matematiche e raccolta dei dati sperimentali

√ KIT SCIENZE DELLA VITA (INCLUSO NEL BANCO AUTONOMO SCIENTIFICO SOPRA INDICATO)
Gli studenti dovranno poter analizzare, osservare e sperimentare con mano alcuni dei principi fondamentali di Chimica, Biologia ed Anatomia, attraverso lo studio di Acidi e basi, Elettrolisi, Osmosi
e tanto altro.
In dotazione nel kit dovrà essere fornita tutta la strumentazione necessaria insieme ad un manuale applicativo illustrato utile ad eseguire diversi esperimenti che trattano argomenti come:
CHIMICA
- Principio di conservazione della massa;
- Studio di acidi e basi con l'uso del pH-metro;
- Principio dell'elettrolisi;
- Studio e costruzione di pile;
ANATOMIA
- Modelli anatomici delle cellule animali e vegetali;
- Modello anatomico umano;
- Anatomia al microscopio degli insetti;
- Anatomia al microscopio delle piante.

BIOLOGIA
- Principio di osmosi
- Principio di capillarità
- Principio di cromatografia
- Principio di germinazione

Lo svolgimento degli esperimenti proposti dovrà essere semplice e guidato in ogni fase di esecuzione
grazie al manuale in italiano.
Il singolo esperimento dovrà essere completato con la descrizione teorica dei principi dimostrati, formule
matematiche e raccolta dei dati sperimentali

√ KIT MECCANICA (INCLUSO NEL BANCO AUTONOMO SCIENTIFICO SOPRA INDICATO)
Gli studenti dovranno poter analizzare, osservare e sperimentare con mano alcuni dei principi fondamentali della Meccanica classica attraverso lo studio delle Leve, delle Carrucole, delle Molle, del
Piano inclinato e tanto altro.

In dotazione nel kit dovrà essere fornita tutta la strumentazione necessaria insieme ad un manuale applicativo illustrato utile ad eseguire diversi esperimenti che trattano argomenti come:
- Misura di precisione con il calibro;
- Misure di densità e calcolo del volume di corpi solidi;
- Uso di macchine semplici come leve e carrucole;
- Studio e misura delle forze;
- Esperimenti su piano inclinato;
- Il principio del pendolo;
- Misura della pressione dei liquidi e dei gas;
- Meccanica dell'acqua attraverso i vasi comunicanti e la spinta di Archimede.

Lo svolgimento degli esperimenti proposti dovrà essere semplice e guidato in ogni fase di esecuzione
grazie al manuale in italiano.
Il singolo esperimento dovrà essere completato con la descrizione teorica dei principi dimostrati, formule
matematiche e raccolta dei dati sperimentali

√ KIT ELETTROMAGNETISMO (INCLUSO NEL BANCO AUTONOMO SCIENTIFICO SOPRA INDICATO)
Gli studenti dovranno poter analizzare ed osservare da vicino gran parte dei principi fondamentali alla
base dell'Elettromagnetismo grazie allo studio della forza magnetica generata da Magneti permanenti,

passando per all'analisi dei campi Elettro-Magnetici e all'osservazione dei fenomeni di attrazione e repulsione di corpi elettrizzati con accumulo di carica elettrica superficiale indotta per frizione o strofinio. In dotazione nel kit dovrà essere fornita tutta la strumentazione necessaria insieme ad un manuale applicativo illustrato utile ad eseguire diversi esperimenti che trattano argomenti come: - Funzionamento della bussola; - Comportamento e composizione dei magneti; - I campi magnetici ed i loro effetti. - Il principio di elettrizzazione dei corpi; - Elettrizzazione positiva e negativa; - Tecniche di elettrizzazione per strofinio; - Proprietà di elettrizzazione dei materiali: barra di ebanite, vetro e plexiglas; - Il Pendolo elettrostatico. Lo svolgimento degli esperimenti proposti dovrà essere semplice e guidato in ogni fase di esecuzione grazie al manuale in italiano. Il singolo esperimento dovrà essere completato con la descrizione teorica dei principi dimostrati, formule matematiche e raccolta dei dati sperimentali
Modulo laterale di stoccaggio per vassoi o apparecchiature di laboratorio
Modulo Electricity Science Set (01)
Modulo Electromagnetism Science Set (02)
Modulo Mechanics Science Set (03)
Modulo Optics Science Set (04)
Modulo Thermodynamics Science Set (05)
Modulo Acoustics Science Set (06)
Modulo Science of life Science Set (07)
Modulo Biology Science Set (08)

Modulo Alternative energies Science set (10)
Modulo Experiments on vacuum Science set (11)
Fornitura e Installazione di n.01 Pacchetto di contenuti a supporto del Laboratorio di scienza Mobile costituito da 50 Esperimenti fruibili con visore o senza al fine di simulare gli esperimenti fatti in ambiente virtuale. Sarà a carico della ditta l'installazione del pacchetto secondo le indicazioni del progettista L'offerta dovrà includere un breve corso di formazione per il corretto utilizzo del prodotto.

aula 5 lab
Fornitura e Installazione di n.21 All in one di Primaria Marca Internazionale avente le seguenti caratteristiche tecniche minime: • Processore tipo Intel i5-1235u o superiore • Ram : 8GB • Hard Disk 512 Gb SSD • Display 23,8" • Sistema operativo : Win 11 Pro Edu • Servizio di installazione e configurazione on site • Servizio di formazione al corretto utilizzo delle apparecchiature Software Didattico incluso avente le seguenti caratteristiche : Avviare • accendere o spegnere e accedere o disconnettersi da tutti i computer della classe dal PC dell'insegnante. • NOVITÀ – Gli insegnanti possono scegliere tre modalità utente (Facile, Intermedio e Avanzato) per rendere le funzionalità accessibili in base al loro livello di sicurezza edtech. • Nascondi gli schermi di tutti gli studenti per attirare l'attenzione e bloccare anche mouse e tastiere. • Ricollegarsi automaticamente ai PC degli studenti se vengono riavviati. • Usa il layout degli studenti sugli schermi degli insegnanti per adattarli al layout della classe fisica. • Utilizza i profili dei singoli insegnanti per fornire le funzionalità richieste da ciascun insegnante. • Utilizzare l'opzione "Richiedi assistenza" con un clic dalla barra degli strumenti dell'insegnante se è necessario il supporto tecnico. • Reimpostazione delle password di sistema per gli studenti senza supporto IT. • Gli insegnanti possono utilizzare Commenti di studenti per valutare come si sentono, la loro

fiducia in un argomento e se hanno bisogno di ulteriore supporto.
• Gamma flessibile di metodi di connessione ai dispositivi degli studenti, inclusa l'integrazione SIS tramite ClassLink OneRoster e Google Classroom.
Gestione della stampante e dei dispositivi
• Impedire agli studenti di stampare in classe.
• Limita l'utilizzo della stampante per numero di pagine.
• Richiedi l'autorizzazione del docente prima della stampa.
• Impedire l'utilizzo di singole stampanti.
• Visualizza un indicatore di stampa in tempo reale che identifica lo studente che sta attualmente stampando.
• Mostra il numero di lavori di stampa in pausa che richiedono l'attenzione dell'insegnante.
• Impedire che i dati vengano copiati su o da periferiche di archiviazione USB e CDR / DVD.
• Disattiva la webcam sui dispositivi della classe.

Registro degli studenti
• Richiedi informazioni standard e personalizzate da ogni studente all'inizio della lezione.
• Stampa il registro degli studenti, incluso un totale di eventuali ricompense o lavori di stampa completati durante la lezione.
• Utilizzare icone personalizzate per ciascun gruppo di studenti.

Distribuisci e raccogli file
• Distribuisci file e cartelle dal PC del tutor a più dispositivi studente.
• Trasferisci file da e verso PC selezionati o multipli in un'unica azione.
• Invio e raccolta automatica dei file, con l'inclusione dei dettagli di ogni Studente.
• Il feedback in tempo reale mostra all'insegnante quali file degli studenti sono pronti per la raccolta e quali studenti devono ricordare.
Barra d'informazioni per gli Studenti
• Visualizza obiettivi della lezione e risultati di apprendimento.
• Fornisce informazioni sulle lezioni in tempo reale, ad esempio il titolo della lezione; tempo rimanente; tutti i premi che sono stati dati dall'insegnante.
• Richiedi assistenza dall'insegnante tramite il pulsante di aiuto.
• Accedi al loro diario digitale.
• Accedi alla cartella delle risorse personali dello studente.
• Verifica quali restrizioni sono attualmente presenti, ad esempio Internet, applicazioni, stampa, chiavette USB.
Strumenti dei tecnici
• Il software viene inoltre fornito con una Console dei tecnici per aiutare il team IT della scuola a supportare gli utenti e gestire i dispositivi in tutta la scuola. I tecnici IT possono eseguire il potente 1:1 PC Remote Control su qualsiasi computer selezionato, acquisire schermate, annotare lo schermo e fornire assistenza tecnica diretta a qualsiasi insegnante di classe. E per un controllo completo, possono anche applicare le impostazioni a livello di scuola come Internet e le restrizioni delle applicazioni che sono "sempre attive".
istruzione in Tempo Reale (Modalità Mostra)
• Mostra il desktop del Tutor a tutti o studenti selezionati.

• Mostrare lo schermo di uno studente (modalità Mostra).
• Limitare l'accesso a Internet ai siti approvati solo durante lo spettacolo.
• Mostra un'applicazione specifica agli studenti selezionati.
• Annotate lo schermo di una Presentazione o durante il Controllo Remoto con una serie di strumenti che facilitano la presentazione (come frecce, forme, evidenziatori e testo).
• Mostrate un "Replay file" (precedentemente registrato) agli studenti selezionati.
• Mostrate un file video agli studenti selezionati.
• Lasciate una registrazione della vostra presentazione sui computer degli studenti, per la revisione in un secondo momento.
• Usate la modalità Audio per parlare agli studenti durante una presentazione.
• Inviate le vostre presentazioni ottimizzate per le reti wireless.

Lavagna virtuale
Una lavagna a tutto schermo, integrata direttamente nella Console Tutor, che contiene una gamma completa distrumenti di disegno per migliorare la collaborazione con l'aula.

Leader di gruppo
Ad uno Studente possono essere assegnati certi diritti di tutor in modo che possa agire da leader di gruppo fino alla revocadi tali privilegi. Adesso include un layout visivo dei leader di gruppo e dei relativi membri del gruppo.

Chat
Apri una discussione in chat a cui puoi partecipare tutti gli studenti o solo quelli selezionati, registrati i loro commenti e condivideteli con gli altri membri della classe (adesso disponibile con emoticon!).

Supporto audio
Trasmettete la voce dell'insegnante durante una presentazione. Il supporto audio è incluso in ogni sessione di Presentazione dello schermo e di Controllo Remoto.

Barra degli strumenti dell'insegnante
Quando l’applicazione dell’insegnante è ridotta a icona, Il software dovrà fornire una comoda barra degli strumenti per accedere rapidamente alle sue funzioni chiave. Questa barra degli strumenti è ottimizzata per l’impiego con le lavagne interattive.

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente

vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso

di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.22 Cuffia e Microfono Professionale avente le seguenti caratteristiche minime:

CARATTERISTICHE FISICHE
- Tipologia Cuffie con filo
- Fattore di forma Sovraurali (On-Ear Headphones)
- Microfono incorporato Sì

CARATTERISTICHE TECNICHE
- Sensibilità 120 dB
- Impedenza 38 Ohm
- Risposta in frequenza 20 - 20.000
- Ascolto musica Sì
- Controllo remoto Controllo chiamate
- Noise canceling si

CONNETTIVITÀ
- Alimentazione USB
- Tipo di porta USB-A

Fornitura e Installazione di n.01 Workstation per la grafica avente le seguenti caratteristiche tecniche minime:

- Processore Intel Core I7-13700F
- Ram 16 Gb DDR4
- Hard Disk 512 GB M2 Pcie
- Scheda Video RTX 3060 VENTUS 2X 8 GB
- Sistema Operativo Windows 11 Professional
- Mouse e Tastiera Usb
- Installazione e configurazione secondo le indicazioni del Progettista
- Corso di formazione al corretto utilizzo del prodotto **Software di sicurezza avente le seguenti caratteristiche**

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.

Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.

Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset, che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.02 Monitor Lcd avente le seguenti caratteristiche tecniche minime:
• Display 23,8” Ips
• Risoluzione 1920x1080 (FullHD)

• Luminosità 300 cd/m2 • Refresh rate 100 Mhz • Connettività Display Port – Hdmi -Vga • Multimediale 2x2W • Less Blue Light (Low Blue) • Installazione e configurazione secondo le indicazioni del progettista • Cavi di collegamento inclusi • Corso di formazione al corretto funzionamento dei prodotti
Fornitura e Installazione di n.01 Monitor Interattivo 75" avente le seguenti caratteristiche tecniche minime: • Tocchi supportati Fino a 40 tocchi simultanei • Vetro Temperato caldo, sp 4mm, anti glare • Modalità di scrittura Dita,penna o strumento non trasparente • Durezza del vetro 7 Mohs • Precisione di puntamento ≤ 1mm • Profondità del tocco 3 ± 0.5mm • Caratteristiche display IPS Direct LED • Rapporto di visualizzazione 16:9 • Risoluzione 4K UHD 3840 x 2160pixels, Freq 60 HZ • Sistema Operativo Android 11 o Cpu Quad core ARM Cortex-A55 o Ram 4 GB DDR4 o Rom 32 Gb o Conettività Bluetooth 5.0 – Wireless Built-in 802.11 a/b/g/n/ac/ax Wifi 6 2.4/5GHz, 2x2 • Casse 2x20W • Porte Frontali Hdmi 2.0 – Usb 3.0 – Usb-c Saranno a carico della ditta i seguenti servizi: • Consegna e installazione on site • Montaggio a parete mediante staffa di supporto omologata • Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria • Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe. • Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore
Fornitura e Installazione di n.01 Software Didattico a supporto dei personal computer avente le seguenti caratteristiche : Avviare • accendere o spegnere e accedere o disconnettersi da tutti i computer della classe dal PC dell'insegnante. • NOVITÀ – Gli insegnanti possono scegliere tre modalità utente (Facile, Intermedio e Avanzato) per rendere le funzionalità accessibili in base al loro livello di sicurezza edtech.

• Nascondi gli schermi di tutti gli studenti per attirare l'attenzione e bloccare anche mouse e tastiere.
• Ricollegarsi automaticamente ai PC degli studenti se vengono riavviati.
• Usa il layout degli studenti sugli schermi degli insegnanti per adattarli al layout della classe fisica.
• Utilizza i profili dei singoli insegnanti per fornire le funzionalità richieste da ciascun insegnante.
• Utilizzare l'opzione "Richiedi assistenza" con un clic dalla barra degli strumenti dell'insegnante se è necessario il supporto tecnico.
• Reimpostazione delle password di sistema per gli studenti senza supporto IT.
• Gli insegnanti possono utilizzare Commenti di studenti per valutare come si sentono, la loro fiducia in un argomento e se hanno bisogno di ulteriore supporto.
• Gamma flessibile di metodi di connessione ai dispositivi degli studenti, inclusa l'integrazione SIS tramite ClassLink OneRoster e Google Classroom.

Gestione della stampante e dei dispositivi
• Impedire agli studenti di stampare in classe.
• Limita l'utilizzo della stampante per numero di pagine.
• Richiedi l'autorizzazione del docente prima della stampa.
• Impedire l'utilizzo di singole stampanti.
• Visualizza un indicatore di stampa in tempo reale che identifica lo studente che sta attualmente stampando.
• Mostra il numero di lavori di stampa in pausa che richiedono l'attenzione dell'insegnante.
• Impedire che i dati vengano copiati su o da periferiche di archiviazione USB e CDR / DVD.
• Disattiva la webcam sui dispositivi della classe.

Registro degli studenti
• Richiedi informazioni standard e personalizzate da ogni studente all'inizio della lezione.
• Stampa il registro degli studenti, incluso un totale di eventuali ricompense o lavori di stampa completati durante la lezione.
• Utilizzare icone personalizzate per ciascun gruppo di studenti.

Distribuisci e raccogli file
• Distribuisci file e cartelle dal PC del tutor a più dispositivi studente.
• Trasferisci file da e verso PC selezionati o multipli in un'unica azione.
• Invio e raccolta automatica dei file, con l'inclusione dei dettagli di ogni Studente.
• Il feedback in tempo reale mostra all'insegnante quali file degli studenti sono pronti per la raccolta e quali studenti devono ricordare.

Barra d’informazioni per gli Studenti
• Visualizza obiettivi della lezione e risultati di apprendimento.
• Fornisce informazioni sulle lezioni in tempo reale, ad esempio il titolo della lezione; tempo rimanente; tutti i premi che sono stati dati dall'insegnante.
• Richiedi assistenza dall'insegnante tramite il pulsante di aiuto.
• Accedi al loro diario digitale.
• Accedi alla cartella delle risorse personali dello studente.
• Verifica quali restrizioni sono attualmente presenti, ad esempio Internet, applicazioni, stampa, chiavette USB.

Strumenti dei tecnici
• Il software viene inoltre fornito con una Console dei tecnici per aiutare il team IT della scuola a supportare gli utenti e gestire i dispositivi in tutta la scuola. I tecnici IT possono eseguire il potente 1:1 PC Remote Control su qualsiasi computer selezionato, acquisire schermate, annotare lo schermo e fornire assistenza tecnica diretta a qualsiasi insegnante di classe. E per un controllo completo, possono anche applicare le impostazioni a livello di scuola come Internet e le restrizioni delle applicazioni che sono "sempre attive".
istruzione in Tempo Reale (Modalità Mostra)
• Mostra il desktop del Tutor a tutti o studenti selezionati.
• Mostrare lo schermo di uno studente (modalità Mostra).
• Limitare l'accesso a Internet ai siti approvati solo durante lo spettacolo.
• Mostra un'applicazione specifica agli studenti selezionati.
• Annotate lo schermo di una Presentazione o durante il Controllo Remoto con una serie di strumenti che facilitano la presentazione (come frecce, forme, evidenziatori e testo).
• Mostrate un "Replay file" (precedentemente registrato) agli studenti selezionati.
• Mostrate un file video agli studenti selezionati.
• Lasciate una registrazione della vostra presentazione sui computer degli studenti, per la revisione in un secondo momento.
• Usate la modalità Audio per parlare agli studenti durante una presentazione.
• Inviate le vostre presentazioni ottimizzate per le reti wireless.
Lavagna virtuale
Una lavagna a tutto schermo, integrata direttamente nella Console Tutor, che contiene una gamma completa distrumenti di disegno per migliorare la collaborazione con l'aula.

Leader di gruppo
Ad uno Studente possono essere assegnati certi diritti di tutor in modo che possa agire da leader di gruppo fino alla revoca di tali privilegi. Adesso include un layout visivo dei leader di gruppo e dei relativi membri del gruppo.
Chat
Apri una discussione in chat a cui puoi partecipare tutti gli studenti o solo quelli selezionati, registrati i loro commenti e condivideteli con gli altri membri della classe (adesso disponibile con emoticon!).
Supporto audio
Trasmettete la voce dell'insegnante durante una presentazione. Il supporto audio è incluso in ogni sessione di Presentazione dello schermo e di Controllo Remoto.
Barra degli strumenti dell'insegnante
Quando l'applicazione dell'insegnante è ridotta a icona, Il software dovrà fornire una comoda barra degli strumenti per accedere rapidamente alle sue funzioni chiave. Questa barra degli strumenti è ottimizzata per l'impiego con le lavagne interattive.

Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime:
• Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in 2.4 GHz + 2402 Mbps in 5 GHz).
• Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore

rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente.
• Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at).
• Piena compatibilità con il sistema di gestione già presente a scuola
• Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista .
• Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

Eventuali spese per acquisto di arredi tecnici

Fornitura e Montaggio di n.01 Tavolo con gambe metalliche canalizzabili a "T" rovescio colore Argento V001, top sp,25mm nobilitato melaminico colore a scelta Aceo, Rovere o Noce esperia, corredato di 2 borchie pasascavi
Dim. cm.180X70X72H

Fornitura e Montaggio di n.03 Tavolo con gambe metalliche canalizzabili a "T" rovescio colore Argento V001, top sp,25mm nobilitato melaminico colore a scelta Aceo, Rovere o Noce esperia, corredato di 2 borchie pasascavi E PANNELLO PARAGAMBE COLORE ARGENTO
Dim. cm.80X70X72H

Fornitura di n.21 Seduta Allievo avente le seguenti caratteristiche , Seduta fissa 4 gambe senza braccioli, telaio cromato, seduta e schienale monoscocca in termoplastica.

Fornitura e Montaggio di n.01 Poltroncina Postazione Docente avente le seguenti caratteristiche: Poltrona operativa con braccioli fissi in nylon. Schienale alto in nylon grigio con Up&Down. Base a 5 razze in nylon grigio. Certificazione di conformità UNI EN 1335-B. Dim. cm. LxPxH 59X65X98/111

Fornitura e Montaggio di n.09 Tavolo con gambe metalliche canalizzabili a "T" rovescio colore Argento V001, top sp,25mm nobilitato melaminico colore a scelta Aceo, Rovere o Noce esperia Dim. cm.160X70X72H

Eventuali spese per piccoli interventi di carattere edilizio strettamente funzionali all'intervento

Installazione e posa in opera di n.02 Punto rete lan RJ45 comprensivo di cavi , canaline , accessori e quanto altro necessario al corretto funzionamento dello stesso .Il cavo per la distribuzione deve
essere di tipo non schermato U/UTP Cat. 6 CAT.6 CCA AWG23 -LSZA - Cca s1a, d1,a1

Installazione di un Quadro elettrico esterno a tenuta con grado di prot. IP65, reversibilità della porta e la completa apertura a 180° , per 12 unità lavorative composta da:
• Indicatore luminoso 1x LED, 230 V rosso
• Interruttore sezionatore 2P 40A 230/400V 2 moduli DIN
• N.03 Interruttori magnetotermici differenziale, 4,5 kA, 1P+N, Tipo AC, 30 mA, Car. C, In: 16 A, Un AC: 230 V
Montante di raccordo da Quadro generale al Quadro da Alimentare mediante cablatura con 3 Cavi

unipolare FG17 Conduttore unipolare di rame rosso ricotto isolato in gomma HEPR di qualità G17.
Tensione nominale: Uo/U: 450/750 V - Classe di reazione al fuoco: Cca-s1b,d1,a1. Sigla di designazione FG17 - 1 x 4 mmq (Max 30 Mt)
Installazione e posa in opera di n.13 punto elettrico con bivalente e shuko con montante al quadro elettrico principale nell'apposito differenziale magnetotermico. Gli impianti saranno realizzati secondo quanto disposto dal d.m. 37/2008

aula 6 polifunzionale
Fornitura e Installazione di n.01 Monitor Interattivo 86" avente le seguenti caratteristiche tecniche minime: • Tocchi supportati Fino a 40 tocchi simultanei • Vetro Temperato caldo, sp 4mm, anti glare • Modalità di scrittura Dita,penna o strumento non trasparente • Durezza del vetro 7 Mohs • Precisione di puntamento ≤ 1mm • Profondità del tocco 3 ± 0.5mm • Caratteristiche display IPS Direct LED • Rapporto di visualizzazione 16:9 • Risoluzione 4K UHD 3840 x 2160pixels, Freq 60 HZ • Sistema Operativo Android 11 o Cpu Quad core ARM Cortex-A55 o Ram 4 GB DDR4 o Rom 32 Gb o Conettività Bluetooth 5.0 – Wireless Built-in 802.11 a/b/g/n/ac/ax Wifi 6 2.4/5GHz, 2x2 • Casse 2x20W • Porte Frontali Hdmi 2.0 – Usb 3.0 – Usb-c Saranno a carico della ditta i seguenti servizi: • Consegna e installazione on site • Montaggio a parete mediante staffa di supporto omologata • Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria • Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe. • Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Carrello Mobile per Monitor Interattivo avente le seguenti caratteristiche tecniche minime : • Adatto per Monitor fino da 55” a 86” • Portata massima 100Kg • Regolazione dell’altezza manuale (1576-1759mm) • Ruote mobili con freno • Sarà a carico della ditta il servizio di installazione del Monitor Interattivo indicato dalla nostra amministrazione sullo stesso .
Fornitura e Installazione di n.01 Kit per la Videoconferenza avente le seguenti caratteristiche : • Piena Compatibilità con il Monitor previsto nel capitolato • Risoluzione fino a 3840x2160P @ 25 FPS IMAGE EDITING OUTPUT • Dimensioni del sensore 1,2.8” • Riduzione del rumore digitale 2d.3d • Camera da 12 MPixel • Auto focus • Grandangolo 120° con ottica 4k • 8 microfono integrati con raggio di rilevamento fino ad 8 metri • Installazione e configurazione secondo le indicazioni del progettista • Corso di formazione al corretto utilizzo del prodotto .

aula 7 musica
Fornitura e Installazione di n.01 Monitor Interattivo 75” avente le seguenti caratteristiche tecniche minime: • Tocchi supportati Fino a 40 tocchi simultanei • Vetro Temperato caldo, sp 4mm, anti glare • Modalità di scrittura Dita,penna o strumento non trasparente • Durezza del vetro 7 Mohs • Precisione di puntamento ≤ 1mm • Profondità del tocco 3 ± 0.5mm • Caratteristiche display IPS Direct LED • Rapporto di visualizzazione 16:9 • Risoluzione 4K UHD 3840 x 2160pixels, Freq 60 HZ • Sistema Operativo Android 11 o Cpu Quad core ARM Cortex-A55 o Ram 4 GB DDR4 o Rom 32 Gb o Conettività Bluetooth 5.0 – Wireless Built-in 802.11 a/b/g/n/ac/ax Wifi 6 2.4/5GHz, 2x2

- Casse 2x20W
- Porte Frontali Hdmi 2.0 – Usb 3.0 – Usb-c

Saranno a carico della ditta i seguenti servizi:
- Consegna e installazione on site
- Montaggio a parete mediante staffa di supporto omologata
- Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria
- Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
- Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Workstation per la grafica avente le seguenti caratteristiche tecniche minime:

- Processore Intel Core I7-13700F
- Ram 16 Gb DDR4
- Hard Disk 512 GB M2 Pcie
- Scheda Video GTX1650 D6 AERO ITX OCV1
- Sistema Operativo Windows 11 Professional
- Mouse e Tastiera Usb
- Installazione e configurazione secondo le indicazioni del Progettista
- Corso di formazione al corretto utilizzo del prodotto **Software di sicurezza avente le seguenti caratteristiche**

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più

importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.

Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito. Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del

browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset, che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.01 Monitor Lcd avente le seguenti caratteristiche tecniche minime:
• Display 23,8” Ips
• Risoluzione 1920x1080 (Full HD)
• Luminosità 300 cd/m2
• Refresh rate 100 Mhz
• Connettività Display Port – Hdmi -Vga

- Multimediale 2x2W
- Less Blue Light (Low Blue)
- Installazione e configurazione secondo le indicazioni del progettista
- Cavi di collegamento inclusi
- Corso di formazione al corretto funzionamento dei prodotti

Fornitura e Installazione di n.01 INTERFACCIA AUDIO USB avente le seguenti caratteristiche tecniche minime:

- Compatibilità multipiattaforma Windows, macOS e iOS per una flessibilità superiore
- Preamplificatori microfonici D-PRE di Classe A con alimentazione phantom +48V
- Gli ingressi a doppia combinazione supportano strumenti e connessioni microfoniche
- Il connettore da USB 3.0 a USB-C può connettersi alla maggior parte dei dispositivi moderni
- Il monitoraggio senza latenza ha controlli di bilanciamento del mix
- L'I/O MIDI consente di sincronizzarsi con l'hardware esterno
- Controllo separato del livello delle cuffie
- Fonte di alimentazione selezionabile: USB 3.0 o 9V CC
- Dimensioni: 159 x 37 x 149mm

Saranno a carico della ditta le operazioni di installazione e configurazione on site

Fornitura e installazione di n.01 Cuffia Professionale avente le seguenti caratteristiche :

- Principio acustico: Dinamico, aperto
- Risposta in frequenza: 6Hz - 38 kHz (-10dB)
- Impedenza: 120 Ohm
- Livello di pressione sonora (SPL): 110dB (1 kHz / 1V RMS)
- THD, Distorsione Armonica Totale: < 0,05% (1 kHz / 90dB SPL)
- Accoppiamento auricolare: Circumaurale
- Temperatura di stoccaggio: -55°C / +70°C
- Temperatura di esercizio: -15°C / +55°C
- Umidità relativa di esercizio: ≤ 90%
- Materiale dei cuscinetti auricolari: Velluto
- Connettore: Jack 3,5mm con adattatore da 6,3mm
- Peso: 240g
- Consegna e installazione on site, fornitura di eventuali cavi di collegamento necessari

Fornitura e installazione di n.01 MICROFONO A CONDENSATORE CARDIOIDE A DIAFRAMMA LARGO avente le seguenti caratteristiche tecniche:

- Microfono a condensatore cardioide a diaframma largo
- Capsula a condensatore HF6 da 1" spruzzata d'oro
- Risposta in frequenza regolare, alta sensibilità e gestione SPL elevata
- Rumore eccezionalmente basso (4dBA): il microfono a condensatore da studio più silenzioso al mondo
- Uscita Dual Connect in attesa di brevetto con connettività XLR e USB
- Prima uscita digitale float a 32 bit al mondo
- Conversione da analogico a digitale ad altissima risoluzione (fino a 192kHz)
- DSP integrato per elaborazione audio APHEX avanzata
- Supporto antiurto e filtro pop da studio, cavi XLR e USB inclusi

• Disponibile in silver con un robusto corpo in alluminio e finiture di alta qualità • Progettato e realizzato negli impianti di produzione di precisione RØDE a Sydney, in Australia • Finitura: Silver • Dimensioni: 52 x 52 x 189mm • Peso: 308g • Installazione on site • Fornitura di eventuali cavi di collegamento necessari +Asta da Tavolo
Fornitura e installazione di n.01 COPPIA DI MONITOR DI RIFERIMENTO 4.5″ 120W avente le seguenti caratteristiche tecniche: • Risposta in frequenza: 69Hz - 22kHz • Potenza in uscita: 120W (picco totale), 2x 25W (RMS) • Driver LF: 4.5"/114,3mm • Driver HF: 1"/ 25,4mm, cupola in seta • Ingressi audio: 1x RCA stereo, 2x TRS da 6,35mm (1/4 "), 1x Aux stereo da 3,5mm (1/8") • Uscita cuffie: 1x Jack 1/8" stereo (3,5mm) • Cavo di interconnessione: TS da 1/8" (3,5mm) • Alimentazione: 100-240V CA, 50/60Hz, 85W • Dimensioni: 156 x 175 x 225mm • Peso (per altoparlante): 4,46kg Software MPC Beats incluso • 3 Virtual Instruments: TubeSynth, Electric, Bassline • 80 FX Plugin: AIR Channel Strip, Half Time • Installazione on site secondo le esigenze dell'amministrazione , saranno a carico della ditta eventuali staffe a parete e cavi di collegamento necessari al corretto funzionamento dell'impianto
Fornitura e installazione di n. TASTIERA CONTROLLER MIDI USB 32 TASTI avente le seguenti caratteristiche tecniche: • 32 Mini tasti sensibili alla dinamica • Perfetta per i mobile studio • 4 Controlli assegnabili • Curve della dinamica selezionabili • Pulsanti Pitch e Modulation assegnabili • Costruzione robusta e con materiali di alta qualità • Alimentata tramite Bus USB • Compatibilità nativa su PC e MAC • Utilizzabile con dispositivi iOS tramite connettore Apple Lightning to USB Camera Adapter (non incluso) • Include suite di software professionali: AIR Xpand!2 • Dimensioni: 418 x 105 x 20mm • Peso: 0,45kg Software MPC Beats incluso • 3 Virtual Instruments (TubeSynth, Electric, Bassline) • 80 FX Plugin (AIR Channel Strip, Half Time) • 2GB di contenuti factory con la libreria di strumenti F9

- Installazione on site
- Cavi di collegamento necessari
- Breve corso di formazione al corretto utilizzo del prodotto

Fornitura e Installazione di n.01 Software per produzione musicale Tipo Cubase Elements 12 Ita avente le seguenti caratteristiche tecniche minime:

- Perfetto per tecnici audio professionisti, cantautori, compositori e direttori d'orchestra
- Il motore audio in virgola mobile a 64 bit di nuova generazione ti offre molta potenza
- La registrazione MIDI retrospettiva tiene traccia dell'input MIDI, anche quando non stai registrando
- La modalità di avvio sicuro ti consente di avviare Cubase senza che siano stati caricati plug-in di terze parti
- I canali del mixer colorati velocizzano il tuo flusso di lavoro
- Strumenti compositivi intelligenti come Chord Track, Chord Pad e Chord Assistant
- L'equalizzazione con confronto spettrale semplifica l'identificazione e l'eliminazione delle collisioni di frequenza
- Consente una facile importazione di audio e dati da altri progetti salvati
- MixConsole cattura l'essenza di una console analogica di fascia alta
- Sampler Track e Caleidoscope per costruire loop e frasi
- Set completo di 3 strumenti eccezionali con oltre 1000 suoni
- Controlli MIDI estesi, personalizzazione flusso di lavoro e dei tasti di comando, automazione dei volumi dei sample e conversione audio / MIDI
- Ora ottimizzato per i processori in silicio Apple tramite Rosetta 2

Saranno a carico della ditta le operazioni di installazione on site sul personal computer indicato dall'amministrazione

Fornitura e Installazione di n.01 SISTEMA MICROFONICO WIRELESS avente le seguenti caratteristiche tecniche minime:

- Tipo di trasmissione: Frequenza digitale 2,4GHz
- Modulazione: GFSK
- Connettore di uscita: Jack 3,5mm
- Livello di uscita audio: -60dBV
- Requisiti di alimentazione: Batteria agli ioni di litio incorporata o USB-C 5V
- Durata della batteria incorporata: 6 ore circa
- Antenna: antenna PIFA
- Temperatura di funzionamento: 0°C - 50°C
- Dimensioni: 62 x 33 x 15,5mm
- Peso: 26,5g
- Caratteristiche B2 Blink500 TX: Frequenza digitale 2.4GHz, GFSK, Potenza di uscita RF 10 mW, Diagramma polare Omnidirezionale, SPL 120dB
- Requisiti di alimentazione: Batteria agli ioni di litio incorporata o USB-C 5V
- Durata della batteria incorporata: 6 ore circa
- Antenna: PIFA

- Ingressi audio: Microfono Lavalier TRS 3,5mm o microfono incorporato
- Temperatura di funzionamento: 0°C - 50°C
- Dimensioni: 63 x 43 x 16,5mm
- Peso: 34g
- Installazione on site
- Breve corso di formazione al corretto utilizzo del prodotto

PLESSO Alberoni
aula 1 lab

Fornitura e Installazione di n.18 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche minime:

- Processore tipo intel I5-1235U o superiore
- Ram 8 Gb DDR4
- Hard Disk 256 Gb SSD
- Scheda Grafica Intel Iris Xe Graphics
- Display 15,6" FHD
- Web Cam e 2 Microfono digitali integrati
- Connettività Bluetooth – Wifi 802.11ax -2 Usb-Type C 1 Hdmi
- Sistema Operativo Windows 11 Home
- Servizio di installazione e configurazione on site Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.

Fornitura e Installazione di n.01 MICROFONO DINAMICO CARDIOIDE PER VOCE avente le seguenti caratteristiche tecniche minime:

- Tipo: Dinamico (Moving Coil)
- Risposta in frequenza: 50Hz - 15kHz
- Diagramma Polare: Cardioide
- Sensibilità (@ 1KHz Tensione a Circuito Aperto): -54,5dBV/Pa (1.85 mV) 1 Pa = 94 dB SPL

- Impedenza: 150 Ohm (nominale), 300 Ohm (effettiva)
- Connettore: XLR M 3-pin
- Peso: 0,298 kg
- Cavi di collegamento necessari al corretto funzionamento dell'impianto+Asta da tavolo

Asta Microfonica avente le seguenti caratteristiche :

- Diametro base: 680mm
- Altezza minima: 900mm
- Altezza max: 1500mm
- Lunghezza giraffa: 750mm
- Finitura: Nero opaco
- Peso: 2,2kg

Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad

esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset, che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.18 Cuffia e Microfono Professionale avente le seguenti caratteristiche minime:
CARATTERISTICHE FISICHE
• Tipologia Cuffie con filo
• Fattore di forma Sovraurali (On-Ear Headphones)
• Microfono incorporato Sì
CARATTERISTICHE TECNICHE
• Sensibilità 120 dB
• Impedenza 38 Ohm
• Risposta in frequenza 20 - 20.000
• Ascolto musica Sì
• Controllo remoto Controllo chiamate

• Noise canceling si CONNETTIVITÀ • Alimentazione USB • Tipo di porta USB-A
Fornitura e Installazione di n.01 Carrello di ricarica avente le seguenti caratteristiche : Il carrello dovrà essere composto da 2 ripiani con 32 postazioni per dispositivi fino a 15,6" (tablet e notebook), ventole raffredamento, Sistema di apertura e chiusura Digital Lock , Smart Charging System, input Volt 100-250V, max power 110V/230V max 16A, adattatore AC, garanzia 24 mesi on center
Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime: • Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in 2.4 GHz + 2402 Mbps in 5 GHz). • Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente. • Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at). • Piena compatibilità con il sistema di gestione già presente a scuola • Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista . • Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

aula 2,3,4
Fornitura e Installazione di n.03 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche minime: • Processore tipo intel I5-1235U o superiore • Ram 8 Gb DDR4 • Hard Disk 256 Gb SSD • Scheda Grafica Intel Iris Xe Graphics • Display 15,6” FHD • Web Cam e 2 Microfono digitali integrati • Connettività Bluetooth – Wifi 802.11ax -2 Usb-Type C 1 Hdmi • Sistema Operativo Windows 11 Home • Servizio di installazione e configurazione on site Software di sicurezza avente le seguenti

caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti

dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.

L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti. Sicurezza con i sistemi Windows Anti-malware avanzato Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore. • DeepGuard Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale. • Patch management Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc. • Protezione web Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing. • Exchange, SharePoint, Citrix, Linux Componenti di sicurezza dedicate disponibili per piattaforme differenti.
Fornitura e Installazione di n.02 abbonamento della durata di 12 mesi ad una piattaforma che offre contenuti didattici e specificatamente : • Categoria di contenuti: o Scene 3d o Lezioni o Strumenti o Video • Tipologia dei contenuti: o Biologia o Fisica o Geografia o Chimica o Storia o Tecnologia o Matematica o Arti Visive o Letteratura La piattaforma dovrà consentire l'esecuzione dei contenuti mediante un player dedicato . Sarà a carico della ditta l'effettuazione di un corso di formazione a supporto del personale preposto della nostra amministrazione al fine di utilizzare al meglio la piattaforma .

aula 5
Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime: • Area Attiva 65” • Tecnologia Pannello Ips • Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K • Contrasto 1200:1 • Color Depth 10bit, 1.07Bilion colors • Surface Treatment(Haze) Anti Glare, 7H(Mohs) • Tempo di risposta 8ms (G to G) • 20 Tocchi simultanei in ambiente Windows • Casse integrate minimo 10W • Connettività Hdmi – Usb – Wifi-Lan • Sistema operativo Integrato Android 8.0 • Cavo Usb 5 Mt • Cavo Hdmi 3 Mt • Staffa di supporto omologata inclusa • Garanzia 36 Mesi Casamadre • Certificazione Radio Equipment Directive 2014/53/EU • Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021 • Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863) • FCC (Regulatory) Class“A” • Ce (Regulatory) Saranno a carico della ditta i seguenti servizi: • Consegna e installazione on site • Montaggio a parete mediante staffa di supporto omologata • Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria • Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe. • Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

aula 6,7,8,9
Fornitura e Installazione di n.04 Tablet di Primaria Marca Internazionale avente le seguenti caratteristiche tecniche minime: CONNETTIVITÀ • WI-FI Sì • Tipo WI-FI 802.11a/b/g/n/ac • Bluetooth Sì PROCESSORE • Tipologia Processore Unisoc T618 SCHERMO • Dimensione 10,5 " • Risoluzione Schermo orizzontale 1.200 px • Tipo TFT • Risoluzione Schermo verticale 1.920 px CONTENUTO CONFEZIONE • Cavo Usb Sì • Altro Caricabatterie 7.75- Cavo dati Type C MEMORIA • RAM 4 GB • ROM 64 GB • Espansione MICROSD Sì • Espansione SD No • Altre caratteristiche Espandibile con microSD fino a 1 TB FOTOCAMERA • Fotocamera frontale Sì • Fotocamera posteriore Sì • Megapixel Fotocamera posteriore 8 • Megapixel Fotocamera frontale 5 ALIMENTAZIONE • Durata Batteria in standby 7.040 min • Connettore di alimentazione Usb Type-C PORTE • Tipo porte USB USB Type-C • Mini Jack Stereo 3,5 mm Sì • USB Tipo C Sì AUDIO • Altoparlanti Sì • Microfono Sì • Caratteristiche Audio Suono surround con quattro speaker: I quattro altoparlanti Dolby riproducono il suono che ami in qualità cinematografica. SISTEMA OPERATIVO/SOFTWARE • S.O. Android • Versione S.O. 11

SERVIZI INCLUSI NELL'OFFERTA
- Servizio di Installazione e configurazione on site secondo le indicazioni del progettista
- Breve corso di formazione al corretto utilizzo del prodotto

Plesso Mazzini

Aula 1,2

Fornitura e Installazione di n.02 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
- Processore Intel Core I5 di 10 Th Generazione o superiore
- Ram 8 Gb DDR4
- Hard Disk tipo SSD da 256 Gb
- Connettività Ethernet 1000 Mbps -Wireless
- Sistema Operativo Windows 10 o superiore
- Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
- Installazione on site , installazione degli applicativi indicati dalla scuola

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità

precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud,

basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito. Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset, che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e installazione di n.02 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:
• Area Attiva 65”
• Tecnologia Pannello Ips
• Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
• Contrasto 1200:1
• Color Depth 10bit, 1.07Bilion colors

- Surface Treatment(Haze) Anti Glare, 7H(Mohs)
- Tempo di risposta 8ms (G to G)
- 20 Tocchi simultanei in ambiente Windows
- Casse integrate minimo 10W
- Connettività Hdmi – Usb – Wifi-Lan
- Sistema operativo Integrato Android 8.0
- Cavo Usb 5 Mt
- Cavo Hdmi 3 Mt
- Staffa di supporto omologata inclusa
- Garanzia 36 Mesi Casamadre
- Certificazione Radio Equipment Directive 2014/53/EU
- Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
- Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
- FCC (Regulatory) Class "A"
- Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:
- Consegna e installazione on site
- Montaggio a parete mediante staffa di supporto omologata
- Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria
- Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
- Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

aula 3
Fornitura e Installazione di n.18 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche minime: • Processore tipo intel I5-1235U o superiore • Ram 8 Gb DDR4 • Hard Disk 256 Gb SSD • Scheda Grafica Intel Iris Xe Graphics • Display 15,6" FHD • Web Cam e 2 Microfono digitali integrati • Connettività Bluetooth – Wifi 802.11ax -2 Usb-Type C 1 Hdmi

- Sistema Operativo Windows 11 Home
- Servizio di installazione e configurazione on site
- Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day,

l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita

la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che

contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.01 Carrello di ricarica avente le seguenti caratteristiche :
Il carrello dovrà essere composto da 2 ripiani con 32 postazioni per dispositivi fino a 15,6" (tablet e notebook), ventole raffredamento, Sistema di apertura e chiusura Digital Lock , Smart Charging System, input Volt 100-250V, max power 110V/230V max 16A, adattatore AC, garanzia 24 mesi on center

Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime:
• Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz).
• Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente.
• Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at).
• Piena compatibilità con il sistema di gestione già presente a scuola
• Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista .
• Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

Fornitura e Installazione di n.02 abbonamento della durata di 12 mesi ad una piattaforma che offre contenuti didattici e specificatamente :
• Categoria di contenuti:
o Scene 3d
o Lezioni
o Strumenti
o Video
• Tipologia dei contenuti:
o Biologia

o Fisica
o Geografia
o Chimica
o Storia
o Tecnologia
o Matematica
o Arti Visive
o Letteratura
La piattaforma dovrà consentire l'esecuzione dei contenuti mediante un player dedicato .
Sarà a carico della ditta l'effettuazione di un corso di formazione a supporto del personale preposto della nostra amministrazione al fine di utilizzare al meglio la piattaforma .

Fornitura e Installazione di n.18 Cuffia e Microfono Professionale avente le seguenti caratteristiche minime:

CARATTERISTICHE FISICHE
- Tipologia Cuffie con filo
- Fattore di forma Sovraurali (On-Ear Headphones)
- Microfono incorporato Sì

CARATTERISTICHE TECNICHE
- Sensibilità 120 dB
- Impedenza 38 Ohm
- Risposta in frequenza 20 - 20.000
- Ascolto musica Sì
- Controllo remoto Controllo chiamate
- Noise canceling si

CONNETTIVITÀ
- Alimentazione USB
- Tipo di porta USB-A

Plesso Nicolini

aula 1,2,3

Fornitura e installazione di n.03 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:

- Area Attiva 65”
- Tecnologia Pannello Ips
- Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
- Contrasto 1200:1
- Color Depth 10bit, 1.07Bilion colors
- Surface Treatment(Haze) Anti Glare, 7H(Mohs)
- Tempo di risposta 8ms (G to G)
- 20 Tocchi simultanei in ambiente Windows
- Casse integrate minimo 10W
- Connettività Hdmi – Usb – Wifi-Lan
- Sistema operativo Integrato Android 8.0
- Cavo Usb 5 Mt
- Cavo Hdmi 3 Mt
- Staffa di supporto omologata inclusa
- Garanzia 36 Mesi Casamadre
- Certificazione Radio Equipment Directive 2014/53/EU
- Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
- Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
- FCC (Regulatory) Class “A”
- Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:

- Consegna e installazione on site
- Montaggio a parete mediante staffa di supporto omologata
- Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria
- Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
- Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.03 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:

- Processore Intel Core I5 di 10 Th Generazione o superiore
- Ram 8 Gb DDR4
- Hard Disk tipo SSD da 256 Gb
- Connettività Ethernet 1000 Mbps -Wireless
- Sistema Operativo Windows 10 o superiore
- Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
- Installazione on site , installazione degli applicativi indicati dalla scuola

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti

dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.

L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

aula 4
Fornitura e Installazione di n.14 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche minime: • Processore tipo intel I5-1235U o superiore • Ram 8 Gb DDR4 • Hard Disk 256 Gb SSD • Scheda Grafica Intel Iris Xe Graphics • Display 15,6” FHD • Web Cam e 2 Microfono digitali integrati • Connettività Bluetooth – Wifi 802.11ax -2 Usb-Type C 1 Hdmi • Sistema Operativo Windows 11 Home • Servizio di installazione e configurazione on site Software di sicurezza avente le seguenti caratteristiche Gestione automatica delle patch Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate. Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un

ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web

fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.

• Protezione web Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing. • Exchange, SharePoint, Citrix, Linux Componenti di sicurezza dedicate disponibili per piattaforme differenti.
Fornitura e Installazione di n.01 Carrello di ricarica avente le seguenti caratteristiche : Il carrello dovrà essere composto da 2 ripiani con 32 postazioni per dispositivi fino a 15,6" (tablet e notebook), ventole raffredamento, Sistema di apertura e chiusura Digital Lock , Smart Charging System, input Volt 100-250V, max power 110V/230V max 16A, adattatore AC, garanzia 24 mesi on center
Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime: • Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz). • Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente. • Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at). • Piena compatibilità con il sistema di gestione già presente a scuola • Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista . • Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione
Fornitura e Installazione di n.02 abbonamento della durata di 12 mesi ad una piattaforma che offre contenuti didattici e specificatamente : • Categoria di contenuti: o Scene 3d o Lezioni o Strumenti o Video • Tipologia dei contenuti: o Biologia o Fisica o Geografia o Chimica o Storia o Tecnologia o Matematica o Arti Visive o Letteratura La piattaforma dovrà consentire l'esecuzione dei contenuti mediante un player dedicato . Sarà a carico della dita l'effettuazione di un corso di formazione a supporto del personale preposto della nostra amministrazione al fine di utilizzare al meglio la piattaforma .

Fornitura e Installazione di n.14 Cuffia e Microfono Professionale avente le seguenti caratteristiche minime:

CARATTERISTICHE FISICHE
- Tipologia Cuffie con filo
- Fattore di forma Sovraurali (On-Ear Headphones)
- Microfono incorporato Sì

CARATTERISTICHE TECNICHE
- Sensibilità 120 dB
- Impedenza 38 Ohm
- Risposta in frequenza 20 - 20.000
- Ascolto musica Sì
- Controllo remoto Controllo chiamate
- Noise canceling si

CONNETTIVITÀ
- Alimentazione USB
- Tipo di porta USB-A

Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:
- Area Attiva 65”
- Tecnologia Pannello Ips
- Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
- Contrasto 1200:1
- Color Depth 10bit, 1.07Bilion colors
- Surface Treatment(Haze) Anti Glare, 7H(Mohs)
- Tempo di risposta 8ms (G to G)
- 20 Tocchi simultanei in ambiente Windows
- Casse integrate minimo 10W
- Connettività Hdmi – Usb – Wifi-Lan
- Sistema operativo Integrato Android 8.0
- Cavo Usb 5 Mt
- Cavo Hdmi 3 Mt
- Staffa di supporto omologata inclusa
- Garanzia 36 Mesi Casamadre
- Certificazione Radio Equipment Directive 2014/53/EU
- Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
- Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
- FCC (Regulatory) Class “A”
- Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:
- Consegna e installazione on site
- Montaggio a parete mediante staffa di supporto omologata
- Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria
- Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in

classe.
• Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio

contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:

Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset, che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Art. 2 Servizi e certificati da fornire

Servizi e lavori minimi richiesti pena esclusione:

1) Trasporto, Montaggio, installazione e collaudo a carico della ditta di tutti i beni forniti secondo le esigenze della scuola.
2) L'assistenza tecnica in garanzia sui beni forniti presso l'Istituto (On Site) da erogarsi nei normali orari di ufficio, che dovrà essere erogata, a partire dalla data del collaudo effettuato con esito positivo, per un periodo minimo di 24 mesi, con intervento entro almeno due giorni lavorativi.
3) Il ritiro e lo smaltimento degli imballaggi.
4) Per la tinteggiatura (se compresa nel capitolato) è necessaria la rispondenza mediante una delle opzioni previste al paragrafo 2.4.2.11 del D.M. 11/10/2017 del M.A.T.T.M.:
   - Marchio Ecolabel UE o equivalente;
   - Una dichiarazione ambientale di tipo III, conforme alla norma UNI EN 15804 ed alla norma ISO 14025.
5) Per la fornitura degli arredi la ditta dovrà fornire il certificato CAM DM 23/06/2022.
6) Per gli adeguamenti dell'impianto elettrico la ditta dovrà fornire la certificazione 37/08 con specifica dei materiali utilizzati.

7) Per la fornitura dei prodotti elettronici (tablet, PC, notebook etc) la ditta deve fornire attestazione di rispetto DNSH di cui all'art. 17 del Regolamento UE 2020/852

Art. 3 Indicazioni per l'offerta

INDICARE MARCA e MODELLO dei prodotti offerti ed allegare documentazione tecnica.

Si precisa che non sono accettati prodotti di importazione che non siano a diffusione internazionale e che non abbiano una garanzia internazionale del produttore, ciò a tutela della stazione appaltante che deve avere garantita la riparazione del prodotto anche in caso di fallimento del fornitore o del distributore nazionale. Si accettano beni prodotti e garantiti direttamente da produttore nazionale solo se aventi le certificazioni previste nel disciplinare; in tal caso inoltre la garanzia del produttore deve prevedere la sostituzione del bene con intervento on-site, ossia presso la stazione appaltante.
Sarà ovviamente sempre e comunque l'operatore economico a rispondere nei riguardi dell'istituzione scolastica nel periodo di garanzia.
Ai fini dell'ammissibilità della spesa, le attrezzature acquistate dovranno rispettare il principio di non arrecare danno significativo agli obiettivi ambientali ai sensi dell'articolo 17 del regolamento (UE) 2020/852 (DNSH). A tal fine è possibile verificare il rispetto di tale principio, applicando i requisiti previsti dal Documento di Lavoro dei Servizi della Commissione "Criteri in materia di appalti pubblici verdi dell'UE per i computer, i monitor, i tablet e gli smart- phone", SWD(2021) 57 final del 5.3.2021, nel caso di acquisto di attrezzature rientranti in tali tipologie saranno ritenute conformi se in possesso delle sottoelencate etichette ambientali :

Etichetta ambientale di tipo I, secondo la UNI EN ISO 14024, ad esempio TCO Certified, EPEAT 2018, Blue Angel, TÜV Green Product Mark o di etichetta equivalente)

In caso di assenza di un etichetta ambientale di tipo I : Etichetta EPA ENERGY STAR o in alternativa dichiarazione del produttore che attesti che il consumo tipico di energia elettrica (Etec), calcolato per ogni dispositivo offerto, non superi il TEC massimo necessario (Etec-max) in linea con quanto descritto nell'Allegato III dei criteri GPP UE

Per condizioni aggiuntive consultare la Scheda 3 - Acquisto, Leasing e Noleggio di computer e apparecchiature elettriche ed elettroniche (Guida Operativa Edizione aggiornata allegata alla circolare RGS n. 33 del 13 ottobre 2022)

Le attrezzature acquistate dovranno rispettare i CRITERI AMBIENTALI MINIMI PER LA FORNITURA DI ARREDI PER INTERNI come da DECRETO del 23 giugno 2022 del MINISTERO DELLA TRANSIZIONE ECOLOGICA (Criteri ambientali minimi per l'affidamento del servizio di fornitura, noleggio ed estensione della vita utile di arredi per interni). **L'operatore economico presenterà le informazioni richieste secondo quanto indicato in appendice "A" del medesimo decreto.**

Art. 4 Schede tecniche

Vanno necessariamente allegate le schede tecniche del materiale, pena esclusione, fornite dal produttore e non da un rivenditore, e devono essere presenti le specifiche richieste, e/o equivalenti e/o superiori.

Art. 5 Fornitura unitaria ed omnicomprensiva

I beni dovranno essere completamente installati e configurati, comprese le funzionalità di ottimizzazione, secondo la formula "chiavi in mano". Nessun altro onere potrà essere chiesto all'Istituto e l'operatore economico presentando l'offerta accetta tutti gli oneri anche imprevisti ed

occulti. E' interesse dell'operatore economico, a sua scelta, effettuare sopralluogo, e comunque non potrà essere addebitato nulla alla stazione appaltante per imprevisti derivanti dalla mancata conoscenza dei luoghi. Non sono ammesse varianti in corso d'opera se non concordate con la stazione appaltante.

Allegato A :
Contiene una planimetria che offre dei suggerimenti indicativi per il posizionamento degli arredi ed apparati e delle postazioni di lavoro. In fase di esecuzione la ditta dovrà interfacciarsi con il progettista per eventuali variazioni.

Il Dirigente Scolastico
Ludovico Silvestri
Documento firmato digitalmente

ALLEGATO A

UBICAZIONE AULE/AMBIENTIOGGETTODI INTERVENTO E DISPOSIZIONE ARREDI

SCUOLA SECONDARIA DI I GRADO
FAUSTINI-FRANK-NICOLINI
VIA ALBERONI, 49, 29100 PIACENZA

PLESSO ALBERONI VIA ALBERONI, 49

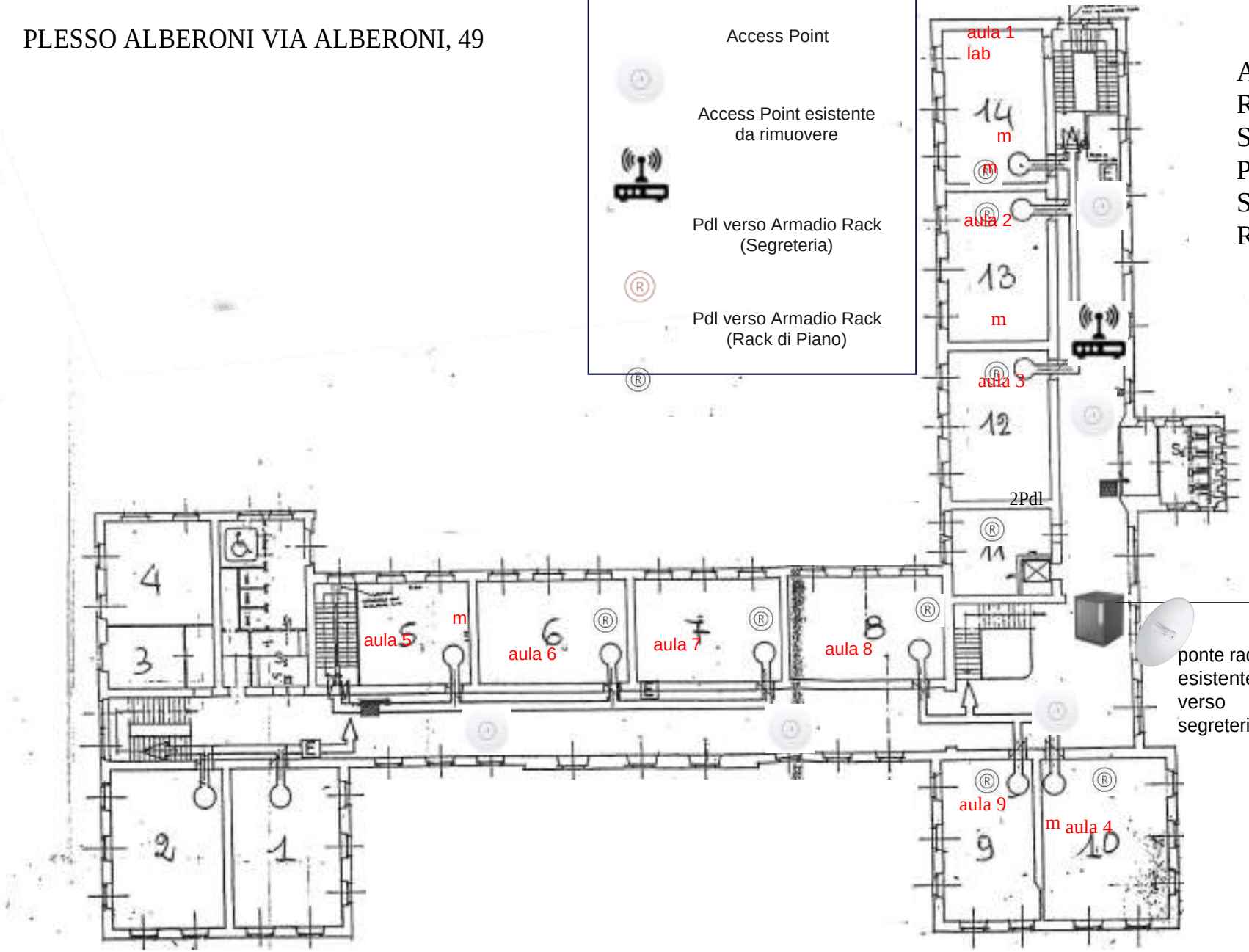
LEGGENDA

Access Point

Access Point esistente da rimuovere

Pdl verso Armadio Rack (Segreteria)

Pdl verso Armadio Rack (Rack di Piano)



Armadio Rack Centro Stella Presente Da Sostituire con R1 (rack 22U)

LEPIDA SPA
IP 86.104.229.200

IC FAUSTINI-FRANK-NICOLINI
VIA ALBERONI, 49, 29100 PIACENZA

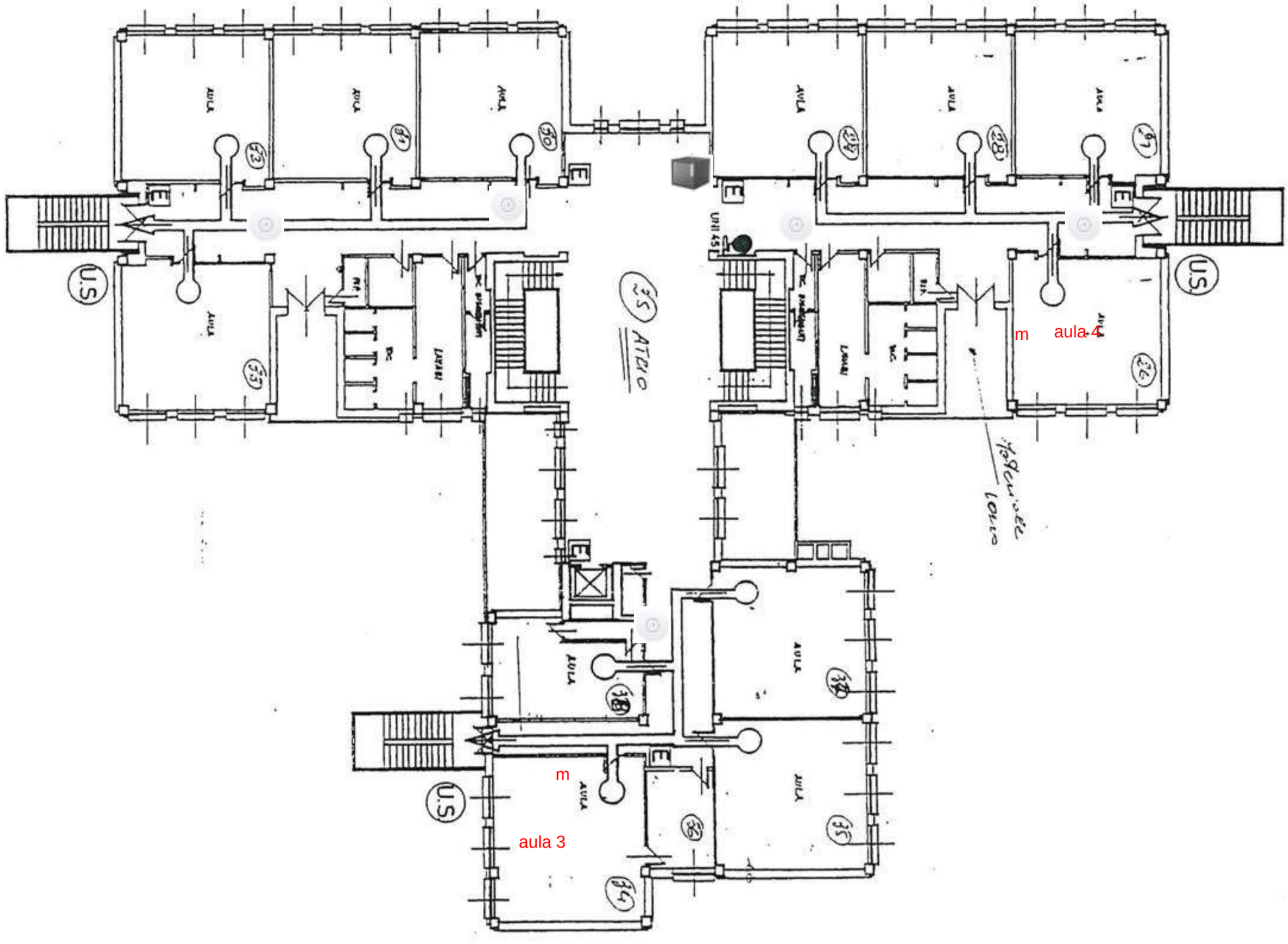
Plesso Anna Frank Piano Primo

ARMADIO RACK
PRESENTE DA
AGGIORNARE
R4

▲

LEGGENDA

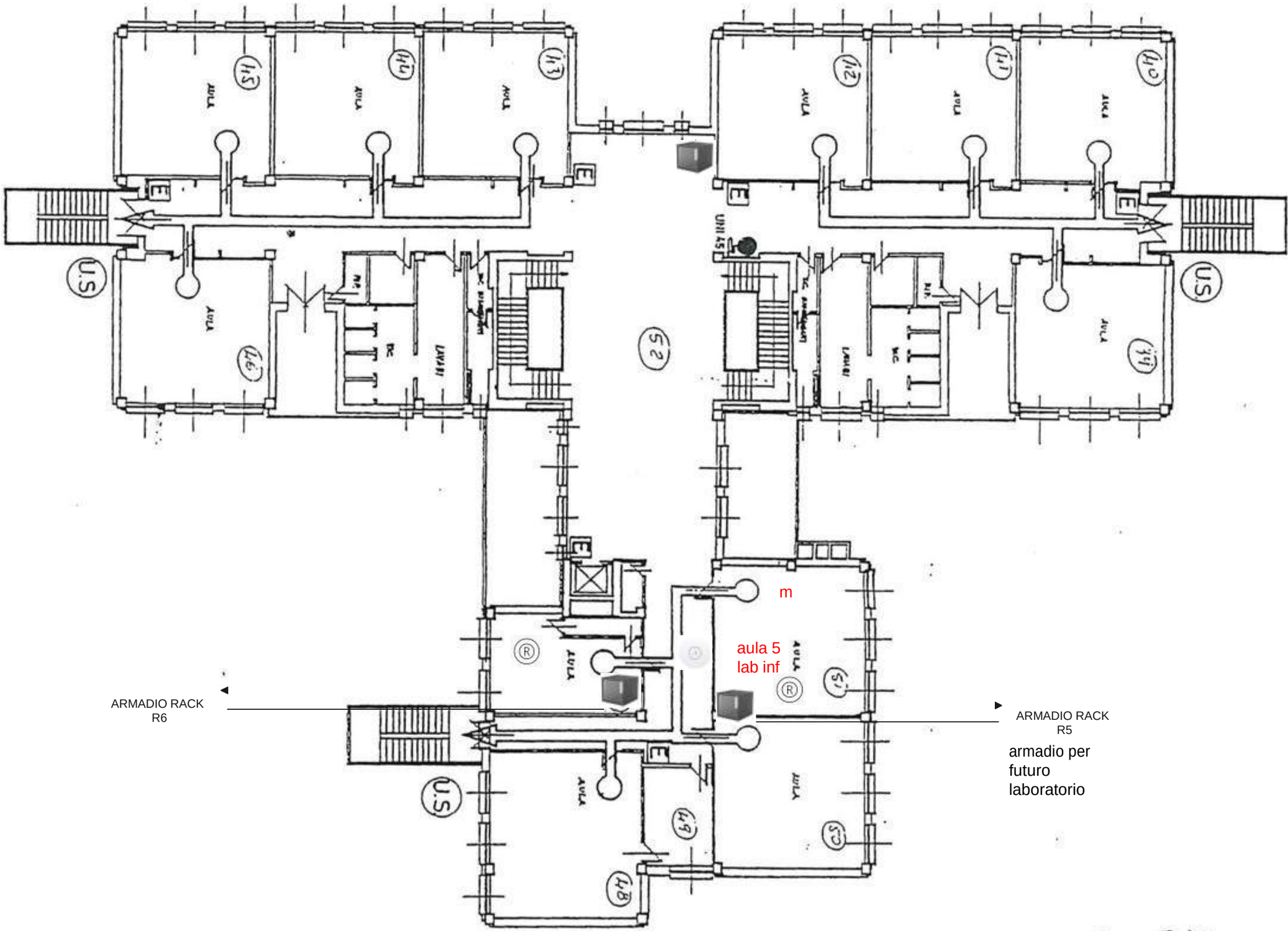
- Access Point
- Access Point esistente da rimuovere
- Pdl verso Armadio Rack (Segreteria)
- Pdl verso Armadio Rack (Rack di Piano)



IC FAUSTINI-FRANK-NICOLINI
VIA ALBERONI, 49, 29100 PIACENZA

Plesso Anna Frank Piano Secondo

ARMADIO RACK
PRESENTE DA
AGGIORNARE
R7

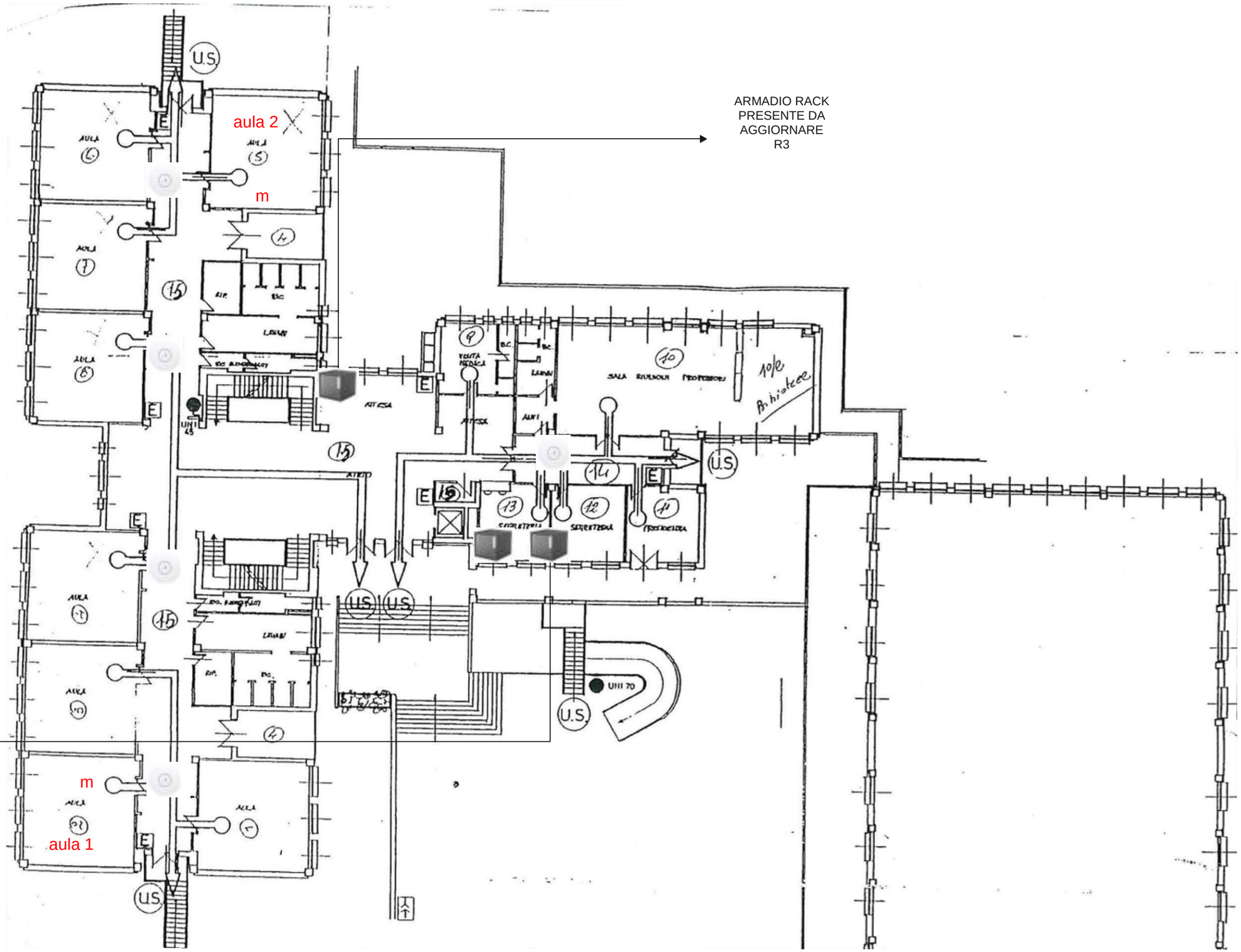


IC FAUSTINI-FRANK-NICOLINI
VIA ALBERONI, 49, 29100 PIACENZA

Plesso Anna Frank Piano Rialzato

LEGGENDA

- Access Point
- Access Point esistente da rimuovere
- Pdl verso Armadio Rack (Segreteria)
- Pdl verso Armadio Rack (Rack di Piano)

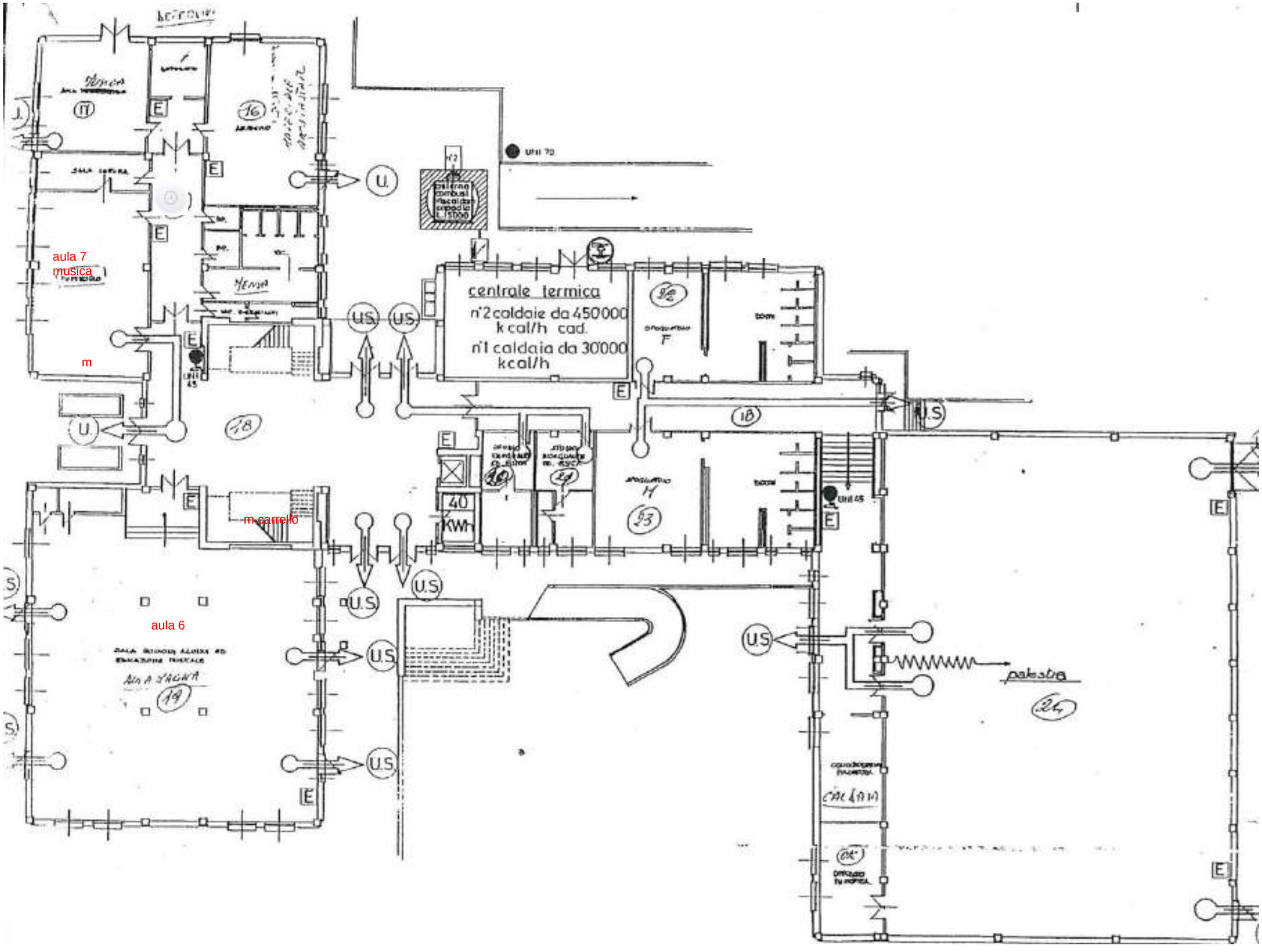


IC FAUSTINI-FRANK-NICOLINI
VIA ALBERONI, 49, 29100 PIACENZA

Plesso Anna Frank Piano Seminterrato

LEGGENDA

- Access Point
- Access Point esistente da rimuovere
- Pdl verso Armadio Rack (Segreteria)
- Pdl verso Armadio Rack (Rack di Piano)



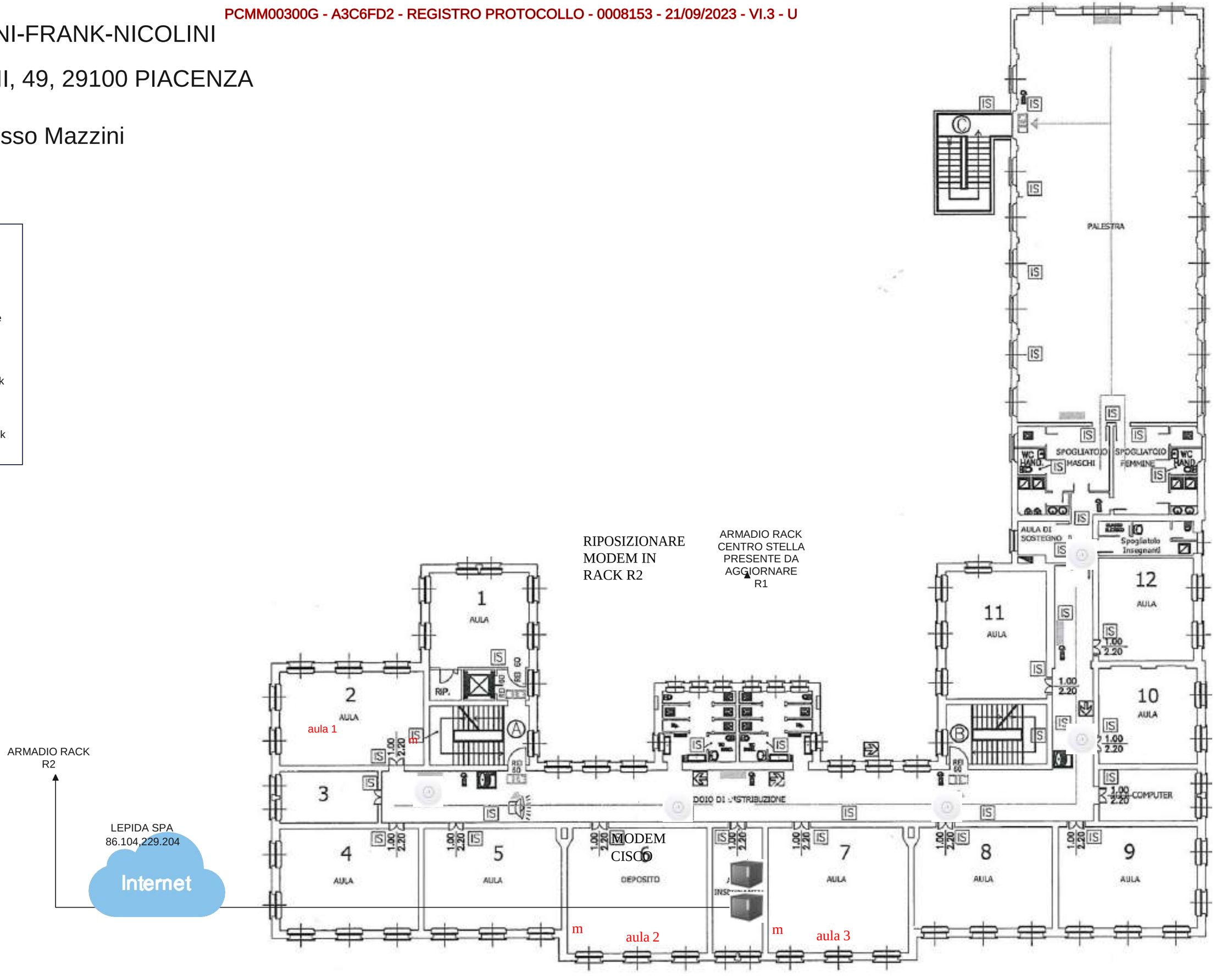
IC FAUSTINI-FRANK-NICOLINI

VIA ALBERONI, 49, 29100 PIACENZA

Plesso Mazzini

LEGGENDA

- Access Point
- Access Point esistente da rimuovere
- Pdl verso Armadio Rack (Segreteria)
- Pdl verso Armadio Rack (Rack di Piano)



IC FAUSTINI-FRANK-NICOLINI
VIA ALBERONI, 49, 29100 PIACENZA

Plesso Nicolini - Piano Primo e Ammezzato

LEGGENDA

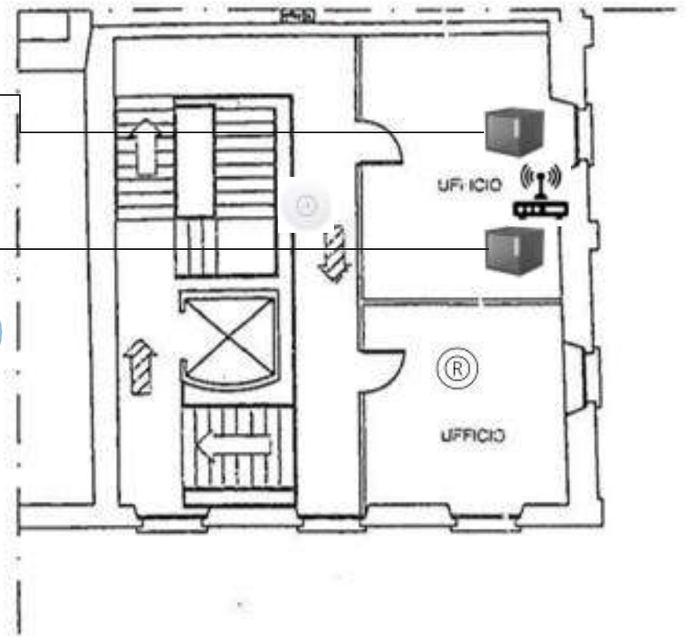
- Access Point
- Access Point esistente da rimuovere
- Pdl verso Armadio Rack (Segreteria)
- Pdl verso Armadio Rack (Rack di Piano)

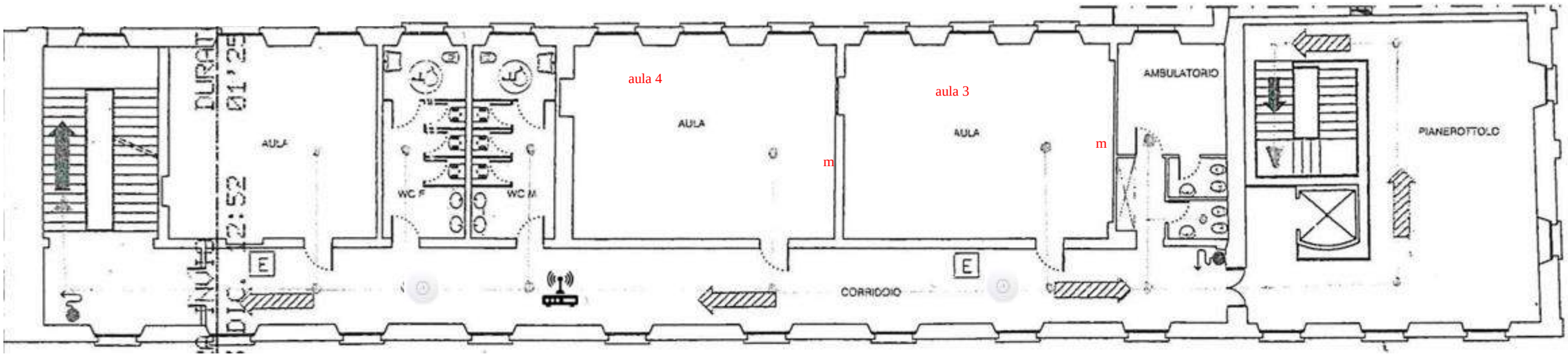
ARMADIO RACK PRESENTE DA AGGIORNARE R2 (AMMEZZATO)

ARMADIO RACK CENTRO STELLA PRESENTE DA AGGIORNARE R1 (AMMEZZATO)

Internet

LEPIDA SPA
IP 86.104.229.203 79/80 Mbps





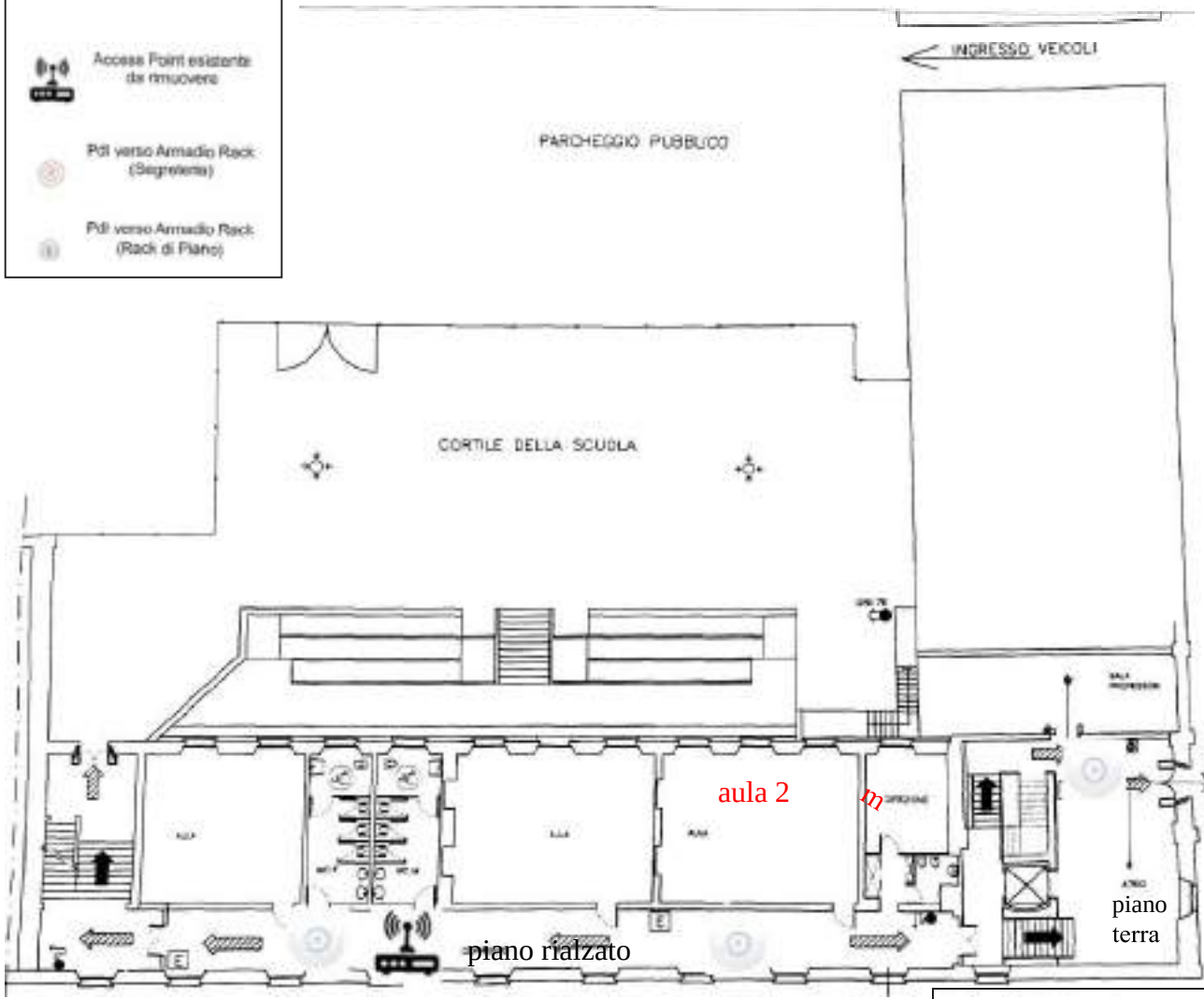
LEGGENDA

Access Point

Access Point esistente da rimuovere

PdI verso Armadio Rack (Segreteria)

PdI verso Armadio Rack (Rack di Piano)



viA S. *VINGEnZO*

Legenda

SGAtA DI SIGUPEZZ4 PftOTSTTA

PORTA TAGLiAFUOCO REI 60

LUOGO SICURO

PERCORSO DI USCITA VERSO L'ALTO

PERCORSO DI USCITA ORIZZONTALE

PERCORSO DI USCITA VERSO IL BASSO

ESTINTORE PORTATILE A POLVERE

IDRANTE A MURO ANTINCENDIO ON 4' CON TUBAZIONE FLESSIBILE

IDRANTE UNI70

SCUOLA MEDIA STATALE "G.NICOLINI"

PIANO DI EVACUAZIONE

PIANO TERRA E RIALZATO

DATA:

SCALA: 1:200

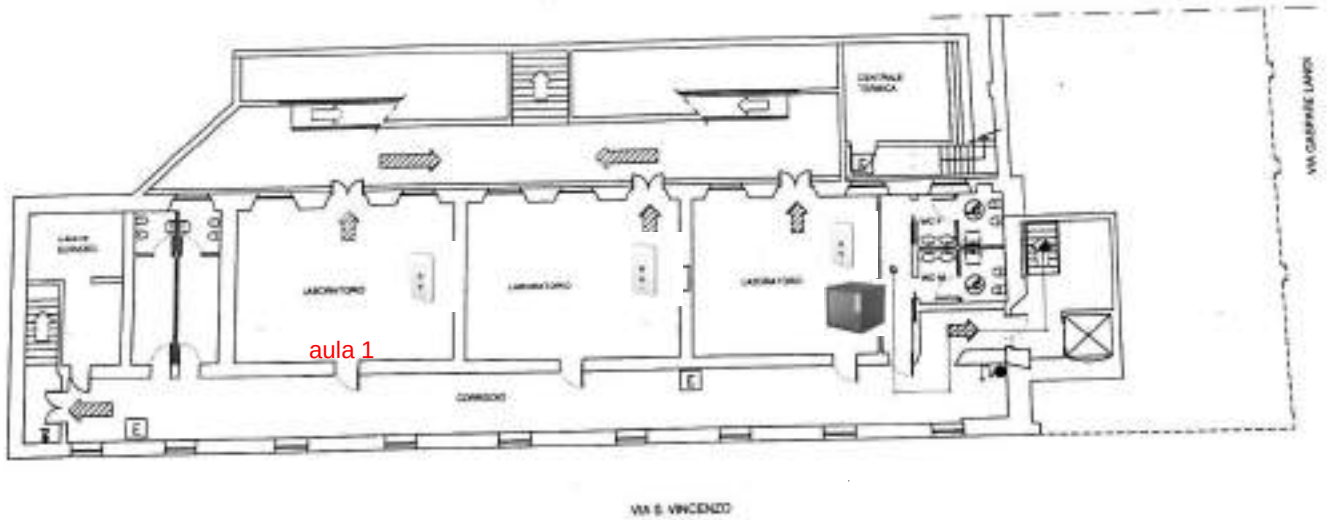
ITAV :2

LEGGENDA

Access Point

Access Point esistente
da rimuovere

Pdl verso Armadio Rack
(Rack di Piano)



LEGENDA

- SCALA DI SICUREZZA PROTETTA
- PORTA TAGLIAFUOCO REI 60
- LUOGO SICURO
- PERCORSO DI USCITA VERSO L'ALTO
- PERCORSO DI USCITA ORIZZONTALE
- PERCORSO DI USCITA VERSO IL BASSO
- E — ESTINTORE PORTATILE A POLVERE
- IDRANTE A MURO ANTINCENDIO ON 45 CON TUBAZIONE FLESSIBILE
- IDRANTE UNI70

ARMADIO RACK
PRESENTE DA
SOSTITUIRE
R3

SCUOLA MEDIA STATALE "G.NICOLINI"

PIANO DI EVACUAZIONE

PIANO INTERRATO

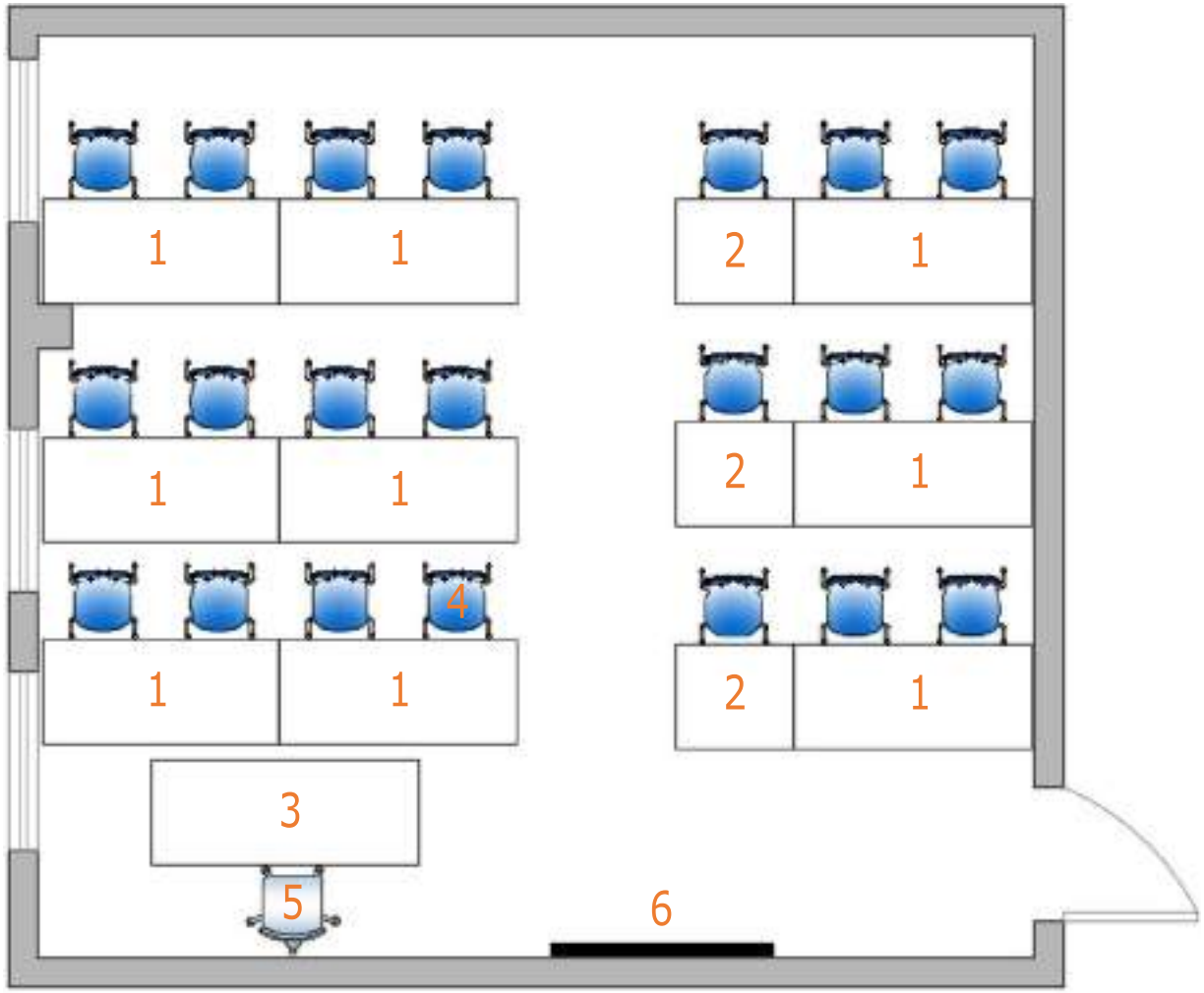
DATA:

SCALA: 1:200

TAV :

Plesso Anna Frank

Secondo Piano – Aula 5 Labor



1. Tavolo 160x70

2. Tavolo 80x70

3. Tavolo 180x70

4. Sedia fissa

5. Poltrona docente

6. Monitor 75"