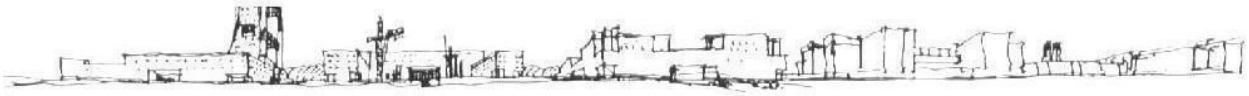
Licenze software, servizi di manutenzione dei Next-Generation Firewall di Ateneo e fornitura di prodotti hardware/software

Relazione Generale Tecnico-illustrativa

MILANO, maggio 2025

Responsabile Unico del Progetto
Dott. Piero Ferraresso
(nomina Determina Dirigenziale Rep. 2615/2025 Prot. 0191621 del 07/05/2025)
[f.to digitalmente ex art. 24 D.lgs. 82/05]



Sommario

1. AMMINISTRAZIONE CONTRAENTE 3
2. OGGETTO DELL'APPALTO 3
3. REQUISITI DI IDONEITÀ PROFESSIONALE 8
4. REQUISITI DI PARTECIPAZIONE E/O CONDIZIONI DI ESECUZIONE 8
5. PROCEDURA DI GARA **8**

1. AMMINISTRAZIONE CONTRAENTE

L'amministrazione contraente è l'Università degli Studi di Milano–Bicocca, che agisce attraverso l'Area Infrastrutture ed Approvvigionamenti, Settore Appalti Beni e Servizi , per le esigenze Area Sistemi Informativi

L'Ateneo, che si articola su 28 edifici, per oltre 350.000 metri quadrati, sito per la gran parte all'interno del Comune di Milano, municipio Zona 9, è divenuto ormai un cardine all'interno del territorio metropolitano, quale centro realizzatore di eventi culturali, progetti formativi e di ricerca in qualità di partner principale del "Distretto Bicocca", cui partecipano quattordici tra Enti, aziende e fondazioni del territorio.

Il Campus Bicocca.

2. OGGETTO DELL'APPALTO

L'Ateneo, al fine di rispondere alle esigenze di miglioramento della sicurezza informatica nelle Pubbliche Amministrazioni come richiesto dalla direttiva NIS - Network and Information Security 2 (recepimento della direttiva UE 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, e del decreto legislativo del Consiglio dei Ministri del 4 settembre 2024, n. 138) e dalle "Misure minime di sicurezza ICT" (parte integrante delle "Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni" e in seguito all'attuazione della "Direttiva del

Presidente del Consiglio dei Ministri 1 agosto 2015") emanate da AgID - Agenzia per l'Italia digitale, ha la necessità di acquistare servizi di manutenzione e le licenze software dei *Next-Generation Firewall* a protezione della rete di Ateneo.

I servizi di manutenzione e le licenze software dei N*ext-Generation Firewall* di marca Palo Alto Networks attualmente presenti a protezione perimetrale di Ateneo (cluster di due PAN-PA-5410-AC acquistati, nell'anno 2022, con gara d'appalto CIG. 9303973966 per 36 mesi), a protezione dell'infrastruttura critica della rete data center (cluster di due PAN-PA-5220-AC acquistati, nell'anno 2017, con gara d'appalto CIG. 7022557D5A) e a protezione dell'infrastruttura dei laboratori virtuali LibaaS di Ateneo (cluster di due PAN-PA-5220-AC acquistati, nell'anno 2019, con gara d'appalto CIG. 7980995D69), sono in scadenza il giorno 3 settembre dell'anno in corso.

In dettaglio, per il cluster di due N*ext-Generation Firewall* PAN-PA-5410-AC a protezione perimetrale di Ateneo, le licenze sono:

. *Advanced Threat Prevention* per la protezione della rete dalle minacce avanzate, identificando e analizzando il traffico (applicazioni, utenti e contenuti) su tutte le porte e protocolli;

a. *Advanced DNS Security* per la rilevazione ed il blocco in modo automatico degli attacchi DNS;

b. *Wildfire* per il rilevamento e la prevenzione del malware zero-day utilizzando una combinazione di sandboxing malware e rilevamento basato su firma, estendendo le funzionalità dei *Next-Generation Firewall* per identificare e bloccare malware sconosciuto;

c. *GlobalProtect* per l'utilizzo degli stessi *Next-Generation Firewall* perimetrali come terminatori VPN fino al massimo di utenze contemporanee gestibili dal hardware;

oltre al :

e. del supporto tecnico *Premium* di Palo Alto Networks per 3 (tre) anni per il cluster di due N*ext-Generation Firewall* descritti ai punti precedenti.

Considerata l'importanza di proteggere l'infrastruttura della rete perimetrale di Ateneo, si rende necessario l'ampliamento dei servizi basati su AI - Artificial Intelligence (che consente di proteggere i servizi ed i dati dalle vulnerabilità e dalle minacce più evolute automatizzando i processi e riducendo i tempi di gestione degli incidenti di sicurezza) attraverso l'upgrade della licenza *Wildfire* precedentemente definita (come descritta al punto *c*) sugli apparati *Next-Generation Firewall* perimetrali (PAN-PA-5410-AC), come segue:

f. *Advanced Wildfire* per il rilevamento e la prevenzione del malware zero-day utilizzando una combinazione di sandboxing malware, rilevamento basato su firma e AI - Artificial Intelligence, estendendo le funzionalità dei *Next-Generation Firewall* per identificare e bloccare malware sconosciuto.

Inoltre si rende necessario l'acquisto delle ulteriori licenze Palo Alto Networks:

g. *Advanced URL Filtering* per la protezione della rete e degli utenti dalle minacce basate sul web, fornendo un controllo granulare sull'accesso degli utenti e sull'interazione con i contenuti su Internet, categorizzando e bloccando gli URL dannosi in tempo reale;

. *Advanced SD-WAN* (Software-Defined Wide Area Networking) per la gestione, il monitoraggio e l'ottimizzazione delle prestazioni delle reti WAN (Wide Area Networks), attraverso la connessione in modo sicuro di utenti, applicazioni e dati in varie sedi.

Alla luce dell'adeguamento tecnologico della rete interna LAN (Local Area Network) attraverso il potenziamento della infrastruttura di comunicazione con connettività fino a 100Gb e della data di fine vendita (EOS - End of Sale) settata al 31 agosto 2023 degli apparati *Next-Generation Firewall* (cluster di PAN-PA-5220-AC), si rende necessario l'acquisto di:

i. n. 2 (due) nuovi apparati *Next-Generation Firewall* perimetrali (PAN-PA-5410-AC di Palo Alto Networks) di fascia alta a elevate prestazioni per il monitoraggio del traffico fino al livello applicazione dello stack TCP/IP, a protezione dell'infrastruttura critica della rete data center, in sostituzione del cluster di due PAN-PA-5220-AC acquistati nell'anno 2017;

- del supporto tecnico *Premium* di Palo Alto Networks per 3 (tre) anni per i N*ext-Generation Firewall* PAN-PA-5410-AC descritti al punto precedente, già presente nel cluster di N*ext-Generation Firewall* PAN-PA-5220-AC;
- della licenza *Advanced Threat Prevention* per la protezione della rete dalle minacce avanzate, identificando e analizzando il traffico (applicazioni, utenti e contenuti) su tutte le porte e protocolli, già presente nel cluster di N*ext-Generation Firewall* PAN-PA-5220-AC;

Inoltre, alla luce della data di fine vendita (EOS - End of Sale) settata al 31 agosto 2023 anche degli apparati *Next-Generation Firewall* (cluster di PAN-PA-5220-AC) a protezione dell'infrastruttura dei laboratori virtuali LibaaS di Ateneo, si rende necessario l'acquisto di:

l. n. 2 (due) nuovi apparati *Next-Generation Firewall* perimetrali (PAN-PA-5410-AC di Palo Alto Networks) di fascia alta a elevate prestazioni per il monitoraggio del traffico fino al livello applicazione dello stack TCP/IP, in sostituzione del cluster di due PAN-PA-5220-AC acquistati nell'anno 2019;
- del supporto tecnico *Standard* di Palo Alto Networks per 3 (tre) anni per i N*ext-Generation Firewall* PAN-PA-5410-AC descritti al punto precedente;
- del *Lab bundle subscription* contenenti le licenze *Advanced Threat Prevention, Advanced DNS, Advanced URL filtering, GlobalProtect, Advanced WildFire* e *Advanced SD-WAN*, per uniformità con le licenze presenti nel cluster di due *Next-Generation Firewall* (PAN-PA-5410-AC) installati a protezione perimetrale della rete di Ateneo.

Per la compliance con la normativa NIS - Network and Information Security 2 riguardo all'ambito IoT, è inoltre necessario acquistare:

o. la licenza *Enterprise IoT Security*, utile per scoprire e mantenere dinamicamente un inventario in tempo reale dei dispositivi IoT, eseguendo l'analisi delle vulnerabilità, rilevando anomalie nel comportamento dei dispositivi e valutando i rischi.

Per continuare il monitoraggio e la risposta agli incidenti informatici utilizzando i dati degli endpoint, si rende necessario aggiornare i servizi cloud Cortex già acquistati di:

p. 4.300 licenze Palo Alto Networks *Cortex XDR Pro* per la protezione degli endpoints.

Inoltre, per semplificare il triage e l'analisi forense, raccogliendo tutti gli artefatti e visualizzandoli in una console forense intuitiva, semplificando le indagini in modo da poter tracciare ogni mossa di un avversario e contenere rapidamente le minacce da un unico posto senza dover passare da uno strumento di sicurezza all'altro, è necessario l'acquisto di:

q. 430 licenze Palo Alto Networks *Annual Forensics add-on for 1 Cortex XDR endpoint*.

Inoltre per migliorare l'integrazione tra dispositivi presenti nella rete, negli endpoint e nel cloud, ottimizzando l'analisi e la risposta agli incidenti informatici, si rende necessario aggiornare:

r. 200GB/mese di spazio storage per la piattaforma di gestione integrata, basata su AI - Artificial Intelligence, erogata in modalità *software as a service - SaaS* (*Cortex XDR* di Palo Alto Networks) su cui confluiscono gli eventi di sicurezza di tutti i dispositivi *Next-Generation Firewall* a protezione dell'infrastruttura della rete di Ateneo per la prevenzione e gestione degli incidenti informatici.

Considerata l'importanza di monitorare le applicazioni cloud native e proteggere l'infrastruttura critica della rete cloud, si rende necessario l'acquisto di:

- 200 workload per *Palo Alto Cortex Cloud* (precedentemente denominata *Prisma Cloud*), piattaforma erogata in modalità *software as a service - SaaS* per la protezione dell'infrastruttura, delle applicazioni, dei dati e delle autorizzazioni nei cloud, con particolare attenzione ai workload e alla sicurezza dei container.

La scelta dei medesimi è giustificata, se non obbligata, in quanto economicamente vantaggiosa in termini di Total Cost of Ownership (TCO) e per il loro naturale inserimento nel complesso di integrazioni e automatismi realizzato nel tempo come dettagliato nei punti seguenti:

1) la rete di Ateneo è già equipaggiata con un'infrastruttura di sicurezza *Next-Generation Firewall* della stessa marca e tecnologia Palo Alto Networks e l'acquisto dei firewall in oggetto si configura come una semplice estensione della tecnologia già testata in produzione;

2) per detto motivo l'acquisto degli apparati in oggetto non comporterebbe ulteriori costi in termini di tempo e risorse per la valutazione della loro integrazione nell'infrastruttura e salvaguarderebbe gli investimenti effettuati nei servizi software e di monitoraggio sviluppati negli anni;

3) si rende possibile l'analisi ed identificazione di eventuali incidenti informatici da un'unica piattaforma di gestione, attraverso la correlazione in modo nativo di tutti i dati provenienti da sorgenti diverse (rete, endpoints e cloud), migliorando la produttività e semplificando l'identificazione, investigazione e neutralizzazione delle minacce;

4) l'acquisto della licenza *Advanced Wildfire* permette di ampliare il rilevamento e la prevenzione del malware zero-day utilizzando l'AI - Artificial Intelligence oltre che una combinazione di sandboxing malware e rilevamento basato su firma;

5) l'acquisto delle licenze *Advanced URL Filtering* (utile per la protezione della rete e degli utenti dalle minacce basate sul web) e *Advanced SD-WAN* (utile per la gestione, il monitoraggio e l'ottimizzazione delle prestazioni delle reti WAN - Wide Area Networks), sono da considerarsi a costo zero in quanto comprese nel bundle commerciale con tutte le altre licenze installate sugli apparati *Next-Generation Firewall* (PAN-PA-5410-AC) a protezione perimetrale della rete di Ateneo.

Inoltre il personale interno è già in possesso degli skill ed expertising necessari per gestire in autonomia tutta l'infrastruttura senza dover ricorrere a corsi di formazione o a risorse esterne; tale determina si configura come una semplice estensione della tecnologia già testata in produzione e non comporta ulteriori costi in termini di tempo e risorse per la valutazione della loro integrazione nell'infrastruttura e salvaguarda gli investimenti effettuati nei servizi software e di monitoraggio sviluppati negli anni.

L'indagine effettuata tra i recenti recenti accordi quadro "Cybersecurity" e "Cybersecurity 2" (accordo quadro con più operatori economici per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni), ha evidenziato l'assenza di modelli specifici della famiglia PA-5400 tra i prodotti Palo Alto Networks offerti.

Per dette motivazioni si giustifica ampiamente, soprattutto in termini di Total Cost of Ownership (TCO), il ricorso a una procedura di gara per i servizi di manutenzione e delle licenze software dei *Next-Generation Firewall* di Ateneo di marca Palo Alto Networks,

Si precisa che la multinazionale americana detiene i diritti di esclusiva e di privativa industriale sui software e che per i servizi di manutenzione e assistenza specialistica si avvale di una rete di fornitori certificati che sono gli unici che possono commercializzare o erogare tale servizio secondo livelli e prezzi presenti a listino ufficiale.

Inoltre, per questa tipologia di apparati, firewall ad alte prestazioni di categoria "enterprise class" ad elevato throughput (20 Gbps), i produttori, per offrire aggiornamenti e rilasci delle release software, richiedono il pagamento di tariffe per la registrazione dei particolari codici seriali delle componenti hardware e software nel proprio programma di assistenza. Questo modello di servizio prevede, per le parti regolarmente registrate, la presenza a listino del servizio di manutenzione erogato direttamente dal produttore e, nel caso non venissero pagate le tariffe previste si avrebbe la violazione dei diritti di proprietà intellettuale dei sistemi hardware e software e la violazione dei termini contrattuali.

L'Ateneo, per motivi di garanzia e efficacia del servizio, nonché per la criticità degli apparati nell'economia del sistema informatico e per la complessità delle tematiche oggetto del servizio, necessita che esso sia erogato dalla struttura di assistenza (Technical Assistance Center - TAC) del produttore;

Palo Alto Networks è un produttore all'avanguardia nel mondo della sicurezza IT, è stato il fondatore della tecnologia *Next Generation Firewall*, ed è tuttora identificato come leader di mercato dai principali analisti mondiali. A conferma si riporta di seguito il Magic Quadrant di Gartner, il principale analista nel comparto dell'Information Technology, che individua Palo Alto Networks come il leader di mercato assoluto per le tecnologie di *Enterprise Network Firewall*:

Figure 1: Magic Quadrant for Endpoint Protection Platforms

Gartner

Che nella fase di ricerca di mercato per la corretta valutazione della congruità degli investimenti da effettuare a tutela di codesta Amministrazione si è addivenuti alla definizione della base d'asta corrispondente a una scontistica sui prezzi di listino del 73%. Questo livello di sconto si ritiene raggiungibile in base al ruolo di cliente strategico (nonché uno dei primi in Italia ad avere optato per questa tecnologia all'avanguardia) che codesto Ateneo rappresenta per Palo Alto Networks e non si discosta dal livello di scontistica già ottenuto nelle precedenti esperienze.

In sintesi si ritiene che l'ottenimento di detto livello di scontistica, per altro molto aggressivo, porterebbe a una valutazione positiva di congruità dell'offerta. In funzione di questo si stima una spesa triennale massima di circa € 750.000,00 IVA esclusa;

***

3. REQUISITI DI IDONEITÀ PROFESSIONALE

a) Iscrizione nel Registro delle Imprese oppure nell'Albo delle Imprese artigiane per attività pertinenti con quelle oggetto della presente procedura di gara.

4. REQUISITI DI PARTECIPAZIONE E/O CONDIZIONI DI ESECUZIONE

Ai sensi dell'art. 113 del D.Lgs. 36/2023 per l'esecuzione del servizio oggetto del presente appalto, ai sensi dell'articolo 113 del Codice, è richiesto che l'Aggiudicatario sia partner certificato PAN a livello Diamond Innovator o superiore. La certificazione dovrà essere posseduta per tutta la durata del contratto.

***

5. PROCEDURA DI GARA

Si procederà con procedura aperta ai sensi dell'art. 71 del D.lgs. 36/2023, con il criterio del prezzo più basso, ai sensi dell'art. 108, c. 3 del D.Lgs.36/2023 in quanto trattasi di servizi standardizzati