



SERVIZIO DI MANUTENZIONE E LICENZE SOFTWARE DEI *NEXT-GENERATION FIREWALL* DI
ATENEO E AMPLIAMENTO DEI SERVIZI DI SICUREZZA CLOUD-NATIVE DI MARCA PALO
ALTO NETWORKS

Doc. 1 - Relazione tecnico-illustrativa

Codice Identificativo Gara – CIG 9303973966

**Il Dirigente e Responsabile Unico del Procedimento
(Dott. Stefano Moroni)**

[f.to digitalmente ex art. 24 D.lgs. 82/05]

MILANO, GIUGNO 2022

Sommario

1. L'AMMINISTRAZIONE CONTRAENTE	3
2. ESIGENZE DELL'ATENEO E SERVIZI RICHIESTI	4





3. LA QUALIFICAZIONE DELL'APPALTATORE	7
4. LA DURATA DEL CONTRATTO	7
5. LA PROCEDURA DI GARA	7





1. L'AMMINISTRAZIONE CONTRAENTE

L'amministrazione contraente è l'Università degli Studi di Milano – Bicocca.

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. ESIGENZE DELL'ATENEO E SERVIZI RICHIESTI

L'Ateneo, al fine di rispondere alle esigenze di miglioramento della sicurezza informatica nelle pubbliche amministrazioni, come richiesto delle "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 rinnovare i servizi di manutenzione e le licenze software dei *Next-Generation Firewall* a protezione della rete data center e perimetrale di Ateneo.

I servizi di manutenzione e le licenze software dei *Next-Generation Firewall* di marca Palo Alto Networks attualmente presenti 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 per 36 mesi) e a protezione perimetrale di Ateneo (cluster di due PAN-PA-5220-AC acquistati, nell'anno 2019, con gara d'appalto CIG. 7980995D69 per 36 mesi), sono in scadenza il giorno 3 settembre dell'anno in corso.

In dettaglio, i servizi da rinnovare sono:

- a. il supporto tecnico *Premium* per la piattaforma di gestione centralizzata di policy e dispositivi *Panorama* di Palo Alto Networks;
- b. il supporto tecnico *Premium* di Palo Alto Networks per tutti i *Next-Generation Firewall* PAN-PA-5220-AC presenti in determina.

Inoltre le licenze da rinnovare sono:

- c. *GlobalProtect* (per un totale di n. 2 licenze) per l'utilizzo degli stessi *Next-Generation Firewall* perimetrali come terminatori VPN fino al massimo di utenze contemporanee gestibili dal hardware;
- d. *Wildfire* (per un totale di n. 2 licenze) 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;
- e. *Threat Prevention* (per un totale di n. 4 licenze) per la protezione della rete dalle minacce avanzate, identificando e analizzando il traffico (applicazioni, utenti e contenuti) su tutte le porte e protocolli.

Alla luce dell'adeguamento tecnologico della rete GARR (la Rete Italiana dell'Università e della Ricerca) attraverso il potenziamento della infrastruttura di comunicazione con connettività fino a 100Gb si richiede l'acquisto di:

- f. 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, della rete perimetrale di Ateneo;
- g. il supporto tecnico *Premium* di Palo Alto Networks per 3 (tre) anni per i *Next-Generation Firewall* PAN-PA-5410-AC descritti al punto precedente.

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 la migrazione delle licenze precedentemente definite (come descritte ai punti *c*, *d*) sui 2 nuovi apparati *Next-Generation Firewall* perimetrali (PAN-PA-5410-AC), l'upgrade di solo n.2 licenze *Threat Prevention* già presenti (definite al punto *e*) come segue:

- h. *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;

ed inoltre l'acquisto della licenza Palo Alto Networks:

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

Le restanti n.2 licenze *Threat Prevention* (definite al punto *e*) saranno configurate sui Next-Generation Firewall PAN-PA-5220-AC già presenti.

Tenuto conto della recente situazione di emergenza Covid che ha richiesto l'aumento dei terminali per lavoro a distanza e degli strumenti per il monitoraggio in tema di cyber-security, si rende necessario ampliare i servizi cloud Cortex già acquistati (dalle attuali 4000) fino alla quota di:

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

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 rinnovare:

- k. 13 TB 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 proteggere l'infrastruttura critica della rete cloud e tenuto conto della recente situazione di emergenza dovuta al conflitto in Ucraina che ha richiesto l'incremento degli strumenti per la visibilità ed il monitoraggio delle applicazioni cloud native, si rende necessario l'acquisto di:

- l. 300 crediti per *Palo Alto 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.

Considerata l'importanza di scoprire, valutare e mitigare i rischi connessi all'esposizione di asset aziendali e risorse su tutto il web riducendo la superficie d'attacco cyber, si rende necessario l'acquisto, come sperimentazione, di:

- m. *Palo Alto Expanse*, piattaforma di gestione della superficie di attacco cyber per il monitoraggio delle attività esterne esposte e non tracciate (anch'essa erogata in modalità *software as a service - SaaS*) per 12 mesi.

Infine per migliorare i tempi di gestione dei ticket legate ad esigenze di fuso orario (la sede americana di Palo Alto in California ha una differenza di 9 ore rispetto all'Italia), si rende necessario effettuare l'upgrade





della modalità di erogazione del supporto da *Premium in Partner enable Premium* per tutti i beni e servizi presenti in determina; tale modalità di erogazione del supporto presenta medesimi condizioni e SLA di intervento rispetto alla precedente ma avverrà esclusivamente attraverso un partner certificato *Diamond Innovator e Authorized Support Center (ASC)* in lingua italiana.

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. Non sarebbe pensabile gestire l'infrastruttura di sicurezza utilizzando allo stesso tempo differenti tecnologie;

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'implementazione e la gestione di policy di sicurezza uniformi per tutti i firewall del campus e l'analisi ed identificazione di eventuali incidenti informatici da un'unica piattaforma di management, compatibilità che viene meno con l'immissione di apparati di altra marca;

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

5) l'acquisto delle licenze *Advanced DNS Security* permette di ampliare la security anche a livello DNS, migliorando la reazione agli attacchi informatici attraverso una soluzione integrata ai *Next-Generation Firewall* perimetrali e non comporta ulteriori limiti derivanti dalla differenza di tecnologia e costi considerevolmente più alti rispetto alla soluzione *Infoblox Advanced DNS Protection*;

6) l'acquisto delle licenze *Cortex XDR Pro* costituisce un upgrade al numero di licenze dalle attuali 4000 fino a 4300 endpoints e non richiede alcun strato aggiuntivo di analisi e software di integrazione rispetto alle soluzioni *Microsoft Defender for Endpoint* e *Elastic Endpoint Security*;

7) l'acquisto delle licenze *Palo Alto Prisma Cloud* per la protezione dell'infrastruttura, delle applicazioni, dei dati e delle autorizzazioni nei cloud, amplia i servizi anche al cloud security e non necessita di ulteriori costi in termini di tempo per l'integrazione rispetto alla soluzione *Microsoft Defender for Cloud*;

8) l'acquisto della licenza *Palo Alto Expanse* permette, in modo sperimentale e per un arco di tempo limitato a 12 mesi, di verificare la superficie di attacco cyber attraverso il monitoraggio delle attività esterne esposte e non tracciate sul web e non comporta ulteriori limiti derivanti dalla differenza di tecnologia e costi considerevolmente più alti rispetto alla soluzione *Rapid7 IntSights*, che, a parità di spesa, presenta limiti sugli asset da scansionare e sui piani di rimedio.

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 le convenzioni CONSIP, in particolare nella recente Convenzione Consip LAN 6 (gara a procedura aperta per la fornitura di prodotti e servizi per la realizzazione, manutenzione e gestione di reti locali per le Pubbliche Amministrazioni) e nel Contratto Quadro SPC lotto 2 (relativo a servizi in cloud e quindi non pertinente alle necessità di codesta Amministrazione), ha evidenziato l'assenza di prodotti di Palo Alto Networks tra quelli offerti.





Per dette motivazioni si giustifica ampiamente, soprattutto in termini di Total Cost of Ownership (TCO), il ricorso a una procedura di gara per il rinnovo dei servizi di manutenzione e delle licenze software dei *Next-Generation Firewall* di Ateneo e per l'ampliamento dei servizi di sicurezza cloud-native di marca Palo Alto Networks, alla quale potranno partecipare gli operatori economici certificati dal produttore per la loro commercializzazione e per l'erogazione del servizio di assistenza.

3. LA QUALIFICAZIONE DELL'APPALTATORE

Il sistema di gara prescelto dall'Amministrazione contraente prevede il possesso in capo all'Appaltatore delle certificazioni Palo Alto Diamond Innovator e ASC Authorized Support Center in lingua Italiana.

4. LA DURATA DEL CONTRATTO

La durata del contratto è di tre anni.

5. LA PROCEDURA DI GARA

L'individuazione dell'Appaltatore cui affidare i servizi in oggetto avverrà tramite procedura aperta, ai sensi dell'art. 60 del D.lgs. 50/16 e il criterio di aggiudicazione quello del minor prezzo in quanto trattasi di servizi e forniture con caratteristiche standardizzate e le cui condizioni sono definite dal mercato.

