Guida all'acquisto di una protezione dalle minacce basata su AI con Next-Generation Firewall

Combinare intelligenza artificiale, sicurezza e scalabilità

Il panorama delle minacce

L'uso dell'intelligenza artificiale (AI) da parte di cattivi attori ha reso più complesse le sfide che i team IT e di sicurezza devono risolvere per proteggere le loro organizzazioni. I criminali informatici infatti fanno ampio uso dell'intelligenza artificiale - dai nuovi exploit ai deepfake, fino alle email di phishing avanzate e altre tattiche - per penetrare le difese in modo più rapido e decisivo. Questo significa che i team IT e di sicurezza, già sotto stress, devono gestire ulteriori pressioni per stare al passo con uno scenario delle minacce di per sé scoraggiante.

Tuttavia, aggiungere nuove tecnologie significa chiedere al personale di imparare a usare più console e gestire diversi flussi di allarmi per il triage e le indagini. Se i team sono già sovraccarichi di lavoro, aggiungere più sicurezza non significa aiutarli a lavorare in modo più efficiente. E questo è un problema.

Operazioni a regime

Oggi le organizzazioni lanciano di continuo nuove iniziative digitali per centrare i loro obiettivi strategici e migliorare l'efficienza, espandendo inevitabilmente le loro superfici d'attacco. Tutte queste iniziative digitali - adozione del cloud, abbattimento dei gap tra IT e OT, proliferare dei dispositivi IoT (Internet-of-Things) che si connettono alla rete o supporto della forza lavoro ibrida - mettono a dura prova i team IT e di sicurezza già sovraccarichi.

Sicurezza, scalabilità ed efficienza

Un livello di sicurezza più elevato o rafforzato richiede necessariamente più efficienza. Le soluzioni di cybersecurity di oggi devono aiutare i team di sicurezza e IT a proteggere efficacemente le organizzazioni da varie minacce, in particolare quelle basate su AI.

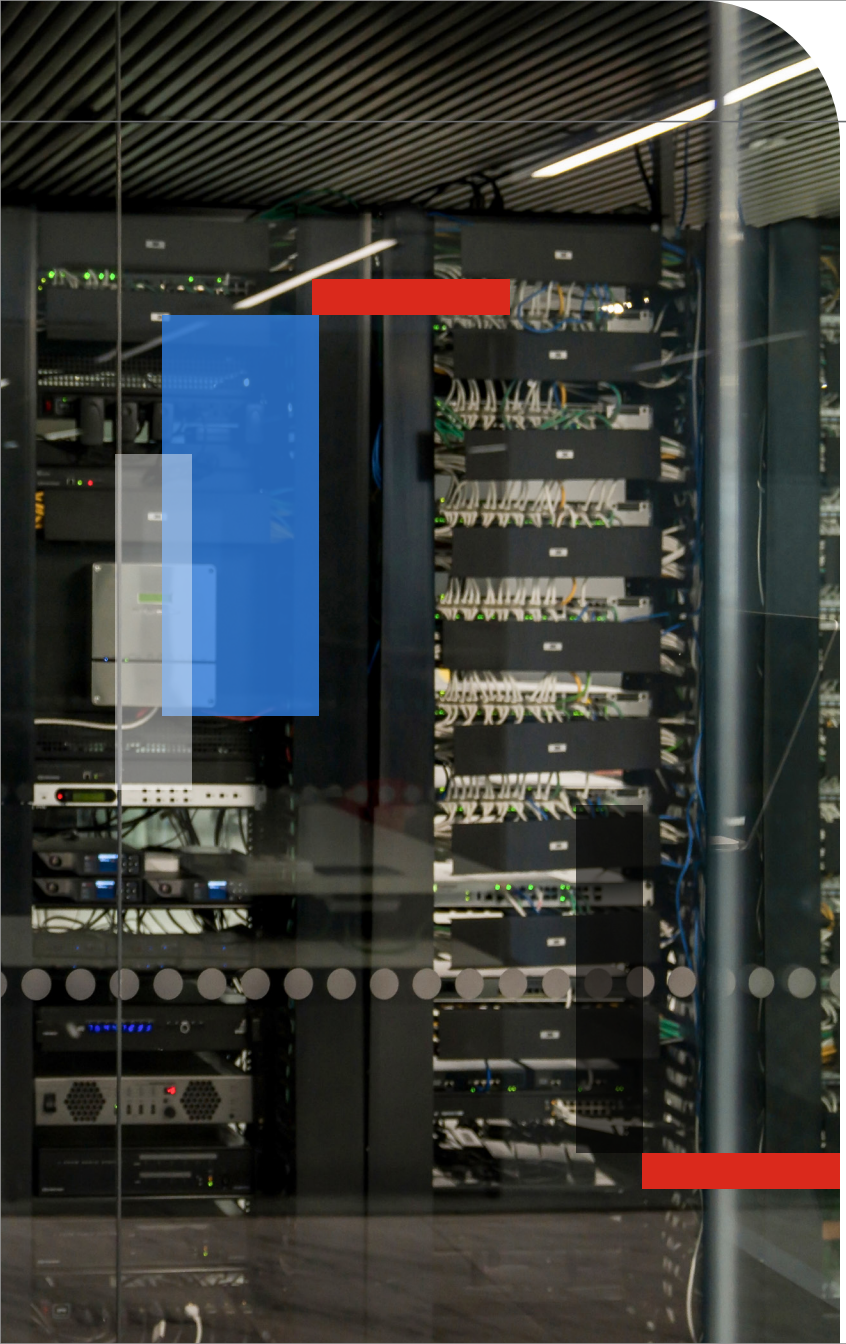
Al tempo stesso, le soluzioni devono aiutare i team a scalare le rispettive attività. In futuro, questo cambiamento di prospettiva e di requisiti dovrà avvenire da due punti di vista:

- I team IT e di sicurezza devono far convergere roadmap separate per integrare le loro attività di sicurezza.
- I vendor di cybersecurity devono offrire soluzioni olistiche che proteggano dalle minacce emergenti basate su AI e migliorino l'efficienza.

I firewall mesh ibridi (HMF) dimostrano ad esempio come unire funzioni di sicurezza basate su AI e un miglioramento dell'efficienza, grazie a un approccio alla sicurezza centralizzato e coordinato. Questa soluzione ibrida offre funzioni di protezione dalle minacce e di sicurezza basate su AI, per aiutare le organizzazioni a combattere efficacemente l'AI con l'AI. Inoltre, fornisce un approccio centralizzato e coordinato alla protezione della superficie d'attacco in continua espansione della rete, inclusi gli ambienti IT e OT, le aree on-premise e cloud, o quelle di diverse sedi fisiche.

Cos'è una soluzione firewall mesh ibrida?

Una HMF è una soluzione di gestione centralizzata e unificata che rende semplici le operazioni di cybersecurity: rappresenta un progresso naturale nell'evoluzione del Next-Generation Firewall. In un ambiente ibrido, le aziende possono distribuire i firewall on-premise o nel cloud con un unico sistema operativo per le comunicazioni e per gli aggiornamenti dell'intelligence sulle minacce in tutte le implementazioni.



Implementare una gestione unificata e centralizzata

- **Gestione semplificata:** unifica la gestione della sicurezza in una singola piattaforma eliminando la complessa gestione di più firewall di vendor diversi
- **Una postura di sicurezza coerente:** riduce il rischio di gap e vulnerabilità della sicurezza applicando un'unica policy di sicurezza sull'intera rete che aiuta le organizzazioni a rispettare la privacy dei dati e le linee guida normative
- **Sicurezza migliorata:** consente una risposta più rapida e precisa agli incidenti di sicurezza usando l'automazione, l'intelligenza artificiale e il machine learning per analizzare il traffico di rete e identificare con più efficacia le potenziali minacce
- **Scalabilità migliorata:** aggiunge nuovi punti di enforcement della sicurezza in base alle necessità, eliminando le criticità gestionali e adattando facilmente la crescita della rete o dei deployment cloud
- **Migliore visibilità:** fornisce una visione olistica della postura di sicurezza dell'intera rete per identificare e risolvere i problemi in modo più efficiente

Perché l'intelligence sulle minacce basata su AI è importante

Nel campo della cybersecurity, un utilizzo critico dell'AI è quello di migliorare l'intelligence sulle minacce. L'uso applicato delle tecnologie AI è decisivo per la raccolta, l'analisi, la correlazione e, infine, la formulazione dei dati in un'intelligence utilizzabile. Questa intelligence sulle minacce con tecnologia AI si può utilizzare tramite le integrazioni per rispondere a un'ampia serie di vettori e minacce, abilitate da AI o meno. L'applicazione dell'AI da parte del vendor e l'estensione delle fonti di dati e i dati stessi sono importanti.
Più un vendor ha visibilità sui dati, più i modelli AI possono apprendere da quella visibilità.

Protezione dalle minacce rafforzata da AI

L'uso dell'AI nella cybersecurity non è solo un avanzamento tecnologico. È un'evoluzione sempre più urgente che può aiutare le organizzazioni a migliorare le difese contro le nuove minacce. La combinazione di funzioni di sicurezza basate su AI con i miglioramenti di efficienza tipici delle soluzioni NGFW aiuta le organizzazioni a creare una postura di sicurezza più resiliente. I NGFW offrono queste funzionalità di sicurezza fondamentali:

Sicurezza della rete e dei file

- **Prevenzione delle intrusioni:** la prevenzione delle intrusioni esegue l'ispezione profonda dei pacchetti del traffico di rete, incluso quello crittografato, per rilevare e bloccare le più recenti minacce e intrusioni nascoste a livello di rete.
- **Antivirus:** l'antivirus protegge dalle più recenti minacce polimorfiche, tra cui ransomware, virus, spyware e altre minacce a livello di contenuto.
- **Controllo delle applicazioni:** il controllo delle applicazioni ti permette di creare rapidamente delle policy per consentire, negare o limitare l'accesso alle applicazioni o a intere categorie di applicazioni.

Sicurezza web/DNS

- **Filtraggio DNS:** il filtraggio DNS assicura una protezione costante contro le minacce sofisticate basate su DNS. Fornisce infatti una visibilità completa del traffico DNS e blocca domini ad alto rischio, tra cui i domini nocivi appena registrati e i domini parcheggiati.
- **Filtraggio URL:** il filtraggio degli URL identifica e blocca gli accessi a URL nocivi da parte di utenti e applicazioni.
- **Anti-botnet e comando e controllo (C2):** le funzionalità anti-botnet e C2 bloccano i tentativi non autorizzati di comunicare con server remoti compromessi per ricevere informazioni C2 nocive o inviare informazioni estratte.

Software-as-a-Service (SaaS) e sicurezza dei dati

- **Cloud access security broker (CASB):** un CASB protegge le applicazioni SaaS in uso, fornendo un'estesa visibilità e un controllo granulare sull'accesso, l'utilizzo e i dati SaaS.
- **Gestione della superficie d'attacco:** la gestione della superficie d'attacco permette di identificare, valutare e monitorare le risorse di rete e la relativa infrastruttura di sicurezza per fornire una valutazione globale della postura di sicurezza dell'organizzazione.

Sicurezza zero-day

- **Sandboxing dei file:** il sandboxing dei file esegue un'analisi avanzata dei file sconosciuti in un ambiente sicuro per stabilire se questi file rappresentano una minaccia.

FORTINET

Considerazioni chiave per una gestione unificata e centralizzata

Per mettere in sicurezza un ambiente ibrido complesso, bisogna iniziare dalla linea di difesa principale: i firewall. Prima di acquistare una soluzione di cybersecurity, come un NGFW con servizi basati su AI, ti consigliamo di valutare:

- **Esigenze di rete:** considera con attenzione le esigenze specifiche del tuo ambiente di rete, come le dimensioni e la complessità della tua rete, la distribuzione dei carichi di lavoro (on-premise o cloud) e la tua attuale postura di sicurezza.
- **Caratteristiche di sicurezza:** valuta le diverse funzionalità offerte dai diversi vendor, come le capacità di rilevamento delle minacce, la crittografia dei dati e l'integrazione con altri strumenti di sicurezza.
- **Facilità di gestione:** verifica che la soluzione di cybersecurity offra una console di gestione centralizzata e intuitiva per ridurre il carico del team di sicurezza.
- **Scalabilità:** esamina la facilità con cui la soluzione di cybersecurity è in grado di scalare per adattarsi alla crescita futura della tua rete o dei deployment cloud.
- **Costo:** calcola i costi di licenza, i costi di abbonamento e dei servizi professionali richiesti per l'implementazione e la manutenzione.
- **Reputazione del vendor:** scegli un vendor affidabile con un'esperienza comprovata e verificata da fonti terze.

Valutando attentamente questi fattori, puoi scegliere un NGFW in linea con le tue specifiche esigenze di sicurezza e che offra il miglior valore per il tuo investimento.

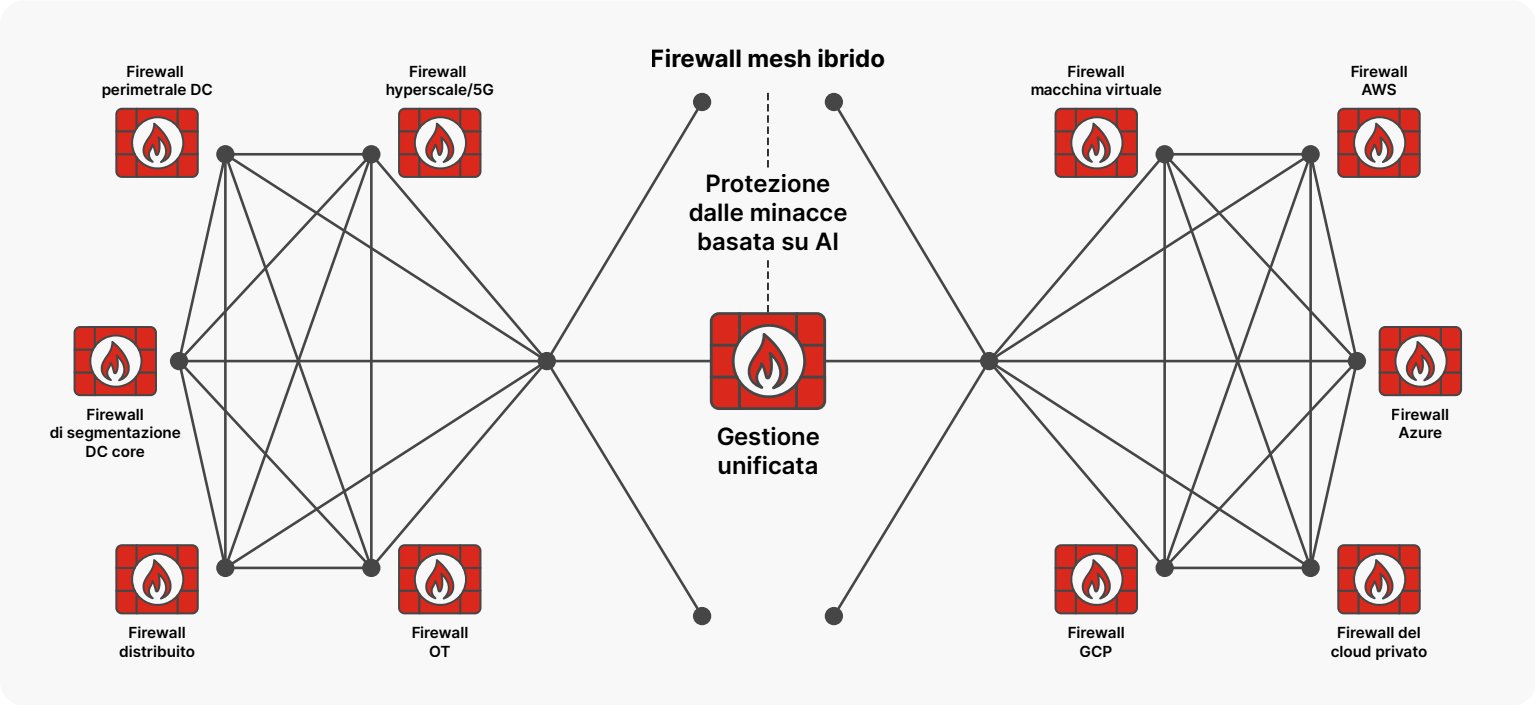


Figura 1: Come funzionano gli HMF con protezione dalle minacce basata su AI

Domande chiave per il tuo vendor di NGFW

1 Capire le capacità di ricerca sulle minacce del vendor

L'intelligence sulle minacce basata su AI è fondamentale. Tutto inizia dal gruppo di persone dedicate che compongono il team di ricerca sulle minacce del vendor (se esistente).

- La tua organizzazione ha un team di ricerca sulle minacce e, in caso affermativo, qual è la sua composizione e il suo ruolo?
- Questo team è coinvolto nell'adozione delle tecnologie AI della tua azienda, e in che misura?

2 Capire la formulazione dell'intelligence sulle minacce

Nella cybersecurity, l'AI migliora l'intelligence sulle minacce; è quindi importante capire quanto sia estesa la visibiltà del vendor. È necessario conoscere l'estensione delle fonti di telemetria e di informazione e le capacità di AI che aiutano a trasformare la telemetria e gli altri dati in intelligence utilizzabile.

- Quale visibilità sulle minacce e sulle relative fonti di dati utilizza la tua organizzazione per formulare l'intelligence sulle minacce integrata nella tua soluzione?
- Come viene utilizzata l'AI nella formulazione dell'intelligence sulle minacce?

3 Capire quanto è esteso l'uso dell'AI

È essenziale sapere a che livello un vendor utilizza tecnologie e strumenti di AI per migliorare le sue offerte e i relativi risultati in termini di sicurezza.

- Qual è l'esperienza della tua organizzazione sull'uso delle tecnologie AI nei vostri prodotti, servizi e soluzioni?
- Quale o quali specifiche tecnologie AI vengono applicate a questa particolare soluzione e quali sono i vantaggi del loro utilizzo?
- Quali fonti di dati utilizza il prodotto, il servizio o la soluzione per il feed delle tecnologie AI in uso?

4 Capire quali funzionalità di sicurezza sono integrate in una soluzione

Ad esempio, i NGFW dovrebbero fornire diverse funzioni e integrazioni chiave di sicurezza. Devi sapere cosa sono, cosa è incluso nell'acquisto di una soluzione e in che modo possono essere utili alla tua organizzazione.

- Quali tra le seguenti funzionalità di sicurezza offre la tua soluzione?
  - Prevenzione delle intrusioni
  - Antivirus
  - Controllo dell'applicazione
  - Anti-phishing
  - Broker di sicurezza per l'accesso al cloud
  - Prevenzione della perdita di dati
  - Sandboxing dei file
  - Sicurezza web, inclusa la sicurezza DNS
  - Gestione della superficie d'attacco
  - Sicurezza OT
  - Sicurezza IoT
  - Altro
- In che modo l'AI viene applicata ai servizi sopra elencati?

5 Cosa cercare in un ambiente ibrido

Quando si sceglie un NGFW, è essenziale conoscere le proprie esigenze di sicurezza e il proprio ambiente di rete. Sarebbe opportuno chiedere ai vendor demo e prove per verificare che la soluzione soddisfi le proprie esigenze. Inoltre, se si utilizza un ambiente multivendor, è fondamentale cercare una soluzione NGFW in grado di integrarsi con i firewall esistenti dei diversi vendor.

Ecco alcune caratteristiche chiave da cercare in un NGFW:

Capacità di sicurezza

- Protezione avanzata dalle minacce con uso di tecnologie AI, incluso il machine learning, per identificare e bloccare le minacce informatiche più sofisticate
- Applicazione granulare delle policy per definire e applicare policy di sicurezza coerenti in tutta l'infrastruttura IT
- Feed di intelligence sulle minacce per rimanere aggiornati sulle vulnerabilità e sui metodi di attacco più recenti

Gestione e scalabilità

- Gestione centralizzata da un'unica interfaccia per gestire e monitorare tutti i tuoi firewall
- Deployment e provisioning automatizzati per implementare e configurare senza problemi tutti i firewall dell'intera rete
- Scalabilità per aggiungere o rimuovere facilmente i firewall quando la rete cresce o si riduce

Risparmio sui costi e vantaggi per l'azienda

"Fortinet offre molto più di un firewall. Ha fatto convergere diversi componenti di rete e di sicurezza migliorando le prestazioni della rete e della sicurezza.
Il punto di forza di Fortinet è che offre molto di più della protezione di un firewall."

- Responsabile della sicurezza tecnica e di rete, risorse naturali

318%
ritorno sull'investimento (ROI)

50%
riduzione delle interruzioni di rete grazie alle migliori prestazioni della rete e della sicurezza

6 mesi
payback in meno di sei mesi

50%[1]
aumento della produttività dei team di sicurezza e di rete

Un nuovo modo di pensare

L'AI è entrata in un'ulteriore fase di innovazione che avrà nuovi impatti negativi e positivi sulle organizzazioni. Oltre a valutare in che modo una soluzione di sicurezza abilitata all'AI raggiunge gli obiettivi di cybersecurity, i leader della sicurezza e IT devono anche considerare in che modo migliora l'efficienza.

I NGFW rappresentano un esempio convincente di questo nuovo modo di pensare. Forniscono una protezione dalle minacce basata su AI e centralizzano la visibilità sulla rete ibrida, coordinando e applicando le policy del firewall. Il risultato è una migliore postura di sicurezza e quindi un aumento della capacità del team di scalare per affrontare le sfide di un panorama di minacce in continua evoluzione.

Se desideri implementare un NGFW nella tua organizzazione, contatta un esperto Fortinet che ti aiuterà a scegliere una soluzione pensata per le tue specifiche esigenze di sicurezza e di rete.

Chiama il numero verde negli Stati Uniti:
+1 866 868 3678

Vendite del governo federale degli Stati Uniti:
+1 833 386 8333

Vendite in Canada: **+1 833 308 3247**

[1] Forrester, The Total Economic Impact™ Of Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution Cost Savings and Business Benefits Enabled by NGFW for Data Center and AI-Powered FortiGuard Security Services Solution, luglio 2023.

FORTINET

www.fortinet.com

21 agosto 2024 10:58

2627272-0-0-IT