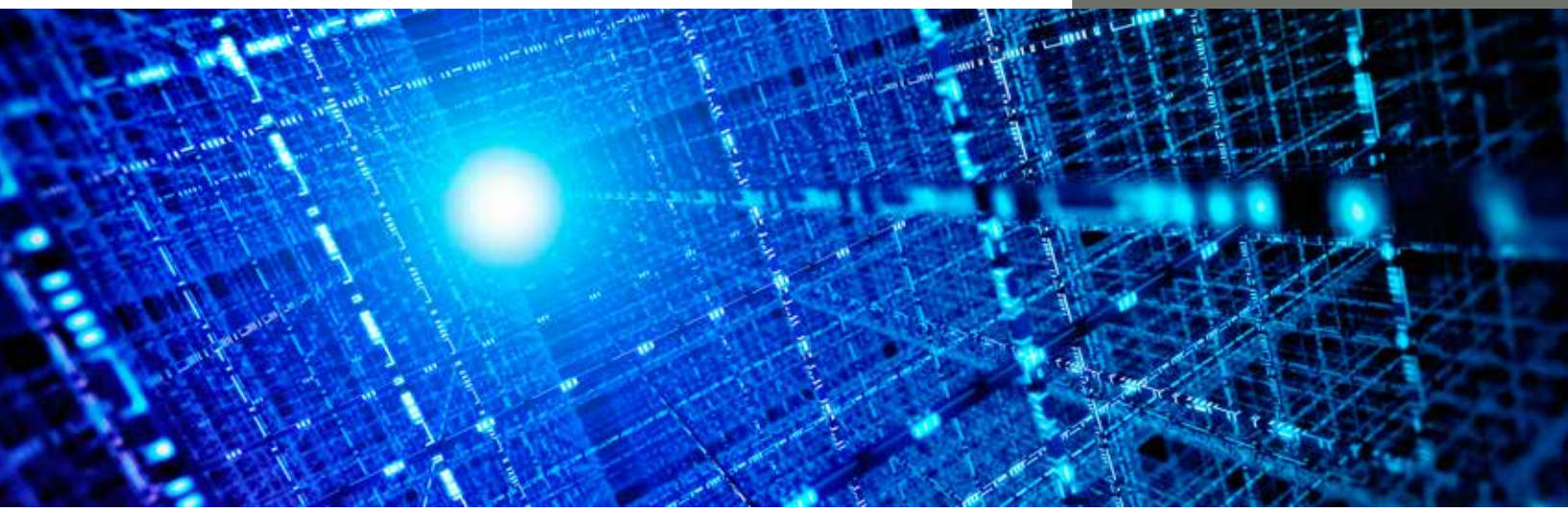


Fortinet Security Fabric

Segmentazione end-to-end

Le reti stanno attraversando in questo momento cambiamenti radicali mai visti negli ultimi trent'anni. Le imprese devono affrontare contemporaneamente problemi come BYOD, IoT, virtualizzazione, SDN, cloud, proliferazione di applicazioni, big data e l'aspettativa della nuova generazione di dipendenti di unire lavoro e vita privata su di un solo dispositivo di loro scelta, con accesso istantaneo a qualsiasi dato in qualsiasi momento da qualsiasi luogo.

Ciò ha aumentato esponenzialmente la superficie di attacco di cui le imprese devono preoccuparsi. Ad esempio:

- L'IoT e le soluzioni cloud fanno si che le organizzazioni debbano preoccuparsi di una superficie di attacco che molte volte può non essere visibile all'IT.
- Molti dispositivi IoT sono headless, eseguono protocolli di comunicazione semplici e non sono in grado di eseguire un client o perfino di ricevere patch. Per la sicurezza fanno affidamento esclusivo sulla rete di accesso.
- Dati aziendali critici e proprietari vengono spostati nel cloud e gestiti da terze parti. Nota come shadow IT, questa tendenza è in espansione e diverse imprese semplicemente ignorano dove si trovano attualmente i dati o da quali misure di sicurezza sono protetti.
- La trasformazione in un modello di business digitale ha ampliato la rete oltre il perimetro e ciò significa che le reti di oggi e la loro sicurezza non hanno ormai più confini definiti.
- I dispositivi BYOD sono estremamente mobili, combinano profili personali e lavorativi e rappresentano un rischio reale quando l'accesso a dati critici avviene da luoghi pubblici o quando i dispositivi vengono persi o rubati.

Il problema è reso più complesso dalla proliferazione di prodotti di sicurezza integrati in tutta la rete distribuita. La tendenza, man mano che le reti diventano più complicate, è quella di aggiungere nuovi dispositivi di sicurezza a un sistema già sovraccarico. Ma il fatto è che la complessità è nemica della sicurezza. Le soluzioni di sicurezza compartimentalizzate, con interfacce di gestione separate e nessun modo significativo di acquisire o condividere informazioni sulle minacce con gli altri dispositivi di rete, hanno un'utilità solo marginale. Accade in effetti che molte nuove soluzioni non vengano mai distribuite completamente, semplicemente perché non vi è abbastanza personale da assegnare al compito di installare, gestire, ottimizzare e aggiornare un altro dispositivo complicato.

La risposta ad ambienti di rete sempre più complessi deve invece essere la semplicità. Per la protezione di questi ambienti in evoluzione vi sono tre requisiti:

1. Segmentazione – Le reti devono essere segmentate in modo intelligente in zone di sicurezza funzionali. La segmentazione end-to-end, dall'IoT al cloud e attraverso ambienti fisici e virtuali, fornisce una visibilità approfondita del traffico che si sposta lateralmente attraverso la rete distribuita, limita la diffusione di malware e permette l'individuazione e la messa in quarantena dei dispositivi infetti.
2. Intelligence collaborativa - L'intelligence globale e locale delle minacce deve essere condivisa tra i dispositivi di sicurezza e una risposta coordinata tra i dispositivi deve essere orchestrata centralmente.
3. Policy universale – È necessario un motore di policy di sicurezza centralizzato che determini i livelli di attendibilità tra i segmenti di rete, raccolga informazioni sulle minacce in tempo reale, stabilisca un'adeguata policy di sicurezza unificata la applichi in modo distribuito e orchestrato.

Il Security Fabric di Fortinet integra tecnologie per endpoint, livello di accesso, rete, applicazioni, data center, contenuti e cloud in un'unica soluzione di sicurezza collaborativa che può essere orchestrata attraverso un'unica interfaccia di gestione. Si basa su cinque principi chiave:

- **Scalabilità: il Fortinet Security Fabric protegge l'impresa dall'IoT al cloud.**

  Una strategia di sicurezza completa ha bisogno sia di profondità (prestazioni ed ispezione profonda) che di ampiezza (end-to-end). La sicurezza deve essere scalabile non solo per venire incontro alle domande relative a volumi e prestazioni, ma anche in direzione laterale, tracciando e proteggendo i dati senza discontinuità dall'IoT e dagli endpoint attraverso la rete distribuita e il data center, fin dentro il cloud. Il Fortinet Security Fabric fornisce una protezione integrata e capillare attraverso l'impresa distribuita, dall'IoT al cloud, nonché l'ispezione di dati a pacchetto, protocolli applicativi e un'analisi approfondita dei contenuti non strutturati, il tutto a velocità wire-speed.

- **Elevata visibilità: il Fabric si comporta come una singola entità per quanto riguarda policy e registrazione, consentendo una segmentazione end-to-end per ridurre il rischio rappresentato dalle minacce avanzate.**

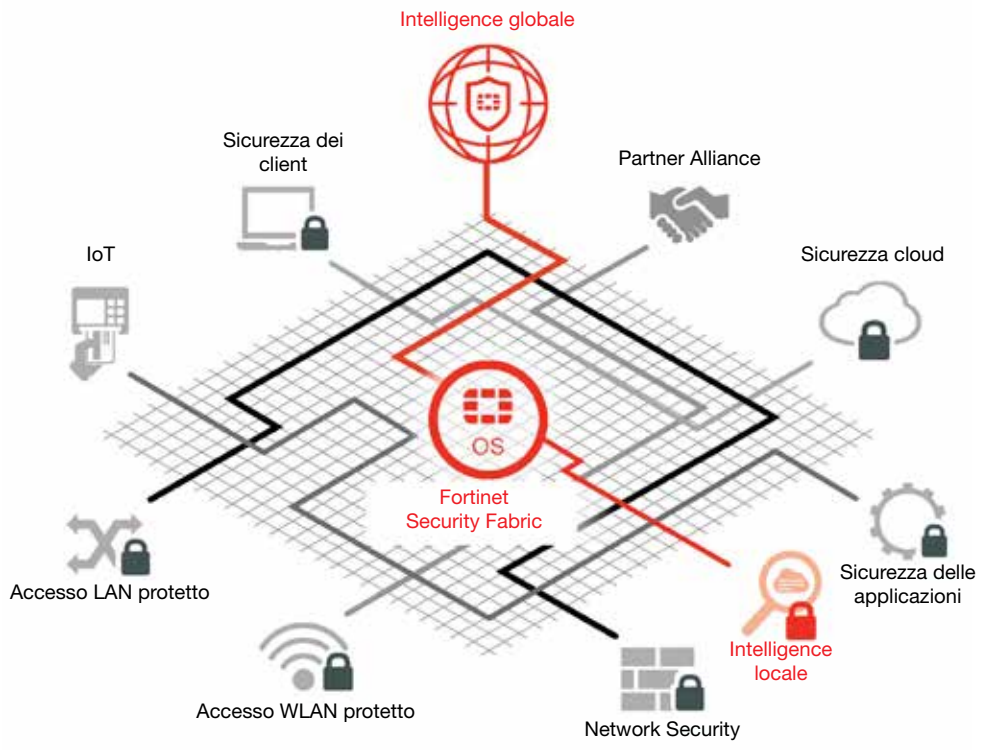
  È necessario avere visibilità non solo dei dati che entrano ed escono dalla rete, ma anche del modo in cui attraversano la rete una volta che sono all'interno del perimetro. Il Fortinet Security Fabric consente una segmentazione della rete end-to-end per una visibilità e ispezione approfondita del traffico interno alla rete e per il controllo sugli spostamenti di dati e utenti, riducendo così il rischio rappresentato dalle minacce avanzate.

- **Sicurezza: Threat Intelligence e informazioni di attenuazione globali e locali possono essere condivise tra i vari prodotti per ridurre il tempo necessario ad attivare le misure di protezione.**

  Non solo la sicurezza deve includere potenti strumenti di sicurezza per le varie posizioni e funzioni della rete, ma una vera visibilità e un vero controllo richiedono che questi elementi discreti lavorino insieme come un sistema di sicurezza integrato. Il Security Fabric di Fortinet si comporta come una singola entità collaborativa da un punto di vista di policy e registrazione, consentendo ai singoli elementi del prodotto di condividere Threat Intelligence globale e locale e informazioni sull'attenuazione delle minacce.

- **Utilità per l'azione: sistemi cloud basati sui big data correlano informazioni sulle minacce e dati sulla rete per fornire una Threat Intelligence utilizzabile in tempo reale.**

  Rilevare traffico sospetto o bloccare il malware utilizzando dispositivi di sicurezza discreti non è abbastanza. È necessario un insieme comune di strumenti di Threat Intelligence e orchestrazione centralizzata che permetta alla sicurezza di adattarsi in modo dinamico man mano che vengono individuate minacce, non solo nella rete, ma ovunque nel mondo. I sistemi cloud di Fortinet, basati sui big data, centralizzano e correlano informazioni sulle minacce e dati sulle reti per fornire Threat Intelligence utile all'azione a ogni dispositivo di sicurezza nel Security Fabric di rete in tempo reale.



- **Standard aperti: API aperte ben definite consentono a partner tecnologici leader di integrarsi nel Fabric.**

  Naturalmente un vero Security Fabric consentirà di massimizzare l'investimento già operato in tecnologie di sicurezza. Per questo motivo Fortinet ha sviluppato una serie di API aperte e ben definite, che consentono ai partner tecnologici di integrarsi nel Fortinet Security Fabric.

  Con questa combinazione, il Fortinet Security Fabric è in grado di adattarsi in modo dinamico a un'architettura di rete in evoluzione, così come a un panorama delle minacce in continuo cambiamento.

  Esaminiamo più da vicino i cinque elementi chiave del Fortinet Security Fabric: Scalabilità, Elevata visibilità, Sicurezza, Utilità per l'azione e Standard aperti.

1. Scalabilità

La sicurezza deve essere scalabile non solo per venire incontro alle domande relative a volumi e prestazioni, ma anche in direzione laterale, tracciando e proteggendo i dati senza discontinuità dall'IoT e dagli endpoint attraverso la rete distribuita e il data center, fin dentro il cloud.

Il Fortinet Security Fabric fornisce tre elementi essenziali:

1. Una piattaforma singola e unificata che condivide Threat Intelligence comune, permette una collaborazione intelligente tra dispositivi di sicurezza e si adatta in modo dinamico a nuove minacce.
2. Una singola console di gestione per tutte le tecnologie di sicurezza, ovunque siano distribuite, per l'orchestrazione centralizzata delle policy, il coordinamento della risposta alle minacce e l'applicazione distribuita in tempo reale delle misure di sicurezza.
3. Una singola fonte di aggiornamenti e intelligence di sicurezza, che unisce servizi di informazioni locali e intelligence globale per una risposta in tempo reale a minacce note ed emergenti.

Scalabilità nel cloud

L'adozione di virtualizzazione e servizi basati su cloud sta trasformando le reti. Questa migrazione verso il cloud presenta diverse sfide di sicurezza distinte, che possono essere affrontate solo attraverso un approccio Fabric sicuro:

1. **Virtualizzazione e cloud privato.** Anche se la virtualizzazione è in corso ormai da tempo, è ancora un'area vulnerabile e in gran parte non protetta di molte reti. Una strategia per proteggere gli ambienti virtualizzati deve tenere conto di diversi aspetti.

   La prima è che circa il 40% delle imprese che adottano la virtualizzazione finisce con il distribuire più Hypervisor. Per garantire una sicurezza integrata e omogenea tra questi ambienti virtualizzati, le soluzioni di sicurezza adottate devono supportare tutti i principali Hypervisor.

   Un'altra sfida sta nel fatto che alcune soluzioni di virtualizzazione lasciano un vuoto tra risorse fisiche e virtuali. La sicurezza deve colmare questo vuoto per garantire una visibilità delle minacce e un'applicazione delle misure di sicurezza coerenti, a prescindere dai dispositivi che elaborano i dati.

   Vi sono diversi nuovi attacchi che prendono di mira in modo specifico le macchine virtuali e che includono rootkit virtuali per mascherare la loro presenza. In molte organizzazioni il traffico tra le macchine virtuali viene raramente ispezionato e ciò lascia scoperti e vulnerabili agli attacchi macchine virtuali, carichi di lavoro e transazioni.

   Infine, la virtualizzazione consente la distribuzione rapida di nuove risorse per i carichi di lavoro e una scalabilità dinamica per gestire picchi inattesi nel traffico dati. La sicurezza per gli ambienti virtualizzati deve essere applicata in tempi brevi e adattarsi rapidamente, in modo che le transazioni di business e i flussi di lavoro critici non vengano mai interrotti o inutilmente reindirizzati per l'ispezione.

   Un approccio di sicurezza basato sul Fabric consente alle imprese di creare policy di sicurezza integrate tra gli ambienti fisici, virtuali e cloud privati.

2. **Data center SDN di nuova generazione.** I data center stanno attraversando rapidi cambiamenti, tra cui l'implementazione di reti di nuova generazione software-defined e ambienti cloud privati. Queste nuove architetture consentono un provisioning istantaneo delle risorse, il concatenamento dei servizi e l'accelerazione dei flussi di lavoro, astraendo allo stesso tempo il sovraccarico di gestione del livello fisico di porte, server e switch.

   Questi nuovi data center richiedono soluzioni di sicurezza dedicate progettate per le loro specifiche architetture. Inoltre questi nuovi ambienti vengono eseguiti insieme ai data center tradizionali, rendendo difficile l'adozione di un unico standard di sicurezza. Per complicare ulteriormente le cose, alcune soluzioni SDN rendono difficile collegare ambienti virtuali e fisici e pertanto la definizione e applicazione di policy di sicurezza uniformi può costituire una sfida.

   Il vantaggio è che la possibilità di integrare i servizi di sicurezza direttamente nelle catene delle transazioni consente un funzionamento inline con provisioning automatico della sicurezza est-ovest e una scalabilità dinamica delle risorse di sicurezza.

   Come per la virtualizzazione, una strategia Fabric sicura consente alle organizzazioni di inserire dispositivi di sicurezza in diversi ambienti architetturali, mantenendo allo stesso tempo una Threat Intelligence centralizzata e un'applicazione delle policy uniforme.

3. **Cloud pubblico e ibrido.** Diverse imprese stanno adottando servizi cloud pubblici per tutto, dall'offload on demand di elevati volumi di traffico, un processo noto come cloud bursting, allo spostamento di parte o di tutta l'infrastruttura nel cloud con una qualche forma di software, piattaforma o infrastruttura come servizio (SaaS, PaaS o IaaS).

   Dal punto di vista della sicurezza, la sfida è come stabilire e mantenere policy di sicurezza omogenee e applicarle in modo uniforme in un contesto in cui i dati si spostano avanti e indietro tra ambienti locali e cloud.

   Per far si che ciò funzioni, devono verificarsi due condizioni. In primo luogo, è necessario lavorare con un service provider in grado di applicare all'ambiente cloud la stessa tecnologia di sicurezza utilizzata in azienda. Ciò significa che è necessario selezionare una soluzione interna già ampiamente adottata dalla comunità dei service provider. In secondo luogo, occorre uno strumento di gestione ed orchestrazione della sicurezza basato su cloud in grado di trasferire policy e intelligence di sicurezza tra dispositivi di sicurezza attraverso ambienti distribuiti.

Il Fortinet Security Fabric fornisce soluzioni per ciascuno di questi ambienti, comprese le soluzioni di sicurezza disponibili sul mercato adottate più ampiamente dai service provider, le quali possono essere unite in un unico Security Fabric integrato per una completa visibilità e controllo attraverso l'intero ambiente distribuito.

Scalabilità per la rete

Con sempre più dispositivi e applicazioni che accedono alle risorse di rete, le prestazioni sono diventate un aspetto critico. Fin troppo spesso, quando la sicurezza diventa un collo di bottiglia, gli utenti e gli amministratori cominciano a cercare escamotage.

Le soluzioni di sicurezza tradizionali che dipendono dalla potenza di elaborazione della CPU non hanno la scalabilità necessaria per soddisfare una domanda in crescita.

- I dispositivi di sicurezza subiscono duri colpi dal punto di vista delle prestazioni quando vengono aggiunti ulteriori strumenti di ispezione
- Il collegamento in cascata di dispositivi di sicurezza per l'ispezione seriale del traffico introduce problemi aggiuntivi di latenza e l'ispezione ridondante degli stessi dati o contenuti applicativi

I dispositivi di sicurezza e il Security Fabric di Fortinet sfruttano ASIC brevettati ad alte prestazioni che forniscono un'elaborazione in percorsi paralleli. Ciò significa che:

- È possibile eseguire l'offload dell'elaborazione dei pacchetti a un processore di rete per accelerarne l'ispezione
- È possibile eseguire l'offload del contenuto al nuovo processore di contenuti di Fortinet per un'ispezione approfondita di dati non strutturati, che richiede una quantità significativa di risorse
- L'uso della CPU potrà essere limitato all'elaborazione dati tradizionale e alla gestione delle policy
- Gli aggiornamenti della Threat Intelligence e il coordinamento delle policy può avere luogo senza ripercussioni sulle operazioni di business critiche

Il risultato è maggiori prestazioni a costi minori, meno latenza, meno consumo energetico e meno spazio di rack necessario.

Accesso sicuro scalabile

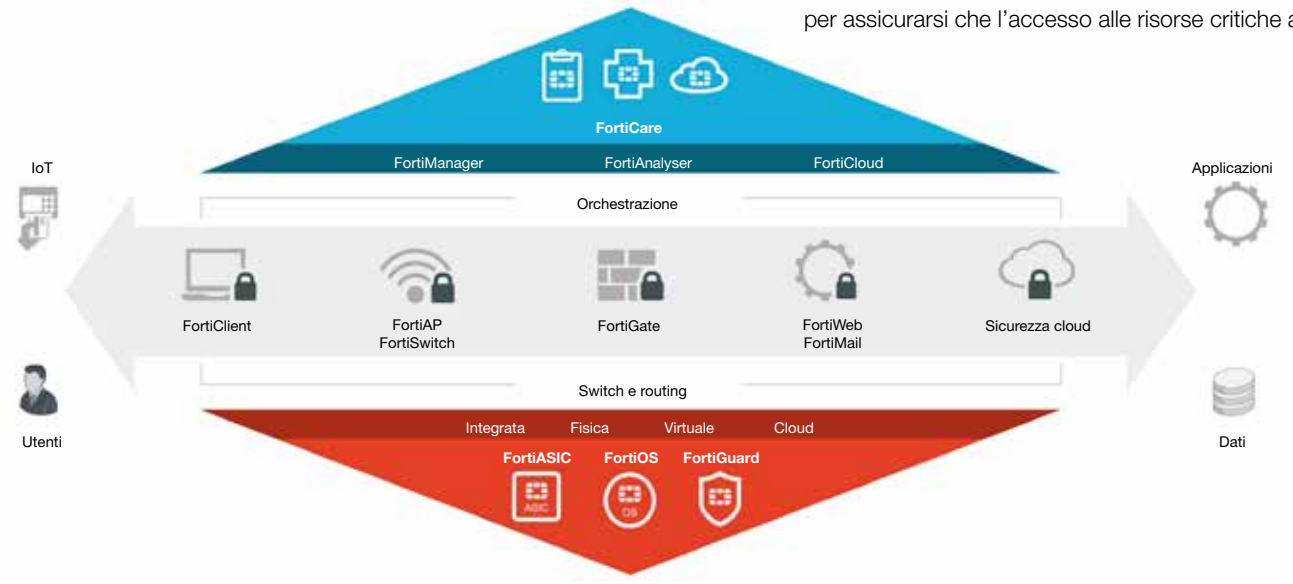
Il controllo degli accessi è un componente critico di qualsiasi strategia di sicurezza. Quando è integrato in un Security Fabric, i dispositivi che si collegano alla rete, sia da fuori che da dentro il perimetro, possono essere identificati, tracciati e protetti mentre attraversano l'ambiente di rete.

Il BYOD ha portato la prima ondata di nuovi dispositivi che sono entrati a fare parte della rete. Ma con l'avvento dell'Internet of Things (IoT) le imprese si devono attendere, nel corso dei prossimi due anni, l'ingresso in rete di miliardi di nuovi dispositivi che utilizzano protocolli IP e che non fanno capo a un utente. Più che mai, la prima fase della sicurezza deve essere la sicurezza degli accessi, per questi motivi:

- Molti di questi dispositivi non possono essere protetti indipendentemente
- La maggior parte dei dispositivi IoT è headless, quindi non è possibile installarvi un client o applicare patch a codice dannoso o non sicuro, e non vi è alcun meccanismo per gli aggiornamenti
- Anche molti dei nuovi dispositivi BYOD non hanno un client installato

E con il continuo sgretolamento dei confini delle reti, l'accesso sicuro non riguarda più solo l'accesso al perimetro.

- I dispositivi possono essere locali o remoti, dentro o fuori il perimetro
- Le applicazioni si collegano attraverso tunnel da dispositivi remoti direttamente al data center o al cloud
- La sicurezza dell'accesso tra i segmenti di rete è fondamentale per assicurarsi che l'accesso alle risorse critiche avvenga



esclusivamente da parte di utenti e dispositivi autorizzati e che i dispositivi infetti non possano diffondere il malware lateralmente attraverso la rete

- Le policy di sicurezza e la loro applicazione dovranno adattarsi in modo dinamico a questo panorama in continuo cambiamento

La risposta a un problema più complesso deve essere la semplicità. Un approccio alla sicurezza basato sul Fabric permette a un'impresa di creare e monitorare una strategia coerente e unificata attraverso tutti i metodi di accesso, che siano cablati, wireless o VPN.

2. Elevata visibilità

La visibilità è critica. Purtroppo, il fatto è che molte imprese hanno molte poche informazioni riguardo a quali utenti e dispositivi sono sulla loro rete in un dato momento. Questa situazione poteva essere accettabile molto tempo fa, quando i confini della rete erano rigidi e chiaramente definiti. Ma con l'avvento di BYOD, IoT, virtualizzazione, cloud e applicazioni commerciali che scambiano dati in rete, una scarsa visibilità è una ricetta sicura per il disastro. Una strategia di visibilità efficace deve includere:

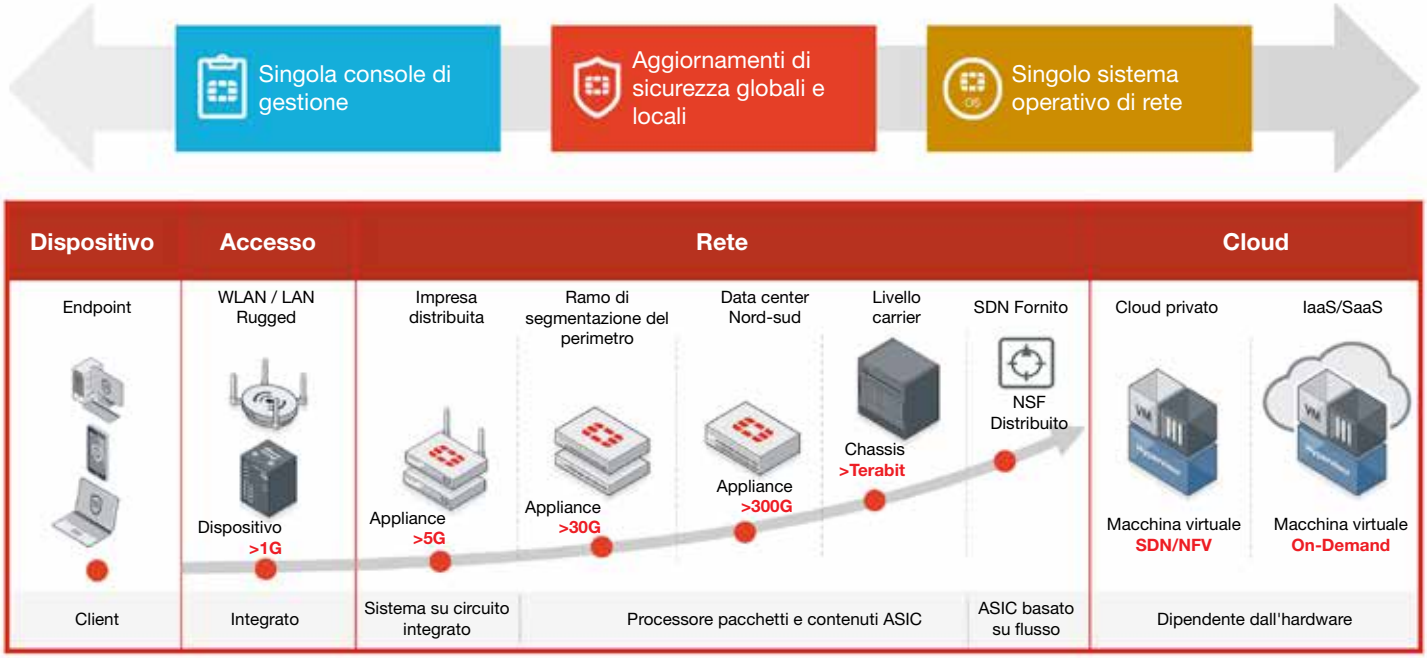
- Identificazione degli utenti: chi è nella rete? Cosa può fare? Quando si è registrato nella rete?
- Identificazione dei dispositivi: quali dispositivi sono presenti nella rete? A chi appartengono? Cosa possono fare? Come posso sapere se mostrano comportamenti sospetti?
- Topologia fisica: in che modo questi dispositivi sono connessi alla rete? Con quali dispositivi possono e non possono interagire?
- Topologia di rete e delle applicazioni: di quali policy abbiamo bisogno? Come vengono distribuite e applicate? Abbiamo una visione unificata di tutta la rete? Come ci rendiamo conto che una policy è stata violata? Una violazione rilevata su un dispositivo può attivare una risposta automatica su un altro dispositivo?

Essere in grado di rispondere a queste domande può servire da catalizzatore per la pianificazione, progettazione, implementazione e ottimizzazione di una strategia di visibilità efficace. Può inoltre servire da metro di misura critico per la valutazione delle tecnologie di sicurezza scelte per la rete.

Visibilità – I vantaggi del Fortinet Security Fabric

Il bisogno di una visibilità completa attraverso l'impresa distribuita, unita a un controllo granulare e a una risposta automatizzata attraverso più dispositivi di sicurezza, è stato un fattore chiave alla base dello sviluppo del Security Fabric da parte di Fortinet. Questo Fabric unisce dati, applicazioni, dispositivi e flussi di lavoro per fornire un livello di visibilità mai reso disponibile da nessun provider di soluzioni di sicurezza. Il Fortinet Security Fabric copre:

- Sicurezza dei client endpoint
- Accesso sicuro (cablato, wireless e VPN)
- Sicurezza di rete
- Sicurezza del data center (fisica e virtuale)
- Sicurezza delle applicazioni (commerciali e personalizzate)
- Sicurezza cloud
- Sicurezza dei contenuti (e-mail e Web)
- Sicurezza dell'infrastruttura (switch e routing)



Il Fortinet Security Fabric è progettato per fornire un'applicazione integrata, collaborativa e adattiva attraverso la rete distribuita e può convertire in modo dinamico dati attuali, registri ed eventi in policy.

3. Sicurezza

Per il successo di una strategia di sicurezza integrata, è necessario che le informazioni disponibili siano coerenti. Gli ambienti complessi con sistemi di più vendor presentano due problemi:

- Una visione non uniforme delle minacce rilevate o cercate
- L'incapacità di condividere con gli altri dispositivi di sicurezza informazioni sulle minacce utili all'azione

La Threat Intelligence deve essere globale

Sapere è potere. L'efficacia di qualsiasi strategia o soluzione di sicurezza sta nella sua abilità di riconoscere e reagire ai pericoli, specialmente quelli mai incontrati prima. Aggiornamenti costanti da una fonte di intelligence attendibile che raccoglie informazioni in tempo reale in tutto il mondo permettono alle soluzioni di essere sintonizzate con le minacce più recenti. Ciò funziona ancora meglio quando tutti i dispositivi nel Security Fabric condividono le stesse informazioni.

Il laboratorio di ricerca sulle minacce di FortiGuard fornisce ai dispositivi Security Fabric informazioni critiche per la sicurezza, provenienti da:

- Threat Intelligence Exchange: la Cyber Threat Alliance è un consorzio di vendor di sicurezza leader che si sono riuniti per condividere threat intelligence sugli attacchi avanzati, le loro motivazioni e le tattiche degli aggressori. Insieme, forniscono la Threat Intelligence più completa disponibile sul mercato.
- Ricerca sulle minacce Fortinet: in aggiunta, il team di ricerca sulle minacce Fortinet fornisce indagini approfondite su minacce e vulnerabilità emergenti, per fornire alle organizzazioni intelligence di sicurezza completa e utile all'azione. Il team Fortinet ha scoperto e segnalato più attacchi zero-day di qualsiasi altra organizzazione nel mondo.
- Feed in tempo reale dalle soluzioni Fortinet: Fortinet ha inoltre milioni di dispositivi in tutto il mondo che rilevano e localizzano minacce e malware e forniscono informazioni in tempo reale su attività, tendenze e problemi emergenti.

L'intelligence acquisita da queste risorse viene raccolta, correlata e convertita in aggiornamenti che vengono inviati continuamente all'intero portfolio di soluzioni di sicurezza Fortinet. Ciò garantisce che il Security Fabric sia in grado di rilevare e reagire alle minacce più recenti, a prescindere da dove si presentano nell'intera rete distribuita.

La Threat Intelligence deve inoltre essere locale

Oltre all'intelligence globale, le soluzioni di sicurezza devono tenere conto di ciò che accade nella rete locale. Comportamenti anomali, malware, dispositivi sconosciuti e utenti non autorizzati devono essere identificati rapidamente, in modo che il Security Fabric possa intervenire con contromisure immediate per proteggere la rete, limitare la propagazione del codice infetto e fornire informazioni forensi utili.

Una strategia di intelligence locale efficace deve comprendere i seguenti elementi:

- La Threat Intelligence deve essere acquisita e correlata dalla rete in tempo reale. Molte minacce, come le minacce avanzate persistenti (APT), possono essere rilevate solo quando una serie di eventi apparentemente non correlati e di basso livello vengono correlati e analizzati
- La Threat Intelligence deve essere acquisita dal traffico che entra ed esce (nord-sud) dalla rete, dai dati che si muovono lateralmente (est-ovest) attraverso la rete e dai dati che si muovono orizzontalmente attraverso la rete (end-to-end)
- La Threat Intelligence deve essere condivisa tra più dispositivi per una risposta coordinata. Quando soluzioni di sicurezza scollegate cercano cose diverse, avvisano in modi diversi utilizzando protocolli diversi e non sono in grado di condividere o correlare informazioni sulle minacce con altri dispositivi, la capacità di rilevare e rispondere agli attacchi è gravemente limitata
- Un singolo strumento di gestione permette una creazione di policy centralizzata, un'orchestrazione unificata e un'applicazione distribuita attraverso una varietà di soluzioni di sicurezza

Questo tipo di rilevamento e risposta cooperativo è difficile se non impossibile da raggiungere con un insieme di prodotti singoli, anche dallo stesso fornitore, se non hanno in comune intelligence, gestione e applicazione delle policy. Per rispondere in modo efficace al sofisticato panorama delle minacce di oggi, è essenziale un Security Fabric integrato e collaborativo.

Certificazione di sicurezza

La certificazione di settore è un buon indicatore dell'impegno di un fornitore ne creare e mantenere soluzioni di sicurezza efficaci. Fortinet certifica in modo aggressivo i suoi prodotti con tutte le principali organizzazioni di certificazione indipendenti, così da poter assicurare ai clienti che le proprie tecnologie rispondono a rigidi standard di sicurezza e sono conformi con i requisiti normativi, e che le proprie soluzioni sono in grado di contrastare i più recenti pericoli e vettori di minacce.

Quando esaminano le certificazioni di un vendor, è importante che le imprese siano informate su quali certificazioni forniscono valore reale. Ad esempio, vi sono diverse organizzazioni di testing e certificazione "pay to play" che, per una determinata cifra, creeranno un report che mostra che il prodotto di un determinato vendor è una soluzione di eccellenza. Tali report sono inaffidabili e Fortinet non ne fa uso.

Oltre alle certificazioni di terze parti, è possibile utilizzare ambienti di prova che consentono di rendersi conto della potenziale efficacia di una soluzione di sicurezza per il monitoraggio del particolare traffico del proprio specifico ambiente aziendale. Fortinet consiglia fortemente questo tipo di confronti, in quanto consentono di distinguere le effettive funzionalità dalle promesse di marketing.

L'intera suite di soluzioni di sicurezza Fortinet raggiunge costantemente punteggi elevati da organismi di test rigorosi e indipendenti come NSS Labs e ha ottenuto più certificazioni da enti normativi di qualsiasi altro vendor nel mercato della sicurezza.

Sicurezza – L'unione fa la forza

Il Fortinet Security Fabric consente l'interoperabilità di diverse tecnologie di sicurezza per proteggere in modo più efficace ambienti di rete in evoluzione e vincere le sfide portate da nuove minacce.

- Firewall: Fortinet fornisce una vasta gamma di soluzioni firewall leader di mercato, tra cui appliance ad alte prestazioni, firewall virtuali e opzioni cloud
- Advanced Threat Protection Framework: Fortinet ATP fornisce soluzioni di sicurezza avanzate come sandbox e sicurezza per e-mail, Web e client
- Sicurezza del data center: appliance di sicurezza ad alta velocità per il traffico nord-sud, dispositivi virtualizzati scalabili in modo dinamico per ispezionare e proteggere il traffico est-ovest e sicurezza a livello di applicazione con ispezione approfondita dei contenuti per proteggere flussi di lavoro e transazioni. Queste soluzioni sono inoltre pienamente integrate con avanzate architetture di data center SDN e ACI di nuova generazione
- Sicurezza cloud: Fortinet fornisce soluzioni per proteggere ambienti cloud privati, cloud pubblici come AWS e Azure, servizi cloud forniti da SP come XaaS, soluzioni cloud bursting e soluzioni cloud ibride on-premise/off-premise
- Secure Access Architecture: una raccolta di strumenti per il controllo degli accessi, la protezione degli switch e l'applicazione di policy, per una gestione degli accessi cablati e wireless uniforme e a elevate prestazioni
- Connected UTM: una soluzione potente per piccole e medie imprese e filiali. Le soluzioni UTM di Fortinet sono soluzioni di sicurezza unificate con gestione basata su cloud, per distribuzioni remote quando il cliente non dispone di risorse tecniche in sede

4. Utilità per l'azione

Il Fortinet Security Fabric è progettato per reagire e adattarsi alle minacce in tempo reale sfruttando threat intelligence utile all'azione. Offre funzionalità collaborative all'interno della suite di tecnologie di sicurezza di Fortinet per migliorare visibilità e risposta, il sistema operativo di sicurezza unificato FortiGate per tutte le implementazioni, per semplificare il controllo, e uno strumento di gestione e orchestrazione basato su cloud che consente un controllo centralizzato in un ambiente di rete dinamico e ampiamente distribuito.

Il Fortinet Security Fabric comprende i componenti critici seguenti:

- FortiManager: una console unificata di gestione e orchestrazione
- FortiCare: servizi di risposta per incidenti critici
- FortiCloud, FortiGuard+, Cloud FortiSandbox: estendono il Security Fabric nel cloud
- Versioni virtualizzate delle soluzioni di sicurezza Fortinet che funzionano con tutti i più importanti Hypervisor
- Integrazione completa con tutte le principali architetture SDN e cloud
- La soluzione di sicurezza più adottata dai provider di servizi per l'applicazione integrata di policy in infrastrutture on-premise e off-premise.

5. Standard aperti – Ecosistema Partner Alliance di Fortinet

Naturalmente le organizzazioni hanno già investito in un'infrastruttura di piattaforme e prodotti di rete e sicurezza che sono una parte essenziale della loro strategia di difesa. La possibilità di estendere le funzionalità e l'intelligence del Fortinet Security Fabric alle principali soluzioni di terze parti è una considerazione critica per molte imprese.

Fortinet si impegna a offrire un insieme di soluzioni di sicurezza collaborativo e interattivo. Questo è uno dei motivi per i quali siamo membri attivi della Cyber Threat Alliance e per cui abbiamo inoltre sviluppato un solido programma di partnership che mette insieme i più importanti vendor di tecnologie di sicurezza per affrontare meglio le complesse sfide delle minacce informatiche.

Fortinet ha sviluppato una serie di API che consentono ai partner Alliance di connettersi al Fortinet Security Fabric per migliorare ulteriormente la visibilità, il controllo e la reattività della vostra azienda. Questi punti di integrazione tramite API comprendono:

- Hypervisor
- Orchestrazione SDN
- Cloud
- Sandbox
- Registrazione
- Gestione policy

L'integrazione va oltre il permettere semplicemente che soluzioni di terze parti acquisiscano o reindirizzino dati e traffico. Le soluzioni Alliance che si integrano con il Fortinet Security Fabric sono in grado di acquisire e condividere attivamente informazioni sulle minacce e istruzioni di attenuazione per migliorare la Threat Intelligence, aumentare la visibilità complessiva delle minacce ed ampliare la risposta alle minacce a tutti gli ambienti interessati.

In sintesi

L'evoluzione della rete aziendale e la sua transizione in un modello di business digitale è oggi uno degli aspetti più problematici della sicurezza di rete. Poiché importanti tendenze nel campo dell'elaborazione e dei servizi di rete continuano a introdurre cambiamenti in molte infrastrutture, architetture e pratiche aziendali critiche, le imprese sono alla ricerca di soluzioni innovative per la sicurezza della rete che consentano loro di adattarsi a questi cambiamenti.

Il Fortinet Security Fabric può fornire la scalabilità, la sicurezza, la visibilità, l'intelligence e la strategia API aperta di cui l'impresa ha bisogno, introducendo sicurezza, flessibilità, scalabilità, collaborazione, adattabilità e gestibilità negli ambienti fisici, virtuali e cloud, con una copertura completa.

Per maggiori informazioni sul Fortinet Security Fabric, visitare il sito Web all'indirizzo http://www.fortinet.com/aboutus/why-fortinet.html

Italia - Roma
Via del Casale Solaro, 119
00143 Roma
Italia
Vendite: +39 06-51573-330

Italia - Milano
Centro Torri Bianche Palazzo Tiglio
20871 Vimercate (MB)
Italia
Tel: +39 039 687211

SEDI GLOBALI
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stati Uniti
Tel: +1.408.235.7700
www.fortinet.com/sales

UFFICIO VENDITE EMEA
905 rue Albert Einstein
Valbonee
06560, Alpes-Maritimes,
Francia
Tel: +33.4.8987.0500

UFFICIO VENDITE APAC
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

UFFICIO VENDITE AMERICA LATINA
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
Messico D.F.
Tel: 011-52-(55) 5524-8428

venerdì 22 aprile 2016