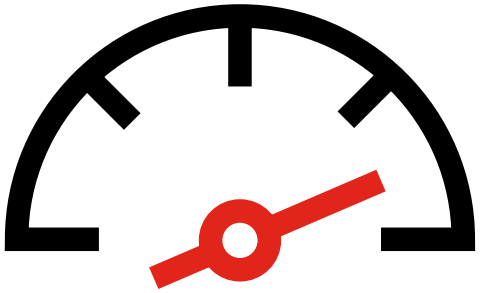
Le minacce informatiche riescono a oltrepassare le tue difese? Security-Driven Networking può porre un freno a tutto questo

Sommario

Sintesi preliminare

Prima che il COVID-19 si abbattesse sul mondo, le aziende di ogni forma e dimensione erano già impegnate nel processo di trasformazione digitale. La trasformazione digitale è "un termine onnicomprensivo utilizzato per descrivere l'implementazione di nuove tecnologie, talenti e processi al fine di migliorare le operazioni aziendali".[1] Oggi, al di là della pandemia, la maggior parte delle organizzazioni sta accelerando le proprie iniziative di business digitale[2] per soddisfare le esigenze di una forza lavoro ibrida, che lavora da qualsiasi luogo. Questo nuovo approccio si chiama accelerazione digitale.

Una delle problematiche dell'accelerazione digitale è l'aggiunta di nuovi perimetri di rete, che sta creando nuove vulnerabilità che, a loro volta, riescono a oltrepassare la capacità dei team di sicurezza IT di proteggere l'azienda dalle minacce informatiche. Per fortuna, esiste una potente strategia, denominata security-driven networking che può contribuire a fortificare le organizzazioni in modo che possano contare su una maggiore sicurezza e compiere con successo i loro sforzi di accelerazione digitale.



“Il 69% dei consigli di amministrazione ha accelerato le proprie iniziative di business digitale in seguito all’impatto del COVID-19”.[3]

Introduzione

La forza lavoro ibrida e il lavoro agile di oggi richiedono l'accesso ad applicazioni distribuite in data center, ambienti multi-cloud e sedi SaaS. Al contempo, questi dipendenti si spostano tra sedi on-premise, filiali interconnesse, uffici domestici e luoghi temporanei durante le trasferte, ma hanno ancora bisogno e si aspettano esperienze utente coerenti e senza interruzioni. Il passaggio ad applicazioni distribuite e a una forza lavoro agile comporta una superficie di attacco in espansione che espone l'azienda a nuove minacce.

Poiché la maggior parte delle architetture di rete tradizionali è stata realizzata utilizzando prodotti monofunzionali, disparati e distribuiti staticamente, che forniscono un accesso implicito a tutte le applicazioni, il risultato si è rivelato disastroso. Ransomware, phishing, botnet e altre attività criminali sono ormai ai massimi storici.

È necessario un nuovo approccio per fornire un accesso sicuro alle risorse critiche su larga scala. In questo eBook, verranno illustrati gli strumenti e le integrazioni chiave per la rete, la sicurezza e le operazioni necessari per implementare una Security-Driven Networking efficace con la strategia del perimetro zero-trust.

Security-Driven Networking e convalida della strategia del perimetro zero-trust

Si pone un serio problema quando l'esperienza dell'utente è ostacolata e rallentata dal traffico reindirizzato per l'ispezione a strumenti di sicurezza fissi che non possono esaminare adeguatamente i flussi di applicazioni, dati e video crittografati. Inoltre, quando le soluzioni di sicurezza informatica non sono integrate e non riescono a interagire tra loro per assicurare protezione da tutte le minacce rilevate, le cose possono peggiorare ulteriormente per la forza lavoro ibrida.

Per risolvere questi problemi, la rete e la sicurezza stanno convergendo in un approccio chiamato Security-Driven Networking. Questa convergenza deve essere disponibile in modo coerente su tutti i perimetri al fine di offrire una migliore esperienza utente e un Application Control ottimizzato.

Dobbiamo verificare ogni tentativo

Un'altra esigenza che dovrebbe far parte di ogni Security-Driven Networking è la strategia del perimetro zero-trust. Una strategia di accesso zero-trust si basa sull'idea che nulla (nessun utente, nessun dispositivo, nessun sistema, nessuna rete, nessun servizio) che operi al di fuori o all'interno del perimetro di sicurezza debba essere considerato attendibile. Dobbiamo invece verificare tutto quello che tenta di accedere alla rete.

Non è più accettabile verificare un utente o un dispositivo solo una volta al livello del perimetro. Oggi è necessaria una verifica continua e più dinamica di ogni utente, dispositivo, applicazione e transazione. Il perimetro zero-trust è una strategia che le organizzazioni possono distribuire in modo olistico per tutti i perimetri, gli utenti e le applicazioni, utilizzando una convergenza coerente di tecnologie di rete e di sicurezza.

Componenti chiave necessari per ottenere un'accelerazione digitale sicura

Sicurezza per perimetri e utenti

Protezione coerente e coordinata basata su IA/ML su tutti i perimetri della rete con NGFW

La superficie di attacco si sta espandendo a causa della crescita esponenziale dei perimetri nelle architetture IT ibride. Questo non rappresenta solo una minaccia per l'accelerazione digitale, ma è necessaria anche una protezione automatizzata dalle minacce per far sì che le operazioni possano essere continuamente svolte senza intoppi. I Next-Generation Firewall (NGFW) necessitano di threat intelligence che sfrutti l'intelligenza artificiale (IA) e il machine learning (ML) per agire come moltiplicatori di forza e accelerare la prevenzione, il rilevamento e la risposta alle minacce per gli attacchi noti, zero-day e sconosciuti.

Inoltre, con la quasi totalità del traffico Internet ormai crittografato, gli utenti malintenzionati possono trovare il modo di entrare o uscire da una rete nascondendosi nella crittografia. Le organizzazioni non possono più disattivare l'ispezione SSL per evitare un calo delle prestazioni. È necessaria una soluzione sufficientemente potente da fornire una visibilità completa ad alta fedeltà su tutti i percorsi protetti, rilevare le minacce con la decrittografia SSL, compresa TLS 1.3, e fornire una protezione automatica dalle minacce. Queste soluzioni devono essere distribuite in modo flessibile in qualsiasi punto dell'azienda: filiale distribuita, campus, data center e cloud.

Il traffico crittografato ha raggiunto il 95%.[4]

Segmentazione della rete per isolare il traffico est-ovest

Per anni, i leader della sicurezza di rete hanno risposto agli attacchi informatici mettendo a punto solide difese perimetrali all'esterno per prevenire gli attacchi e segmentando le reti all'interno per i controlli operativi. Ma una volta che il perimetro è stato compromesso, gli hacker possono aggirarsi liberamente e creare scompiglio sottraendo dati o interrompendo le attività aziendali finché non viene pagato un riscatto.

Ecco cosa serve:

- La sicurezza on-premise è necessaria per proteggere il traffico est-ovest.
- Poiché le soluzioni firewall fornite solo nel cloud non sono sufficienti, la convergenza coerente di un NGFW on-premise e cloud è fondamentale per fornire il massimo livello di protezione.
- Le organizzazioni devono creare strutture di segmentazione dinamica che isolino le applicazioni e gli utenti business-critical.
- Il controllo dinamico degli accessi deve verificare continuamente gli utenti e i dispositivi.
- Applicazioni raggruppate e interconnesse tra loro secondo una solida strategia di difesa che consente solo la comunicazione est-ovest e nord-sud attraverso l'ispezione di sicurezza e la protezione tramite micro-segmentazione.

Protezione degli utenti remoti con SASE erogato nel cloud

La tecnologia SASE (Secure Access Service Edge) distribuita nel cloud deve fornire FWaaS, CASB (Cloud Access Security Broker) in-line, Web Filtering, sicurezza DNS, antivirus, antimalware, anti-botnet, ispezione SSL e prevenzione della perdita di dati (DLP, Data Loss Prevention) per assicurare un accesso remoto sicuro. Tutto questo consente di adottare una solida strategia di difesa con più livelli di difesa, fornendo una protezione a tutto spettro contro le minacce note e zero-day su larga scala. In questo modo, gli utenti remoti possono adottare un solido approccio di sicurezza Web. Supporta opzioni di distribuzione flessibili, da quelle basate su agenti a quelle senza agenti, offrendo una sicurezza Web coerente su rete, endpoint e cloud. Fornisce inoltre un onboarding semplice con l'impostazione automatica del proxy e la gestione dei certificati, oltre a offrire registrazioni ed eventi granulari per una risoluzione efficiente dei problemi e delle operazioni.

Le capacità chiave devono includere:

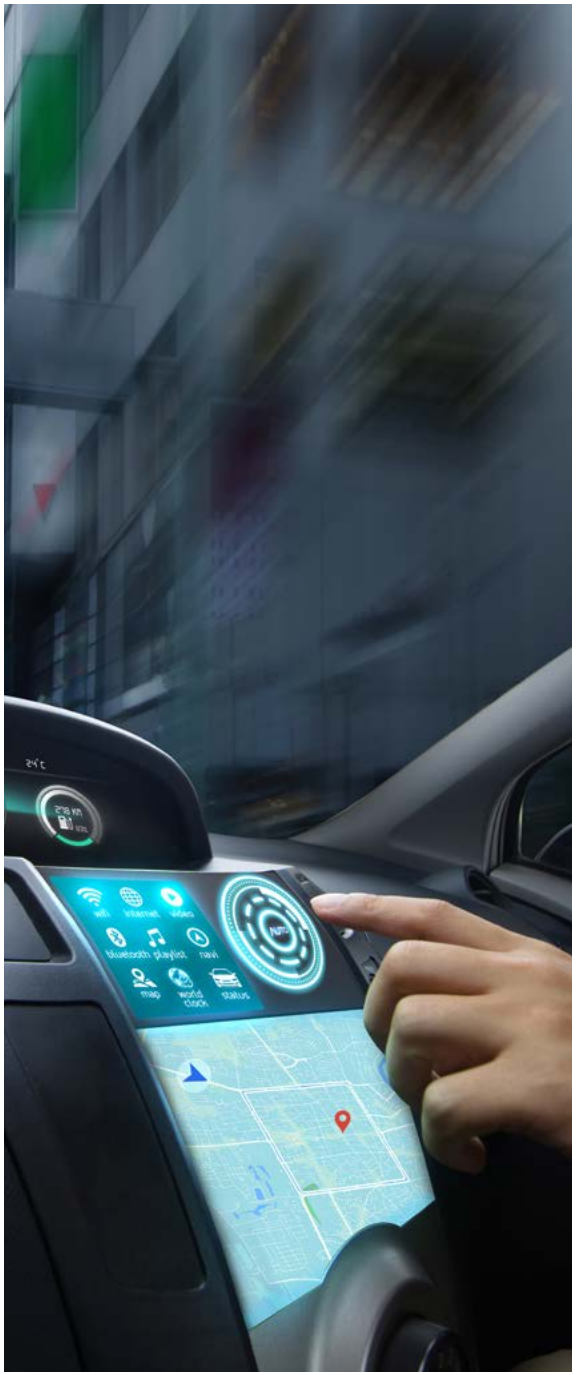
- **Accesso sicuro a Internet.** Connetti in sicurezza tutti gli utenti e i dispositivi remoti, compresi i dispositivi IoT (Internet-of-Things) headless, senza necessità di installare agenti. Tutto questo offre una sicurezza Web completa per una protezione in tempo reale contro minacce precedentemente sconosciute.
- **Rilevamento e protezione dei dati sensibili.** Evita lo shadow IT e l'esfiltrazione dei dati con CASB in-line per una copertura completa. Rileva, monitora e controlla le applicazioni autorizzate e non autorizzate.
- **Controllo dell'approccio zero-trust ovunque.** L'accesso ZTNA (Zero-Trust Network Access) integrato in modo nativo consente alle organizzazioni di passare da un'attendibilità implicita a un accesso esplicito per applicazione basato sull'identità e sul contesto con una convalida continua. In questo modo, è possibile controllare con efficacia chi e cosa si trova nella rete o persino controllare i dispositivi fuori rete.

Innovazioni di rete che favoriscono l'accelerazione digitale

SD-WAN

L'accelerazione digitale, il lavoro agile e i gli attacchi informatici avanzati stanno determinando cambiamenti nella tradizionale architettura WAN incentrata su router, hub-and-spoke e solidamente MPLS, creando un'esperienza utente insoddisfacente, una sicurezza inefficace e operazioni complesse.

Per essere efficiente sotto ogni punto di vista, una soluzione SD-WAN (Software-Defined Wide-Area Networking) deve disporre di una sicurezza NGFW integrata. Deve inoltre includere funzioni avanzate di routing e proxy di accesso ZTNA.
Il tutto deve convergere in un'unica soluzione per semplificare la gestione. La soluzione deve essere abbastanza potente da gestire tutti i controlli di sicurezza e le funzioni SD-WAN, rispettando le prestazioni previste.

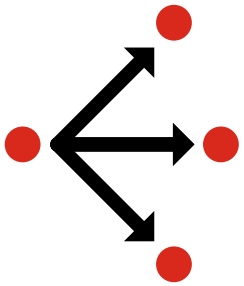


I vantaggi principali di SD-WAN, NGFW e routing avanzato sono la capacità di:

- **Offrire un'esperienza utente di qualità superiore** su qualsiasi scala, selezionando il percorso più adatto per le principali applicazioni aziendali
- **Accelerare la convergenza di rete e sicurezza** e semplificare l'architettura WAN
- **Raggiungere l'efficienza operativa** attraverso l'automazione, l'analisi approfondita e l'auto-riparazione, nonché orchestrare criteri di rete e di sicurezza coerenti
- **Assicurare un ROI migliore** passando da un modello tradizionale basato su router a un'architettura avanzata basata su SD-WAN.

La giusta soluzione SD-WAN sarà in grado di:

- **Ottimizzare l'esperienza della forza lavoro ibrida.** Migliora l'esperienza di lavoro agile e l'approccio di sicurezza con criteri di sicurezza coerenti e accesso esplicito per applicazione su tutti i perimetri.
- **Migliorare la connettività ibrida e multi-cloud.** Offri connettività sicura, continua e più veloce, verso il cloud, all'interno del cloud e tra i cloud con un'unica macchina virtuale (VM), semplificando la gestione, riducendo l'ingombro e consentendo l'orchestrazione della rampa di accesso al cloud.
- **Far convergere WAN e sicurezza.** Offri SD-WAN, NGFW, routing avanzato e proxy di accesso ZTNA integrati in un'unica soluzione per proteggere l'intera superficie di attacco digitale.



“Entro la fine del 2023, il 60% delle aziende avrà implementato la SDWAN, rispetto a meno del 20% nel 2019, per aumentare l’agilità della rete e migliorare il supporto per le applicazioni cloud”.[5]

WAN wireless LTE/5G

Man mano che le aziende adottano le tecnologie cloud e si allontanano dalle reti MPLS nella loro continua ricerca di accelerazione digitale, è necessario affrontare tutta una serie di problematiche. Ad esempio, Internet come mezzo di connettività aziendale è opaco e spesso inattendibile, rendendo difficile per l'IT offrire un'esperienza di alta qualità agli stakeholder. Inoltre, le linee fisiche via cavo/ADSL/fibra hanno una portata limitata, impedendo alle aziende di distribuire la banda larga in ogni filiale. Infine, l'apertura di numerose filiali alla connettività Internet diretta presenta una moltitudine di rischi di gestione e di sicurezza per l'azienda, poiché i perimetri della rete si moltiplicano.

È necessario un gateway cellulare sicuro che fornisca una WAN wireless LTE/5G per una connettività perimetrale ultraveloce, affidabile e diffusa verso il cloud. Questi gateway sono dotati della più recente tecnologia LTE/5G per trasformare la connettività delle filiali, indipendentemente dalla loro prossimità al cavo/ADSL/fibra.

Devono inoltre includere opzioni dual SIM e dual modem per garantire un rapido failover cellulare e High Availability. La gestione fuori banda garantisce la Business Continuity per un ROI ottimale.

Un gateway cellulare sicuro può essere utilizzato nei seguenti modi:

- **LTE/5G come collegamento WAN primario della filiale.** Consente un accesso diretto e affidabile a Internet nelle filiali senza accesso a cavo/ADSL/fibra. È ideale per scuole, ospedali o negozi al dettaglio, sedi industriali ed eventualmente flotte mobili e ambienti esterni.
- **Failover LTE/5G.** È possibile fornire una maggiore affidabilità della banda larga laddove l'operatività è un elemento di fondamentale importanza. I luoghi di utilizzo vanno dai negozi al dettaglio con elevati flussi di clienti ai siti industriali e di pubblica utilità, agli ospedali, alle scuole e ai luoghi di intrattenimento.
- **Sicurezza dei breakout locali della tecnologia LTE/5G.** La sicurezza può essere applicata alle filiali che si aprono a Internet.

Soluzione per il perimetro della LAN (switch e access point sicuri)

La rete locale cablata e wireless (LAN) costituisce la spina dorsale dell'IT: consente di eseguire applicazioni di nuova generazione e aumentare la produttività degli utenti. La LAN influisce notevolmente sull'esperienza degli utenti ed è l'inizio o la fine di molti eventi di sicurezza che si verificano in azienda.

Una moderna soluzione per il perimetro della LAN deve far convergere la sicurezza con gli switch e gli access point (AP) per assicurare un'esperienza utente sicura e senza interruzioni. La combinazione di un NGFW con prodotti Wi-Fi ed Ethernet riduce la complessità della rete e migliora la sicurezza. Una soluzione LAN deve essere in grado di identificare quello che è connesso alla rete per implementare l'accesso zero-trust.

Una soluzione per il perimetro della LAN Security-Driven Networking deve fornire:

- **Gestione unificata.** Il livello di accesso cablato e wireless, insieme ai controlli di sicurezza, deve essere gestito con un'unica interfaccia.
- **Scalabilità completa.** Le porte di accesso impilabili da 1, 10 e 40 GE con uplink fino a 100 GE devono essere disponibili per la scalabilità dal desktop al data center.
- **Provisioning zero-touch.** Il provisioning automatico delle apparecchiature con rilevamento automatico, VLAN globale, criteri di sicurezza, interfacce firewall e porte Ethernet deve essere semplice.
- **Controllo degli accessi alla rete.** La LAN deve essere in grado di identificare i dispositivi aziendali e IoT e determinare il loro livello di privilegio o di accesso alla rete.

"Entro il 2024, l'80% delle imprese dovrà trasformare le proprie reti e i propri processi per offrire esperienze online ricche di contenuti multimediali più personalizzate e interattive, in grado di soddisfare le aspettative dei clienti".[6]

Operazioni NOC semplificate per l'accelerazione digitale

Automazione e gestione centralizzata

Le operazioni manuali mettono un freno all'efficienza operativa. Non solo sono soggette a errori e rallentamenti, ma causano anche violazioni, vanificando lo scopo di creare una rete attendibile. L'architettura del perimetro zero-trust necessita di visibilità su tutte le sedi, gli utenti, i dispositivi e le applicazioni. Senza questa visibilità, le organizzazioni non potranno contare su informazioni approfondite o sulla capacità di agire sulle loro operazioni.

Uno strumento di gestione NOC deve consentire alle organizzazioni di ridurre al minimo gli errori umani, automatizzare la risposta alle minacce e fornire una strategia zero-trust con una gestione centralizzata. L'automazione DevSec e criteri di sicurezza coerenti tra gli ambienti ibridi e multi-cloud aumentano l'efficienza operativa e la protezione.

È necessario cercare le seguenti capacità in uno strumento di gestione NOC:

- **Gestione centralizzata.** Controlla i criteri di rete e di sicurezza in tutta la rete in un'unica console di gestione.
- **Automazione degli scambi di dati.** Supporta il trasferimento automatico di informazioni tra il SOC e le applicazioni e i servizi aziendali esistenti.
- **NOC basato sull'automazione.** Semplifica le operazioni del giorno zero e ottimizza la risoluzione dei problemi del primo e del secondo giorno con tecnologie avanzate come AIOps per le operazioni IT.
- **Semplificazione delle operazioni.** Semplifica il flusso di lavoro operativo dell'IT ibrido.

Monitoraggio dell'esperienza digitale (DEM, Digital Experience Monitoring)
La migrazione al cloud, il SaaS e il lavoro agile assicurano dinamicità all'azienda e la corretta distribuzione dei dipendenti, i quali restano sempre connessi digitalmente. Le organizzazioni non possiedono più l'infrastruttura su cui transita il traffico, ma sono comunque responsabili dell'esperienza utente end-to-end. DEM supporta le moderne richieste dei team NetOps di spostare la loro attenzione dal tradizionale monitoraggio delle prestazioni all'accelerazione della disponibilità delle applicazioni dalle reti interne ed esterne. La modernizzazione degli strumenti di monitoraggio delle prestazioni, che sono frammentati, con una piattaforma DEM completa, consente di ottenere una visibilità end-to-end sull'esperienza complessiva dell'utente, indipendentemente dal luogo in cui risiede o è ospitata l'applicazione.

Una soluzione DEM consente alle organizzazioni di:

- **Monitorare al perimetro.** La trasformazione digitale ha modernizzato l'infrastruttura aziendale con i perimetri della rete e dei carichi di lavoro, mentre il monitoraggio tradizionale delle prestazioni è rimasto nel data center centrale. DEM offre visibilità end-to-end monitorando i perimetri per migliorare la produttività dei dipendenti.
- **Fruire della visibilità delle applicazioni business-critical utilizzate dai dipendenti.** Le applicazioni incentrate sul business si sono spostate nel cloud e l'adozione di SaaS è in crescita. Tuttavia, i team NetOps non hanno visibilità sull'esperienza dei dipendenti. I DEM consentono ai team NetOps di garantire che l'esperienza digitale dei dipendenti sia produttiva per l'azienda.
- **Soddisfare e superare gli SLA.** Soddisfare gli accordi sui livelli di servizio (SLA) è fondamentale per la maggior parte delle aziende, ma ci sono molti punti ciechi in termini di esperienza dell'utente soddisfacente. Una DEM può testare continuamente gli utenti con un'esperienza applicativa in tutto il mondo, non solo per soddisfare, ma anche per superare gli SLA, migliorando al contempo la soddisfazione dei clienti.

L’approccio esclusivo di Fortinet

Fortinet ha un approccio innovativo alla sicurezza dell’accelerazione digitale grazie all’utilizzo della strategia del perimetro zero-trust con la convergenza di rete e sicurezza di classe enterprise.

Questa capacità esclusiva assicura un accesso sicuro alle applicazioni e alle risorse critiche, sia che gli utenti si trovino on-premise sia che accedano alle risorse tramite il cloud. Il nostro approccio di rete orientato alla sicurezza, che comprende una combinazione unica di ASIC esclusivi realizzati appositamente, soluzioni di sicurezza distribuite nel cloud e funzionalità di rete integrate, offre un’esperienza utente di livello superiore, unita a una protezione coordinata dalle minacce per ogni perimetro della rete.

Perimetro zero-trust La strategia risolve una delle problematiche più persistenti che i team IT di oggi devono affrontare: estendere la sicurezza di classe enterprise e il controllo granulare degli accessi ai telelavoratori. La soluzione di Fortinet fornisce un approccio unico nel suo genere per soddisfare al meglio le esigenze degli utenti, offrire tecnologie di rete/sicurezza efficienti e risolvere le problematiche di attendibilità implicita che creano ostacoli alle organizzazioni che cercano di perseguire un percorso di accelerazione digitale.

[1] Clint Boulton, "What is digital transformation? A necessary disruption", CIO, 24 giugno 2021.

[2] "Gartner Says 69% of Boards of Directors Accelerated Their Digital Business Initiatives Following COVID-19 Disruption", Gartner, 30 settembre 2020.

[3] Ibid.

[4] "HTTPS encryption on the web", Google Transparency Report, visitato il 10 marzo 2022.

[5] Gaspar Valdivia, Lisa Unden-Farboud, To Chee Eng, Grigory Betskov e Susanna Silvennoinen, "Forecast Analysis: Enterprise Networking Connectivity Growth Trends, Worldwide", Gartner, 20 settembre 2019.

[6] Paul Hughes, Carrie MacGillivray, Rohit Mehra, Ghassan Abdo, Brandon Butler, Ajeet Das, James Eibisch, Mark Leary, Courtney Munroe e Leslie Rosenberg, "IDC FutureScape: Worldwide Future of Connectedness 2022 Predictions", International Data Corporation, 7 dicembre 2021.

FORTINET®

www.fortinet.com

luglio 27, 2022 9:06 AM

1452320-0-0-IT