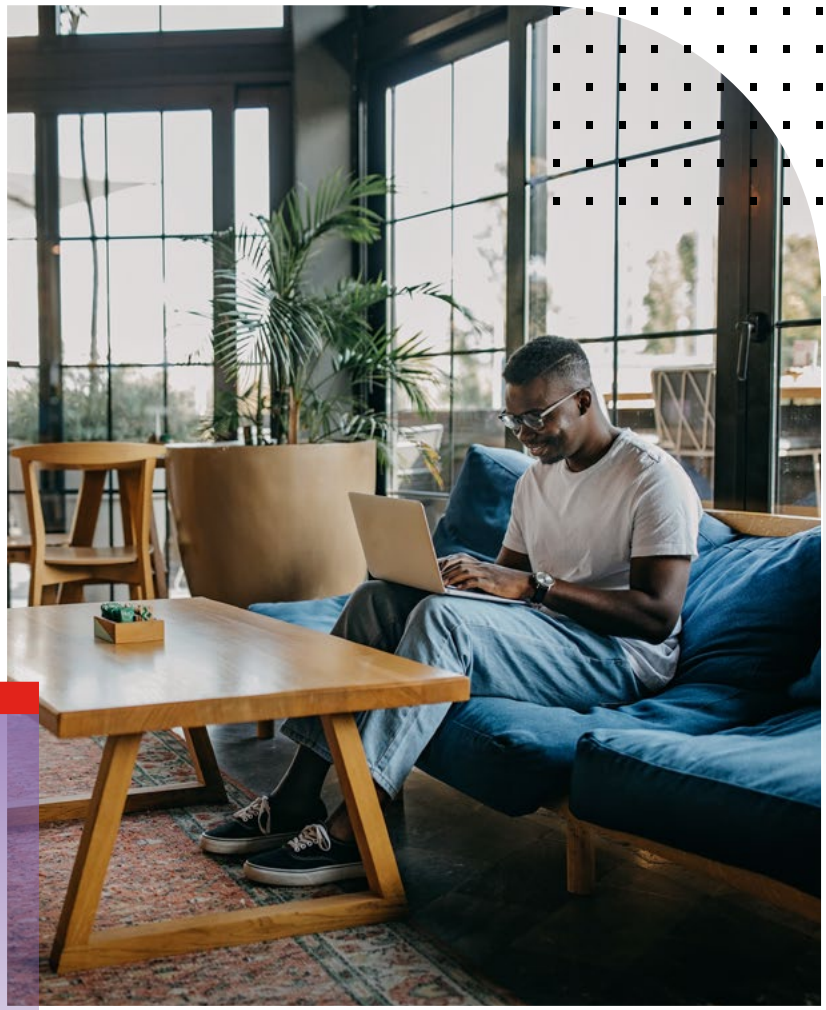
WHITE PAPER

Semplicità e sicurezza per il lavoro agile

Una soluzione per proteggere utenti e dati ovunque si trovino



Sintesi preliminare

Nell'ultimo decennio o giù di lì, la tecnologia si è evoluta costantemente per dare ai lavoratori più flessibilità nei dispositivi che usano, nei luoghi da cui possono lavorare e nelle risorse a cui possono accedere. La filosofia BYOD (Bring your own device) e l'accesso alle applicazioni cloud sono stati i primi passi verso la diffusione del lavoro flessibile.

Anche se le imprese avevano già pianificato l'adozione di una vera strategia di lavoro agile nel giro di qualche anno, la pandemia da COVID-19 ha accelerato il processo. E ora sempre più lavoratori chiedono ai propri datori di poter lavorare da remoto. La sfida è come offrire un'esperienza di lavoro ibrida che garantisca produttività e sicurezza.

Secondo il Global Threat Landscape Report, gli incidenti ransomware sono aumentati di quasi il 1100% da giugno 2020 a giugno 2021.[1]

Proteggere una forza lavoro ibrida

Quando è scoppiata la pandemia, erano poche le aziende preparate a supportare il lavoro remoto. Da un giorno all'altro, i dipendenti hanno cominciato a collegarsi all'ufficio da reti domestiche con standard di sicurezza scadenti. I controlli di accesso erano inadeguati e i dispositivi endpoint vulnerabili. Non sorprende che i cybercriminali abbiano prontamente approfittato di queste debolezze. È un fatto che, come rilevato recentemente da Forrester, il 67% delle organizzazioni abbia subito un attacco informatico con impatto sul business attribuibile a vulnerabilità create dal lavoro remoto.[2]

Guardando al futuro, molte aziende prevedono di consentire a molti dei loro dipendenti di continuare a lavorare almeno in parte da remoto. Avendo già investito in strumenti e soluzioni per supportare la produttività dei dipendenti fuori dall'ufficio, non hanno motivo di negare a chi preferisce lavorare a distanza la possibilità di continuare a farlo.

Emerge quindi la figura del lavoratore ibrido, che va in ufficio in certi giorni della settimana e lavora da casa o da altri posti negli altri giorni. Questi lavoratori e i loro dispositivi devono potersi spostare tra i vari ambienti senza interruzioni nella produttività. Ovunque si trovino, devono essere in grado di accedere in modo sicuro ad applicazioni e risorse presenti nel cloud o nel data center.

Per supportare il lavoro da qualsiasi luogo, le organizzazioni devono pensare alla sicurezza e implementare soluzioni che siano in grado di seguire, supportare e proteggere gli utenti ovunque si trovino. Servono funzioni di sicurezza sull'endpoint, combinate all'accesso zero-trust (ZTA) e all'accesso di rete zero-trust (ZTNA). Serve anche una connettività sicura supportata da funzionalità SD-WAN (Software-Defined Wide-Area Networking) e SASE (Secure Access Service Edge). I motori di policy devono controllare adeguatamente gli accessi in base all'identità e alla posizione degli utenti e dei dispositivi, al tipo di dispositivo e alla strategia di sicurezza, per stabilire un accesso sicuro.

La sfida che la maggior parte delle organizzazioni deve affrontare è cercare di supportare il lavoro agile utilizzando prodotti di decine di fornitori indipendenti. Un fornitore potrebbe provvedere alla protezione degli endpoint (EPP), un altro al rilevamento e alla risposta degli endpoint (EDR), un altro all'identità e così via. Possono anche esservi diversi fornitori di firewall distribuiti nel data center, nelle filiali e sulle varie piattaforme cloud utilizzate. Creare una soluzione coesa e affidabile con così tanti fornitori è quasi impossibile. Le organizzazioni finiscono per ricorrere a complessi espedienti per riuscire in qualche modo a far funzionare insieme le diverse soluzioni. E la manutenzione di questi sistemi richiede notevoli risorse e tempo ai reparti IT.

Un approccio migliore è quello di distribuire soluzioni facenti parte di un'architettura di piattaforma mesh di sicurezza informatica completamente integrata. Questo approccio offre una sicurezza più robusta, una gestione e un'orchestrazione più facili e un migliore costo totale di proprietà rispetto alle soluzioni che operano separatamente.

Protezione ovunque

Il supporto del lavoro ovunque richiede funzioni di sicurezza efficaci sia che l'utente lavori dall'ufficio aziendale, da un ufficio domestico o mentre è in viaggio e non si trova nell'ufficio aziendale o domestico. Ognuno di questi luoghi pone delle sfide e richiede una determinata tecnologia di sicurezza per una protezione completa.

Nel sondaggio globale sul ransomware di Fortinet, il 67% delle organizzazioni riferisce di avere subito un attacco ransomware.[3]

Lavoro dall'ufficio

Poiché le aziende si affidano ad applicazioni per condurre la loro attività, proteggere l'accesso a tali applicazioni, le reti per connettersi ad esse e i dispositivi che le eseguono permane un aspetto essenziale di una difesa a più livelli anche quando il dipendente lavora da un tradizionale ufficio aziendale. Negli uffici aziendali si trovano in genere tutte le risorse che fanno gola agli hacker: dati dei clienti, server, applicazioni, informazioni sulle identità, credenziali degli utenti e codice sorgente. La sicurezza di utenti, dispositivi e server in ufficio inizia con i firewall di prossima generazione (NGFW), che costituiscono la prima linea di difesa di questa raccolta di informazioni critiche. Agli NGFW le aziende devono poi aggiungere una combinazione integrata di sicurezza degli endpoint, zero-trust e gestione delle identità:

- NGFW, che proteggono gli accessi esterni all'azienda con funzionalità di sicurezza avanzate e uniformi nei campus, nei data center, nelle filiali e negli ambienti cloud;
- servizi di identità e agenti ZTNA, che controllano e proteggono l'accesso alle applicazioni e ad altre risorse. Le soluzioni ZTNA assicurano il controllo interno sorvegliando l'accesso alle applicazioni, i tunnel crittografati in ufficio e le verifiche degli utenti;
- tecnologie per la sicurezza degli endpoint, come EDR, per la protezione di utenti e dispositivi. La tecnologia EDR consente di proteggere i dispositivi degli utenti e interagisce con i dati critici.

Gli ambienti di ufficio devono anche includere soluzioni di rete e di sicurezza, come Secure SD-WAN, che offrono strumenti di rete avanzati, progettati per operare da una piattaforma di sicurezza unificata che ottimizza la connettività WAN tra data center, cloud, filiali e sedi di campus con intelligence application-aware.

Lavoro da casa

I dipendenti che operano in modalità remota o ibrida solitamente si collegano da un ambiente home office con un laptop, un monitor e una webcam esterna. Tuttavia, queste reti domestiche sono spesso protette in modo insufficiente da router wireless economici e potrebbero comprendere dispositivi IoT (Internet of Things) vulnerabili, che possono fungere da via d'accesso per gli hacker. I dipendenti che utilizzano reti domestiche incontrano inoltre difficoltà in caso di videoconferenze e altre attività caratterizzate da flussi elevati di dati. La produttività dei lavoratori può essere influenzata negativamente se le altre persone che si trovano in casa, che siano familiari o conviventi, consumano larghezza di banda con videostreaming o giochi online. Chi lavora da casa ha bisogno di:

- tecnologie per la sicurezza degli endpoint, come EDR, per la protezione di utenti e dispositivi;
- servizi di identità e agenti ZTNA, che controllano e proteggono l'accesso alle applicazioni e ad altre risorse;
- sicurezza di classe enterprise per le reti domestiche per garantire un accesso sicuro alla rete aziendale e alle applicazioni nel cloud e nel data center. Deve includere la gestione del traffico per dare priorità al traffico aziendale rispetto al videostreaming o al gaming.

Una soluzione per l'home office deve estendere le protezioni del firewall aziendale all'intera rete domestica. Deve anche segmentare la rete domestica per consentire al team IT di controllare tutto il traffico aziendale e ottimizzare la larghezza di banda per le applicazioni aziendali, garantendo al contempo la privacy dei dipendenti per la sezione della rete non utilizzata per lavoro.

Lavoro in viaggio

Gli utenti che viaggiano o lavorano al di fuori dell'ufficio aziendale o del loro spazio remoto primario si trovano spesso in ambienti esposti a minacce particolari. Quando gli utenti mobili si connettono alle applicazioni e alle risorse di cui hanno bisogno per svolgere il loro lavoro, possono utilizzare reti e punti di accesso sconosciuti e non protetti, che potrebbero essere utilizzati per compromettere la rete. Chi lavora in mobilità ha bisogno di:

- tecnologie per la sicurezza degli endpoint, come EDR, per utenti e dispositivi;
- servizi di identità e agenti ZTNA, che controllano e proteggono l'accesso alle applicazioni e ad altre risorse;
- soluzioni SASE per la sicurezza delle reti remote, che offrono funzionalità firewall basate su cloud per proteggere i dipendenti lontani dalla rete aziendale o domestica.

Una soluzione per reti mobili deve includere l'autenticazione a più fattori, nonché un gateway SWG (Secure Web Gateway) basato sul cloud e un servizio CASB (Cloud Access Security Broker).

Sicurezza integrata per il lavoro agile, supportata dalla threat intelligence

Per supportare il lavoro agile, le organizzazioni devono individuare una piattaforma mesh di sicurezza informatica con soluzioni progettate per funzionare come un sistema integrato, con threat intelligence fruibile per mantenere gli strumenti di sicurezza aggiornati con i dati più recenti e preparati con informazioni di identificazione e protezione dalle minacce in qualsiasi luogo. Questo tipo di approccio mediante piattaforma consente di unificare la sicurezza di rete, zero trust ed endpoint grazie a un insieme comune di API (Application Programming Interface) e punti di integrazione, per fare in modo che gli utenti possano passare senza problemi da un posto all'altro sperimentando sempre lo stesso ambiente sicuro. E sul lato IT, il mesh di sicurezza informatica semplifica la creazione e l'applicazione delle policy, rende uniformi le configurazioni, centralizza la gestione e consente il monitoraggio e il controllo di utenti, dispositivi, dati, applicazioni e flussi di lavoro.

Il lavoro da qualsiasi luogo è diventato più importante a causa della recente pandemia, ma questa ha solo accelerato una tendenza che era già in atto. L'ambiente di lavoro ibrido è destinato a restare e le organizzazioni devono assicurarsi di essere pronte a utilizzare in modo sicuro questo modello di lavoro.

[1] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, agosto 2021.

[2] "Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work," Forrester, 2021

[3] "The 2021 Ransomware Survey Report," Fortinet, 3 novembre 2021.

FORTINET

www.fortinet.com

maggio 23, 2022 4:44 p.
1400814-0-0-IT