Quattro considerazioni critiche per la progettazione dell'architettura di sicurezza

Introduzione al Fortinet Security Fabric per una sicurezza ampia, integrata e automatizzata

Sommario

Panoramica preliminare

Le organizzazioni stanno rapidamente adottando iniziative di innovazione digitale (DI, Digital Innovation) per accelerare il loro business, ridurre i costi, migliorare l'efficienza e fornire una migliore esperienza ai clienti. Per ottenere risultati di innovazione digitale, riducendo al minimo la complessità e gestendo i rischi in tutta efficacia, le organizzazioni devono adottare una piattaforma di sicurezza informatica che garantisca visibilità dell'intero ambiente e i mezzi per gestire facilmente sia la sicurezza che le operazioni di rete.

Fortinet Security Fabric risolve queste problematiche con soluzioni ampie, integrate e automatizzate che consentono di realizzare reti basate sulla sicurezza, accesso alla rete zero-trust, sicurezza dinamica del cloud e operazioni di sicurezza basata su intelligenza artificiale (IA). L'offerta Fortinet è arricchita da un ecosistema di prodotti di terzi perfettamente integrati che riducono al minimo le lacune delle architetture di sicurezza aziendali, sfruttando al massimo il ritorno sull'investimento (ROI).

L'84% dei responsabili della sicurezza ritiene che il rischio di attacchi informatici aumenterà.[1]

L’innovazione digitale sta trasformando tutti i settori

In tutti i settori economici del mondo, l’innovazione digitale è vista come un imperativo per la crescita del business e per migliorare l’esperienza dei clienti.[2]

Dal punto di vista dei leader IT e della sicurezza informatica dei cloud service provider, l’innovazione digitale si traduce in un’ampia gamma di cambiamenti nei loro ambienti di rete. Gli utenti sono sempre più mobili e accedono alla rete da luoghi ed endpoint che non sempre sono sotto il controllo dell’IT aziendale. Si collegano anche direttamente ai cloud pubblici per utilizzare le principali applicazioni aziendali, come Office 365. A superare in numero gli endpoint controllati dall’uomo sono i dispositivi IoT (Internet of Things), che sono ampiamente distribuiti, spesso in postazioni remote e non presidiate. Infine, le impronte aziendali dei cloud service provider si stanno diffondendo in numerose filiali, alcune delle quali anche geograficamente distanti: la maggior parte di queste si connette direttamente ai servizi cloud e mobili, aggirando i data center aziendali.

Tutti questi cambiamenti rendono obsoleto il concetto di perimetro di rete difendibile, richiedendo ai cloud service provider di adottare una nuova strategia di difesa in profondità basata su più livelli.

Il 77% dei professionisti della sicurezza afferma che la propria organizzazione ha spostato applicazioni o infrastrutture nel cloud nonostante i noti problemi di sicurezza.[3]

Migrazione di applicazioni e carichi di lavoro nel cloud

Quasi tutte le aziende hanno iniziato a spostare alcuni carichi di lavoro e applicazioni nel cloud, o almeno prevedono di farlo. Queste decisioni sono spesso guidate dal desiderio di ridurre i costi e migliorare l'efficienza operativa e la scalabilità sfruttando la flessibilità offerta dal cloud.

I cloud service provider offrono un'ampia gamma di possibili modelli di distribuzione, dal Software-as-a-Service (SaaS) alla Platform-as-a-Service (PaaS).

Diffidando della dipendenza esclusiva dai cloud service provider e mirando a distribuire ogni applicazione e carico di lavoro nel cloud per il quale è più adatto, molte organizzazioni hanno adottato un'infrastruttura multi-cloud. L'aspetto negativo di tale libertà di scelta è la necessità di apprendere le idiosincrasie di ogni ambiente cloud. Inoltre, le organizzazioni devono utilizzare diversi strumenti per gestire l'ambiente e le sue disposizioni di sicurezza, con il rischio di mettere a dura prova la visibilità e richiedere l'uso di più console per la gestione delle policy, il reporting e altro ancora.

Gli ambienti cloud sono dinamici: il 74% delle aziende ha spostato un'applicazione nel cloud per poi riportarla on-premise.[4]

Profusione di endpoint in più ambienti

Gli endpoint sono probabilmente i nodi più vulnerabili della rete del cloud service provider. I fornitori più grandi hanno migliaia di dipendenti, ognuno dei quali utilizza diversi dispositivi di lavoro e personali per accedere alle risorse di rete. Garantire una buona integrità informatica e l'aggiornamento della sicurezza degli endpoint su tutti questi dispositivi è un compito piuttosto arduo. Ancora più scoraggiante è la proliferazione dei dispositivi IoT. Verso la fine del 2019, il numero di dispositivi attivi ha superato i 26,66 miliardi e, nel corso del 2020, gli esperti stimano che questo numero raggiungerà i 31 miliardi.[5]

I dispositivi IoT sono presenti in numerosi contesti aziendali. Propongono esperienze personalizzate ai clienti del commercio al dettaglio e dell'ospitalità, tengono traccia dell'inventario nella produzione e nella logistica e monitorano i dispositivi nelle fabbriche o nelle centrali elettriche.

Spesso robusti ed efficienti dal punto di vista energetico, i dispositivi IoT si concentrano sulle prestazioni, in molti casi a scapito delle caratteristiche di sicurezza e dei protocolli di comunicazione sicuri. E a differenza della maggior parte dei dispositivi collegati in rete, le apparecchiature IoT sono comunemente distribuite in sedi distaccate, all'esterno o in strutture non dotate di personale o con poco personale (come le centrali elettriche). Da questi luoghi insicuri, le apparecchiature trasmettono spesso dati critici e sensibili a data center on-premise e a servizi cloud.

L'84% delle imprese ha adottato una strategia multi-cloud. L'81% considera la sicurezza una delle principali problematiche del cloud.[6]

Espansione della presenza commerciale nei mercati e nelle aree geografiche distribuite

Man mano che le aziende espandono la loro presenza globale aprendo nuove strutture, filiali e altre sedi secondarie, si trovano a dover far fronte a crescenti limitazioni della larghezza di banda delle reti WAN. Sebbene le applicazioni SaaS, i video e il Voice over IP (VoIP) aumentino la produttività e consentano nuovi servizi, contribuiscono anche a una crescita esponenziale del volume di traffico WAN.

La tecnologia MPLS (Multiprotocol Label Switching), di per sé estremamente affidabile, è stata la tecnologia di connettività WAN di elezione per molti anni. Tuttavia, con questa è difficile ottimizzare l'uso della larghezza di banda WAN e variare i livelli di qualità del servizio in base alle esigenze delle diverse applicazioni. Di conseguenza, l'espansione delle filiali e il miglioramento del servizio possono portare rapidamente all'esplosione dei costi della WAN.

Di conseguenza, le organizzazioni si stanno orientando verso la tecnologia SD-WAN (Software-Defined WAN), che fa un uso efficiente di MPLS, delle connessioni Internet e persino dei collegamenti di telecomunicazione. Inoltre, questa tecnologia instrada dinamicamente ogni tipo di traffico sul collegamento ottimale. L'adozione della SD-WAN ha aumentato la necessità di una SD-WAN sicura, che viene fornita al meglio come combinazione di funzioni di rete e di sicurezza in una piattaforma integrata.

Dal 2017 al 2019, si è registrato un aumento del 73% del numero di organizzazioni che hanno subito violazioni dei dati a causa di dispositivi o applicazioni IoT non protetti.[7]

La tecnologia SD-WAN garantisce migliori prestazioni e sicurezza a un costo inferiore rispetto a MPLS.[8]

Quattro considerazioni per la progettazione dell'architettura di sicurezza

Poiché le organizzazioni stanno adottando con entusiasmo le iniziative di innovazione digitale, le implicazioni per la sicurezza della rete sono spesso trascurate o minimizzate. Infatti, quasi l'80% delle organizzazioni aggiunge nuove innovazioni digitali più velocemente di quanto non possa proteggerle dalle minacce informatiche.[9]

I leader IT devono tenere conto di quattro considerazioni nella progettazione di architetture sicure per le loro aziende che innovano digitalmente:

1. Comprendere la superficie d'attacco in espansione

I dati sensibili possono potenzialmente risiedere ovunque e possono viaggiare su numerose connessioni al di fuori del controllo dell'azienda. Le applicazioni nel cloud sono esposte a Internet in modo che ogni nuova istanza cloud si aggiunga alla superficie di attacco dell'impresa. I dispositivi IoT estendono la superficie di attacco a postazioni remote e non presidiate da personale. In queste parti oscure della superficie di attacco, le intrusioni possono passare inosservate per settimane, se non addirittura per mesi, seminando il caos nel resto dell'impresa. I dispositivi mobili e gli endpoint di proprietà degli utenti causano imprevedibilità nella superficie di attacco mentre gli utenti si aggirano tra le sedi aziendali, in spazi pubblici e oltre i confini nazionali. Infatti, la massiccia migrazione verso il cloud, l'ampio uso delle piattaforme mobili e l'uso estensivo dei dispositivi IoT sono fattori che amplificano il costo per record di una violazione dei dati di centinaia di migliaia di euro.[10]

Il 61% dei CISO dichiara di svolgere già attività in termini di cloud, IoT e mobile.[11]

Fino al 40% del nuovo malware rilevato in un determinato giorno è zero-day o precedentemente sconosciuto.[12]

Questa superficie di attacco dinamica ed espansa dissolve il perimetro di rete, una volta ben definito, e le protezioni di sicurezza ad esso associate. È molto più facile per gli aggressori infiltrarsi nella rete: una volta all'interno, spesso trovano pochi ostacoli, riuscendo a raggiungere indisturbati i loro obiettivi. Pertanto, la sicurezza nelle imprese che promuovono l'innovazione digitale deve essere a più livelli, con controlli su ogni segmento di rete, partendo dal presupposto che prima o poi il perimetro verrà violato. E l'accesso alle risorse di rete deve essere basato sul minor privilegio possibile e sull'attendibilità continuamente verificata.

Le iniziative di innovazione digitale implicano che i team di sicurezza dell'impresa debbano distribuire protezioni per 17 diversi tipi di endpoint.[13]

2. Affrontare l'evoluzione delle minacce informatiche

Il panorama delle minacce informatiche è in rapida crescita, mentre gli utenti malintenzionati cercano di aggirare e sconfiggere le tradizionali difese della sicurezza informatica. Fino al 40% delle nuove minacce malware rilevate in un dato giorno è di tipo zero-day o sconosciuta in precedenza. [14] Che ciò sia dovuto all'aumento dell'uso di malware polimorfico o alla disponibilità di toolkit di malware, la crescita del malware zero-day rende meno efficaci gli algoritmi di rilevamento del malware tradizionali basati su signature. Inoltre, gli utenti malintenzionati continuano a utilizzare l'ingegneria sociale sfruttando i metodi di attendibilità statici utilizzati negli approcci di sicurezza tradizionali. Gli studi rivelano che l'85% delle organizzazioni ha subito attacchi di phishing o di ingegneria sociale nell'ultimo anno.[15]

Man mano che le minacce informatiche diventano sempre più sofisticate, gli incidenti e le violazioni dei dati sono più difficili da rilevare e da risolvere. Tra il 2018 e il 2019, il tempo necessario per identificare e contenere una violazione di dati è passato da 266 a 279 giorni.[16] Oltre alla capacità di individuare e prevenire un tentativo di attacco, le organizzazioni devono anche essere in grado di identificare e risolvere rapidamente un attacco sferrato con successo. Oltre l'88% delle organizzazioni ha dichiarato di aver subito almeno un incidente nei dodici mesi precedenti, a dimostrazione del fatto che tutte le organizzazioni sono a rischio di attacco e che la resilienza informatica è fondamentale.[17]

Nell'ultimo anno, un terzo delle imprese ha subito una violazione dei dati business-critical, che potrebbe causare sanzioni normative.[18]

3. Semplificare un ecosistema IT sempre più complesso utilizzando l'automazione

Secondo quasi la metà dei CIO, l'aumento della complessità è la principale problematica di una superficie d'attacco in espansione.[19] Questa maggiore complessità è dovuta al fatto che molte organizzazioni si affidano a una serie di prodotti specifici non integrati per la sicurezza. L'impresa media utilizza oltre 75 soluzioni di sicurezza distinte.[20]

Questa mancanza di integrazione della sicurezza significa che tali organizzazioni non sono in grado di trarre vantaggio dall'automazione nella distribuzione della sicurezza. Infatti, il 30% dei CIO indica il numero di processi manuali come una delle principali problematiche di sicurezza nella propria organizzazione.[21] Senza automazione della sicurezza, i CIO hanno bisogno dei professionisti della sicurezza informatica più qualificati per monitorare e proteggere la rete.

Tuttavia, molte organizzazioni non riescono ad assumere personale con solide competenze di sicurezza informatica. Le stime indicano che oltre 4 milioni di posizioni lavorative nell'ambito della sicurezza informatica sono attualmente non occupate e il numero è in costante crescita.[22] Questa impossibilità di accesso ai talenti necessari sta mettendo a rischio le organizzazioni: il 67% dei CIO, infatti, afferma che la carenza di competenze in materia di sicurezza informatica inibisce la loro capacità di tenere il passo con il ritmo del cambiamento.[23]

Gli aggressori sono ben consapevoli di queste problematiche e le sfruttano a loro vantaggio.

4. Stare al passo con le crescenti esigenze normative

Il Regolamento generale sulla protezione dei dati personali (RGPD) dell'Unione Europea (UE) e il California Consumer Privacy Act (CCPA) sono due dei più noti regolamenti in materia di protezione dei dati. Tuttavia, non sono gli unici. In ogni Stato americano è attualmente in vigore una legge sulla notifica delle violazioni dei dati, e molti di essi stanno attuando ulteriori misure di protezione della privacy dei consumatori. Spinti dalla pressione politica e sociale, si prevede un'espansione delle normative nei prossimi anni e le sanzioni per il mancato rispetto delle stesse stanno diventando sempre più esose, diffuse e punitive.

Le organizzazioni sono inoltre tenute a rispettare gli standard di settore, e molte ci riescono con enormi sforzi. Ad esempio, meno del 37% delle organizzazioni supera l'audit di conformità agli standard PCI DSS (Payment Card Industry Data Security Standard) ad interim.[24] Poiché il PCI DSS è sostituito dal PCI Software Security Framework (PCI SSF), è probabile che queste organizzazioni debbano affrontare ostacoli ancora maggiori per continuare a garantire la conformità.

La necessità di soddisfare e continuare a garantire la conformità alle normative ha un impatto significativo sulla capacità di un'organizzazione di raggiungere gli obiettivi di trasformazione della sicurezza, segnalando anche in che modo le organizzazioni investono nelle soluzioni tecnologiche. Ad esempio, del 71% delle organizzazioni che hanno trasferito applicazioni basate sul cloud nei data center on-premise, il 21% lo ha fatto per continuare a garantire la conformità con le normative.[25]

Il Fortinet Security Fabric

Il Fortinet Security Fabric affronta tutte le quattro sfide di sicurezza sopra menzionate proponendo un'ampia visibilità e controllo dell'intera superficie di attacco digitale di un'organizzazione per ridurre al minimo il rischio. Il Security Fabric è una soluzione integrata che riduce la complessità del supporto di più prodotti specifici e un flusso di lavoro automatizzato per aumentare la velocità di funzionamento.

Con il Fortinet Security Fabric, i team possono fruire dei seguenti vantaggi:

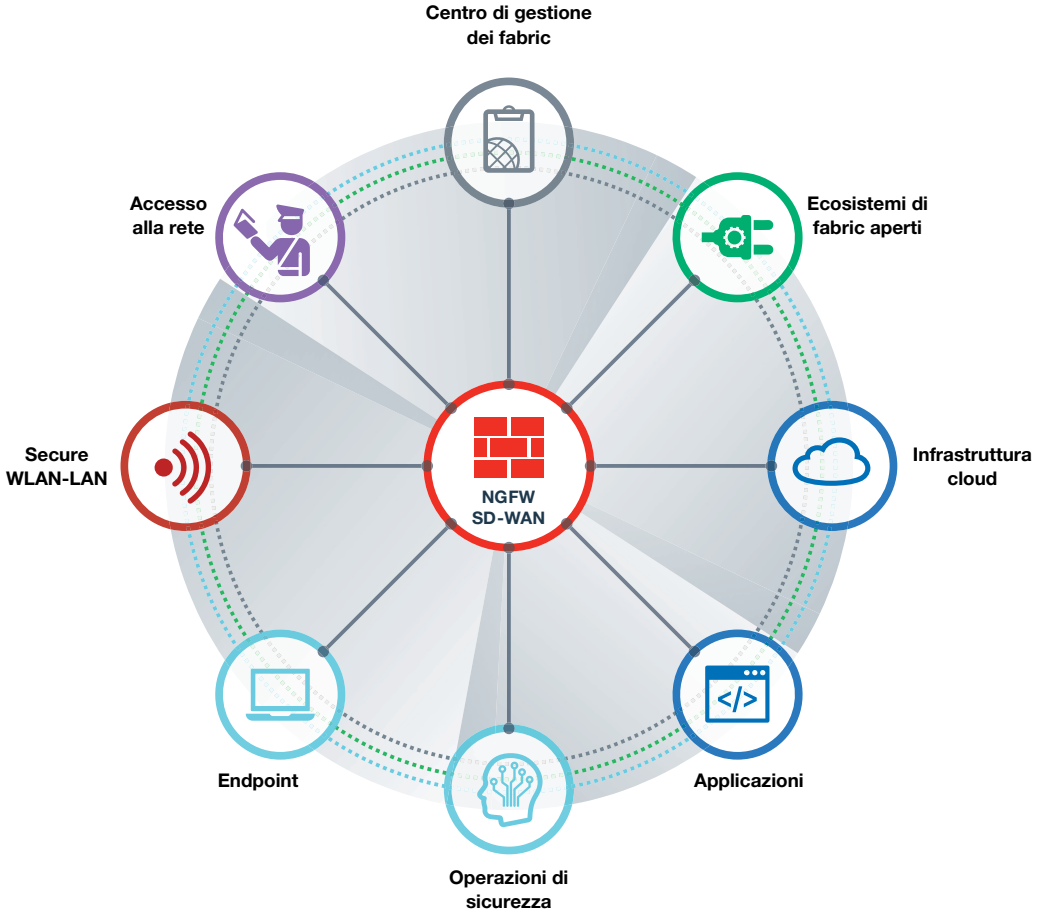

Figura 1: il Fortinet Security Fabric favorisce la perfetta integrazione di più tecnologie di sicurezza in tutti gli ambienti, supportate da un'unica fonte di threat intelligence in un'unica interfaccia. Elimina inoltre le lacune di sicurezza nella rete e accelera le risposte ad attacchi e violazioni.

Quasi la metà dei CISO considera l'integrazione della sicurezza e il miglioramento dell'analisi tra le principali priorità della loro strategia tecnologica di sicurezza informatica. [26]

Ampia e profonda visibilità della superficie di attacco

Con la più ampia gamma di soluzioni di rete ad alte prestazioni e basate sulla sicurezza per data center, filiali e piccole imprese e tutti i principali fornitori di cloud, il Fortinet Security Fabric offre tutto quanto necessario per proteggere ogni segmento della rete. Tutti i componenti sono configurati, gestiti e monitorati da un unico sistema di gestione centralizzata. Oltre a eliminare i compartimenti stagni associati alle infrastrutture di sicurezza dei prodotti specifici, l'interfaccia unica per tutti i componenti di sicurezza riduce l'onere di formazione del personale. Il sistema di gestione facilita anche la distribuzione di componenti remoti zero-touch, riducendo i costi di trasporto e abbattendo ulteriormente i costi operativi.

Architettura di sicurezza realmente integrata

Con tutti i componenti gestiti dallo stesso sistema operativo di rete FortiOS, il Fortinet Security Fabric garantisce una configurazione uniforme, oltre alla gestione delle policy e una comunicazione in tempo reale e senza sforzo nell'ambito dell'infrastruttura di sicurezza. In questo modo, si riducono al minimo i tempi di rilevamento e attenuazione delle minacce, nonché i rischi per la sicurezza derivanti da errori di configurazione e dalla compilazione manuale dei dati, con una risposta tempestiva e accurata agli audit di conformità. Oltre all'integrazione dei prodotti e delle soluzioni Fortinet, il Security Fabric include connessioni API predefinite per oltre 70 Fabric-Ready Partner che garantiscono una solida integrazione tra tutti gli elementi del Security Fabric.

I firewall NGFW FortiGate garantiscono il più alto rapporto prezzo-prestazioni nelle valutazioni di terzi durante la scansione del traffico crittografato. Raggiungono prestazioni SSL a 5,7 Gbps bloccando il 100% delle evasioni.[27]

La riduzione dei tempi di rilevamento delle violazioni e di risposta può favorire una riduzione del 25% dei costi complessivi di una violazione di dati.[28]

Operazioni e risposta automatizzate

Oltre alla perfetta integrazione, il Fortinet Security Fabric è leader del settore nell'applicazione di tecnologie di apprendimento automatico che contribuiscono a stare al passo con il panorama delle minacce informatiche in rapida evoluzione. Il Fortinet Security Fabric include funzionalità avanzate di orchestrazione della sicurezza, automazione e risposta (SOAR, Security Orchestration, Automation, and Response), così come il rilevamento proattivo delle minacce, la correlazione delle minacce, gli avvisi di condivisione dell'intelligence e la ricerca e l'analisi delle minacce.

Per le operazioni di rete, il Security Fabric offre operazioni e flussi di lavoro automatizzati per contribuire a ridurre le complessità in tutta l'organizzazione e in tutte le implementazioni, indipendentemente dal fatto che si tratti di un'installazione on-premise, nel cloud o presso le filiali.

Gestire i rischi, perseguire le opportunità

L'innovazione digitale consente alle organizzazioni di raggiungere nuovi livelli di efficienza e di risparmio sui costi, nonché migliorare le esperienze dei propri clienti. Tuttavia, le iniziative di innovazione digitale ampliano e modificano anche la superficie di attacco dell'organizzazione, consentendo alle minacce informatiche di sfruttare nuovi vettori di attacco.

Per le organizzazioni che adottano iniziative di innovazione digitale, il riconoscimento, l'accettazione e la corretta gestione dei rischi sono di fondamentale importanza. Il Fortinet Security Fabric rappresenta la base di tutto questo. Unifica le soluzioni di sicurezza in un'unica interfaccia, rende visibile la crescente superficie di attacco digitale, integra la prevenzione delle violazioni basata sull'intelligenza artificiale e automatizza le operazioni, l'orchestrazione e la risposta. In sintesi, consente alle organizzazioni di sfruttare nuovi vantaggi in termini di innovazione digitale senza compromettere la sicurezza dell'agilità, delle prestazioni e della semplicità del business.

[1] Nick Lansing, "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes e Fortinet, 2019.

[2] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[3] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019.

[4] Ibid.

[5] Gilad David Maayan, "The IoT Rundown For 2020: Stats, Risks, and Solutions", Security Today, 13 gennaio 2020.

[6] "Rightscale 2019 State of the Cloud Report", Flexera, 2019.

[7] Larry Ponemon, "Third-party IoT risk: companies don't know what they don't know", ponemonsullivanreport.com, visitato il 4 febbraio 2020.

[8] Nirav Shah, "SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019" Fortinet, 9 settembre 2019.

[9] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security e Ponemon Institute, 2019.

[10] "2019 Cost of a Data Breach Report", IBM Security e Ponemon Institute, 2019.

[11] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[12] In base a dati interni di FortiGuard Labs.

[13] "6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders", Fortinet, 8 settembre 2019.

[14] In base a dati interni di FortiGuard Labs.

[15] Kelly Bissell, et al.,"The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security e Ponemon Institute, 2019.

[16] "2019 Cost of a Data Breach Report", IBM Security e Ponemon Institute, 2019.

[17] In base a una ricerca interna di Fortinet.

[18] In base ai dati della ricerca interna di Fortinet.

[19] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[20] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating", CSO, 14 marzo 2016.

[21] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[22] "Strategies for Building and Growing Strong Cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study, 2019", $(ISC)^2$, 2019.

[23] "CIO Survey 2019: A Changing Perspective", Harvey Nash e KPMG, 2019.

[24] "2019 Payment Security Report", Verizon, 2019.

[25] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019.

[26] "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes e Fortinet, 2019.

[27] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, gennaio 2020.

[28] "2019 Cost of a Data Breach Report", IBM Security e Ponemon Institute, 2019.

www.fortinet.com

664959-0-0-IT

settembre 22, 2020 9:26 AM

ebook-considerations-security-architect_IT