WHITE PAPER

Accesso sicuro per la tecnologia operativa su larga scala

Abilitare il lavoro remoto e assicurare la Business Continuity

Sintesi preliminare

L'Operational Technology (OT) consente a fabbriche, impianti di generazione e trasmissione di energia, reti di trasporto pubblico, impianti petroliferi e di gas e servizi di pubblica utilità di operare con successo. Poiché queste organizzazioni forniscono prodotti e servizi critici, è particolarmente importante che dispongano di un piano di Business Continuity.

Fortinet offre una soluzione integrata per l'accesso remoto sicuro che risponde alle esigenze dell'OT. I Next-Generation Firewall (NGFW) FortiGate supportano in modo integrato le reti VPN IPSec, che permettono ai dipendenti di connettersi in modo sicuro alla rete IT o OT aziendale da postazioni di lavoro alternative. La protezione degli endpoint offerta da FortiClient e l'autenticazione a più fattori (MFA) di FortiToken, combinata con il Single Sign-On (SSO) di FortiAuthenticator, consentono alle aziende di supportare in modo sicuro il lavoro remoto e assicurare la Business Continuity.

9 organizzazioni OT su 10 hanno subito almeno un'intrusione dei sistemi nell'ultimo anno e il 63% ha avuto 3 o più intrusioni.[1]

Gestire al meglio le operazioni grazie al lavoro a distanza

Molte organizzazioni OT sono fondamentali per la sicurezza pubblica e devono quindi assicurarsi di poter svolgere le proprie operazioni senza interruzioni in caso di avversità e potenziali situazioni di emergenza, come patologie, inondazioni, uragani e blackout elettrici.

Per sviluppare correttamente un piano di Business Continuity, è importante considerare che l'organizzazione potrebbe non essere in grado di sostenere le normali operazioni in loco. La capacità di supportare in modo sicuro i dipendenti che lavorano a distanza è essenziale per assicurare la Business Continuity dell'OT. Le organizzazioni OT hanno bisogno di un accesso remoto sicuro anche perché potrebbero dover mettere in funzione nuove apparecchiature, applicare patch critiche oppure occuparsi di riparazioni e attività di risoluzione dei problemi da remoto. Inoltre, le organizzazioni OT possono eseguire il monitoraggio e la diagnostica a distanza oppure utilizzare centri operativi remoti per gestire in modo efficiente asset distribuiti geograficamente. La sicurezza è fondamentale perché una violazione in un ambiente OT potrebbe causare interruzioni dei servizi, con conseguente perdita di vite umane oppure avere un impatto negativo sulle infrastrutture critiche.

Le soluzioni Fortinet sono facilmente distribuibili nelle sedi di lavoro distaccate. Tuttavia, molte organizzazioni richiedono anche risorse in loco o nel cloud per supportare in modo sicuro i telelavoratori. In molti casi, le organizzazioni dispongono già di queste risorse perché fanno parte dell'infrastruttura di sicurezza esistente.

In caso di calamità naturale o di altri eventi che interrompono le normali operazioni aziendali, un'organizzazione deve essere in grado di passare rapidamente a una forza lavoro completamente remota. Oltre a fornire la crittografia dei dati in transito tramite una rete privata virtuale (VPN, Virtual Private Network), le soluzioni Fortinet offrono una serie di altre funzionalità che possono consentire a un'organizzazione di proteggere la propria forza lavoro e infrastruttura remota. Queste funzionalità includono:

- **Autenticazione a più fattori (MFA) e Single Sign-On (SSO).** FortiToken e FortiAuthenticator consentono l'autenticazione a due fattori e il Single Sign-On per dipendenti remoti e parti esterne.
- **Next-Generation Firewall (NGFW) e sistema di Intrusion Prevention, antivirus, Web Filtering e Software-Defined Wide-Area Networking (SD-WAN).** FortiGate offre tutte queste funzionalità e altre ancora in un'unica appliance.
- **Connettività wireless.** FortiAP e FortiExtender offrono accesso wireless sicuro, incluse connessioni cellulari 3G/4G LTE/5G wireless alle postazioni di lavoro remote con gestione completa dell'integrazione e della configurazione da una sola interfaccia.

Un firewall NGFW FortiGate è in grado di ispezionare il traffico crittografato e in chiaro su scala aziendale con un impatto minimo sulle prestazioni. I NGFW FortiGate includono anche un gateway VPN integrato che funge da endpoint per le connessioni crittografate ai telelavoratori. I firewall NGFW FortiGate in cui viene eseguito FortiOS 7.0 dispongono anche di Zero Trust Network Access (ZTNA) integrato. ZTNA è una tecnologia che consente di controllare l'accesso alle applicazioni indipendentemente dal luogo in cui risiede l'utente o l'applicazione. ZTNA è la naturale evoluzione della VPN e offre una maggiore sicurezza, un controllo più granulare e una migliore esperienza utente, quindi può essere un'ottima opzione per connettere in modo sicuro la forza lavoro remota.

Il firewall NGFW FortiGate si integra anche con gli elementi comuni dell'infrastruttura IT, compresi i servizi di directory aziendali, come Microsoft Active Directory (AD) e le soluzioni MFA e SSO. FortiAuthenticator fornisce un unico punto di integrazione centralizzato per le soluzioni di autenticazione e supporta soluzioni di terzi e FortiToken, dotato di opzioni di token hardware, software e basati su email. I token software sono supportati da una serie di smartphone e dispositivi mobili.

Poiché l'appliance virtuale FortiGate VM è in grado di funzionare a 20 Gbps su AWS e altri servizi cloud utilizzando tipi di istanza di grandi dimensioni, può supportare migliaia di utenti remoti, indipendentemente dall'utilizzo di FortiClient o di altri client VPN di terzi. Molti siti utilizzano FortiGate VM per connettersi in modo sicuro a un hub di servizi di sicurezza basato su cloud pubblico per accedere alle applicazioni ubicate nel cloud. L'accesso alle applicazioni on-premise è disponibile anche attraverso l'area geografica cloud più vicina e nel data center privato, che fornisce un supporto continuo per i trasferimenti di dati ad alta velocità dal cloud ai data center e viceversa.

I firewall NGFW FortiGate e gli access point wireless FortiAP includono il provisioning zero-touch; possono essere preconfigurati prima della spedizione, in modo da poter essere configurati automaticamente in loco.

Garantire la sicurezza dei telelavoratori con i firewall NGFW FortiGate

Le VPN IPSec e Secure Sockets Layer (SSL) ad alte prestazioni e lo ZTNA integrato in ogni NGFW FortiGate offrono un modello di distribuzione flessibile per le organizzazioni IT e OT. I telelavoratori possono usufruire di un'esperienza ZTNA o VPN senza client o accedere a funzionalità aggiuntive attraverso una VPN o ZTNA basata su client con la soluzione di sicurezza per endpoint FortiClient. Anche i dipendenti dell'azienda e i fornitori esterni possono trarre vantaggio dalla distribuzione di un access point wireless FortiAP o di un extender WAN wireless FortiExtender abbinato a un firewall NGFW FortiGate per le funzionalità wireless.

Le soluzioni Fortinet sono progettate per essere facili da usare, dall'acquisto iniziale fino al termine del ciclo di vita. Sia i firewall NGFW FortiGate che i FortiAP includono il provisioning zero-touch. Le appliance distribuite nelle sedi distaccate possono essere preconfigurate prima della spedizione, in modo da poter essere configurate automaticamente in loco. Il provisioning zero-touch contribuisce ad assicurare la Business Continuity e il supporto per il lavoro a distanza, perché nessuno in loco deve effettuare ulteriori configurazioni oltre a collegare la spina e i cavi di rete. I firewall NGFW FortiGate sono disponibili sia come dispositivi fisici che virtuali e i dispositivi virtuali FortiGate possono essere ospitati in cloud pubblici e privati.

Il Fortinet Security Fabric sfrutta il sistema operativo di rete Fortinet FortiOS e un ambiente API (Application Programming Interface) aperto per creare un'architettura di sicurezza ampia, integrata e automatizzata. Con il Fortinet Security Fabric, tutti i dispositivi di un'organizzazione, compresi quelli distribuiti in remoto per supportare il lavoro a distanza, possono essere monitorati e gestiti da una piattaforma di gestione centrale. I team di sicurezza possono ottenere visibilità e controllo completi di tutti i dispositivi connessi, indipendentemente dalla loro situazione di distribuzione, sia in locale da un FortiGate NGFW che a livello centrale da una piattaforma di gestione centralizzata integrata FortiManager distribuita presso la sede centrale.

Casi d'uso dei prodotti Fortinet che supportano l'accesso sicuro

Non tutti i dipendenti remoti di un'organizzazione richiedono lo stesso livello di accesso alle risorse aziendali. E non tutti gli appaltatori o i fornitori esterni devono disporre di accesso ai sistemi e alle reti critiche di un'azienda senza un'autorizzazione formale della richiesta di accesso remoto e un controllo delle connessioni remote. Fortinet offre soluzioni su misura per diversi tipi di telelavoratori.

1 Accesso sicuro per terzi remoti, ad esempio per la manutenzione o il monitoraggio e la diagnostica a distanza (FortiClient, FortiToken, FortiAP, FortiGate)

Gli utenti terzi remoti possono includere i tecnici di manutenzione esterni all'organizzazione che si occupano della manutenzione delle apparecchiature industriali. A volte richiedono un livello di accesso più elevato per la risoluzione dei problemi, il funzionamento o la gestione dei sistemi di controllo industriale (ICS, Industrial Control System) mentre lavorano da una postazione remota. Nell'ambiente della tecnologia operativa (OT), possono avere bisogno di accedere ai controller logici programmabili (PLC, Programmable Logic Controller) e alle unità terminali remote (RTU, Remote Terminal Unit). Possono anche richiedere la capacità di operare in ambienti IT multipli e paralleli. In alcuni casi, gli utenti terzi remoti includono integratori di sistemi, produttori di apparecchiature industriali originali (OEM, Original Equipment Manufacturer), fornitori e operatori.

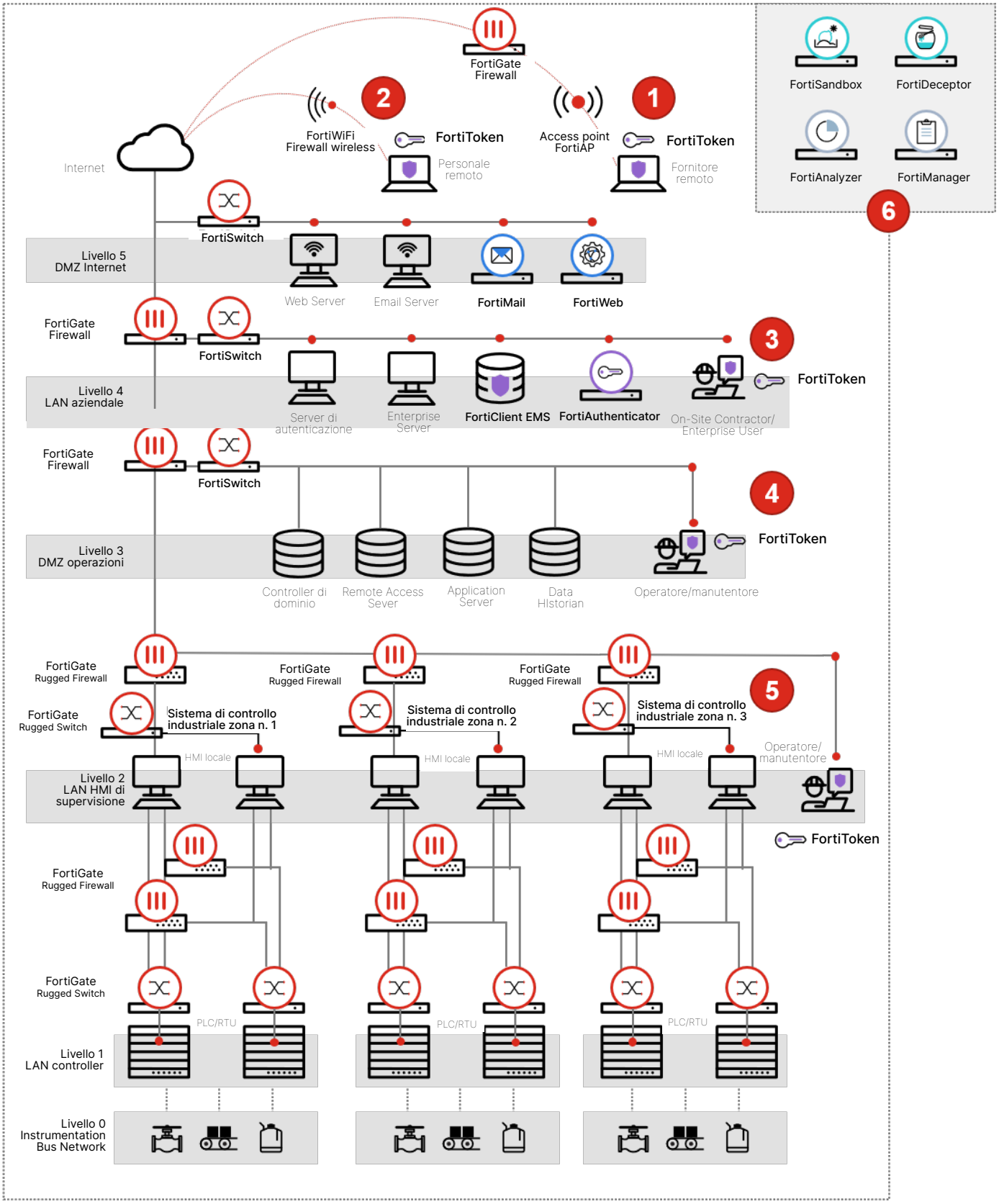

Figura 1: accesso sicuro con le soluzioni Fortinet in un'infrastruttura IT e OT connessa.

Questi utenti remoti possono richiedere un accesso di livello amministrativo alle reti e agli asset industriali, in modo da poter eseguire attività di messa in servizio, risoluzione dei problemi e manutenzione delle apparecchiature, compresi gli aggiornamenti del software o del firmware, nonché attività di risposta agli incidenti, come l'analisi forense e/o le attività associate all'attenuazione dei rischi.

I dipendenti remoti possono connettersi sia ai sistemi OT che ai servizi IT aziendali utilizzando il software client VPN integrato FortiClient o ZTNA e verificare la propria identità utilizzando un FortiToken per l'autenticazione a più fattori.

2 Accesso sicuro per il personale remoto, ad esempio i dipendenti che lavorano da casa (FortiClient, FortiToken, FortiWiFi)

I dipendenti remoti hanno bisogno di accedere ai sistemi aziendali per svolgere le loro attività quotidiane. L'accesso remoto può includere l'accesso alle funzionalità IT aziendali, come la posta elettronica, Internet, le teleconferenze, la condivisione di file e funzionalità specifiche, ad esempio l'accesso alle finanze o alle risorse umane. Per le aziende che gestiscono infrastrutture OT, alcuni dipendenti possono richiedere l'accesso ai sistemi OT per la registrazione e il recupero dei dati e, in alcuni casi, per eseguire la manutenzione e la diagnostica. I dipendenti responsabili della manutenzione dell'infrastruttura OT devono essere in grado di monitorare da remoto le prestazioni di uptime degli asset OT ed eseguire la risoluzione dei problemi di base su tali asset in caso di problemi.

I dipendenti remoti possono connettersi sia ai sistemi OT che ai servizi IT aziendali utilizzando il software client VPN integrato FortiClient o ZTNA e verificare la propria identità utilizzando un FortiToken per l'autenticazione a più fattori.

3 Accesso sicuro per gli appaltatori in loco o per gli utenti aziendali che hanno bisogno di accedere ai sistemi OT dalle reti IT (FortiClient, FortiToken, FortiGate, FortiClient EMS, FortiAuthenticator)

Analogamente ai casi d'uso 1 e 2, gli appaltatori in loco e gli utenti aziendali possono richiedere l'accesso ai sistemi OT dalla rete aziendale IT per scopi di acquisizione e manutenzione dei dati. Tuttavia, i sistemi OT possono trovarsi in reti OT geograficamente disperse in molte sedi. In alcuni casi, le reti OT possono essere ubicate in luoghi remoti dove la visita del personale non è possibile a causa di restrizioni di viaggio o di condizioni inospitali del sito.

La rete aziendale IT può essere situata in una posizione centrale e può connettersi alle reti OT in diverse sedi. In queste situazioni, l'abilitazione dell'accesso sicuro alle varie reti OT dalla rete aziendale IT centrale può offrire agli appaltatori in loco o agli utenti aziendali un accesso remoto sicuro ai sistemi OT. La posizione centrale può anche fornire una sede per implementare tecnologie centralizzate per la gestione dell'accesso remoto sicuro, come l'autorizzazione e il monitoraggio centralizzati delle connessioni di accesso remoto.

Pur rispettando i requisiti normativi, può essere necessario un accesso sicuro dalla rete aziendale IT alle reti OT per scopi di revisione e conformità. Il personale aziendale può aver bisogno di accedere alle reti OT per estrarre le informazioni necessarie dall'infrastruttura OT e condividerle con gli enti normativi come le organizzazioni CERT, NERC/FERC (nell'ambito del NERC CIP) ed ENISA/CSIRT (nell'ambito del NIS-D). (Il caso d'uso 6 contiene ulteriori informazioni sulla segnalazione e la gestione centralizzate).

4 Accesso sicuro per gli operatori o i tecnici della manutenzione che necessitano di un accesso ICS dalle reti OT (FortiClient, FortiToken, FortiGate)

Gli operatori o i manutentori che lavorano nei centri di controllo o nelle sale di controllo possono avere bisogno di accedere agli asset ICS per eseguire le loro operazioni di routine, come il monitoraggio, la diagnostica e la manutenzione degli asset ICS. Il centro di controllo può essere situato nelle stesse vicinanze o lontano dal sito ICS. La connessione di rete tra il centro di controllo e il sito ICS può essere cablata oppure LAN o WAN. La protezione dell'accesso e della comunicazione tra il centro di controllo e i siti ICS diventa fondamentale per prevenire attacchi di rete come man-in-the-middle e intercettazioni. Per migliorare le misure di sicurezza di questi accessi e di queste reti, nell'ambito dell'implementazione dell'accesso remoto sicuro, è possibile implementare funzioni come l'autenticazione a più fattori per l'accesso e la crittografia dei collegamenti di rete. Funzionalità come SD-WAN possono svolgere un ruolo importante se il centro di controllo e i siti ICS sono collegati utilizzando più collegamenti di comunicazione ed è importante mantenere la disponibilità di questi collegamenti a costi contenuti.

5 Accesso sicuro per gli operatori o i tecnici della manutenzione che necessitano di un accesso ICS locale (FortiClient, FortiToken, FortiGate)

L'accesso sicuro agli asset ICS non deve sempre avvenire da una sede distaccata. In alcuni casi, per fornire un accesso sicuro agli asset ICS, può essere necessario che gli operatori o i tecnici si trovino in loco. Questo tipo di accesso può offrire un'autenticazione a più fattori e migliorare notevolmente le funzionalità di autenticazione, autorizzazione e accounting (AAA) per l'accesso agli asset ICS. Inoltre, se necessario, è possibile implementare la crittografia di rete all'interno delle reti ICS.

6 Analisi, reporting e gestione della sicurezza centralizzati e Advanced Threat Protection centralizzata (FortiAnalyzer, FortiManager, FortiSandbox, FortiDeceptor)

Sia che l'implementazione dell'accesso sicuro riguardi sedi locali o sedi distaccate, la registrazione, il monitoraggio, il reporting e la gestione centralizzati dell'implementazione sono importanti per ottenere informazioni preziose e gestire in modo efficiente l'infrastruttura di accesso sicuro. L'implementazione centralizzata per la registrazione, il monitoraggio e il reporting può essere effettuata sotto forma di un centro operativo di rete (NOC, Network Operations Center) o di un centro operativo di sicurezza (SOC, Security Operations Center).

Per le implementazioni di accesso sicuro su larga scala, le funzionalità di gestione centralizzata possono ridurre notevolmente l'onere della gestione di più tecnologie e semplificare i costi di manutenzione in caso di necessità, come l'aggiornamento del software o del firmware per più tecnologie.

In alcuni casi, la segnalazione centralizzata può essere richiesta per scopi di conformità interna, come la segnalazione delle informazioni ai team interni di sicurezza delle informazioni o al Consiglio di Amministrazione. A volte queste informazioni sono fondamentali per rispettare i requisiti normativi, per cui il gestore o il titolare degli asset potrebbe dover fornire le informazioni alle comunità CERT nazionali o regionali.

Per le implementazioni di accesso sicuro su larga scala, le funzionalità di gestione centralizzata possono ridurre notevolmente l'onere della gestione di più tecnologie e semplificare i costi di manutenzione in caso di necessità, come l'aggiornamento del software o del firmware per più tecnologie.

Inoltre, per tenere il passo con le minacce emergenti, è possibile implementare a livello centrale tecnologie Advanced Threat Protection, come l'uso di strumenti di sandboxing, tra cui FortiSandbox, e honeypot, come FortiDeceptor, per identificare le minacce interne o esterne e attenuare i rischi.

Ottenere la totale integrazione della sicurezza con le soluzioni Fortinet

Quando si gestisce una forza lavoro remota e distribuita, la visibilità e la gestione centralizzate dell'infrastruttura di sicurezza è essenziale. Tutte le soluzioni Fortinet possono essere integrate utilizzando il Fortinet Security Fabric, che fornisce una piattaforma unificata per la visibilità, la configurazione e il monitoraggio. I connettori del fabric, un ambiente API aperto, il supporto della community DevOps e un ampio ecosistema esteso di Security Fabric consentono l'integrazione con oltre 250 soluzioni di terzi.

Quando un'organizzazione prepara un piano di Business Continuity, la visibilità e la gestione dell'architettura di sicurezza dell'organizzazione sono essenziali perché l'azienda potrebbe essere costretta a passare a una forza lavoro completamente remota con poco o nessun preavviso. Il supporto al telelavoro non deve mettere a rischio la sicurezza informatica di un'organizzazione.

Le seguenti soluzioni fanno parte del Fortinet Security Fabric e supportano telelavoro e operazioni sicuri:

- **FortiClient** offre funzionalità di telemetria degli endpoint, Vulnerability Management, prevenzione del malware, Web Filtering/Application Firewall, client VPN, ZTNA e supporto dell'autenticazione a più fattori.
- **FortiClient EMS** fornisce la configurazione dei client VPN, la gestione dei profili e delle policy di sicurezza degli endpoint ed è un connettore Security Fabric per la distribuzione e la gestione centralizzate dei client.

- **FortiAP** fornisce una connessione sicura con un controller wireless ed estende le reti agli utenti remoti. Elimina la necessità di client VPN software e offre il provisioning zero-touch.
- **FortiExtender** offre connettività WAN-LAN ibrida, connettività WAN wireless flessibile e supporta le reti cellulari 3G/4G LTE/5G. È adatto per siti mobili, parchi di veicoli e personale sul campo.
- **FortiWiFi/FortiGate** è un controller wireless sicuro con servizi VPN e ZTNA che offrono controllo di ammissione e applicazione, NGFW/Next-Generation Intrusion Prevention (NGIPS), connettori Security Fabric, policy di sicurezza dinamiche, SD-WAN e provisioning zero-touch.
- **FortiToken** conferma l'identità degli utenti con token di autenticazione hardware e software. Offre una perfetta integrazione con FortiGate e/o FortiAuthenticator con token software disponibili per iOS/Android e un'attivazione online sicura e protetta con i servizi di sicurezza FortiGuard.
- **FortiAuthenticator** assicura la gestione dell'autenticazione con integrazione LDAP/RADIUS/SAML, gestione di autenticazione a più fattori/token, supporto di token hardware e software e autorità di certificazione.
- **FortiAnalyzer** offre registrazione e reporting centralizzati, visualizzazione centralizzata degli asset e della rete, gestione centralizzata degli eventi e degli incidenti e consente l'analisi NOC/SOC con il supporto di distribuzioni basate su appliance hardware o macchine virtuali (VM).
- **FortiManager** fornisce gestione e monitoraggio centralizzati, automazione della sicurezza e integrazione di classe enterprise con supporto di multitenancy e amministrazione basata sui ruoli, provisioning SD-WAN sicuro e distribuzioni basate su appliance hardware o VM.
- **FortiSandbox** offre il rilevamento e la risposta alle minacce informatiche basati su intelligenza artificiale (IA) e la protezione automatizzata dalle violazioni con analisi che si basano sul framework MITRE ATT&CK. Offre una perfetta integrazione con FortiGate e il Security Fabric e supporta applicazioni e protocolli ICS/OT. Sono supportate le distribuzioni standalone o centralizzate e le distribuzioni basate su appliance hardware o VM.
- **FortiDeceptor** utilizza uno strato di esche e di richiami per eliminare le minacce informatiche nelle fasi iniziali. Emula Windows, Linux, VPN e RTU ICS e fornisce una perfetta integrazione con FortiGate e il Security Fabric. Supporta applicazioni e protocolli ICS/OT. Sono supportate le distribuzioni standalone o centralizzate e le distribuzioni basate su appliance hardware o VM.

Una base sicura a garanzia della Business Continuity

Sia per le organizzazioni OT che per quelle IT, prepararsi alla Business Continuity e al disaster recovery è di vitale importanza. Quando sviluppano piani di Business Continuity, le organizzazioni devono assicurarsi di disporre delle risorse necessarie per proteggere la forza lavoro remota e semplificare il funzionamento delle infrastrutture OT e IT senza interruzioni sia a livello locale che remoto, adottando al contempo un approccio di sicurezza ottimale. Le soluzioni Fortinet sono facilmente distribuibili e configurabili, in modo che le organizzazioni OT e IT possano assicurare sicurezza, visibilità e controllo end-to-end per i loro asset digitali, indipendentemente dall'ambiente di distribuzione.

[1] "2021 State of Operational Technology and Cybersecurity Report", Fortinet, 26 maggio 2021.

agosto 26, 2022 5:17 PM

950814-0-0-IT