SOLUTION BRIEF

Piena trasparenza e controllo centralizzato negli ambienti OT grazie a Fortinet

Panoramica preliminare

La convergenza tra tecnologia dell'informazione (IT) e tecnologia operativa (OT) espande la superficie di attacco dei sistemi OT, mettendo sotto forte pressione gli analisti delle operazioni di rete affinché garantiscano sicurezza, operatività e protezione. I sistemi OT richiedono ora un'infrastruttura di sicurezza integrata in grado di offrire fornire visibilità e controllo dei dispositivi, nonché informazioni sul contesto in cui si trovano e sulle vie di accesso che possono offrire a una serie in continua espansione di minacce basate su Internet. Il Fortinet Security Fabric offre un'architettura di sicurezza end-to-end per gli ambienti OT. Realizza una protezione integrata e automatizzata attraverso tecnologie come segmentazione, NAC (Network Access Control, controllo degli accessi alla rete) e SIEM (Security Information and Event Management, gestione delle informazioni e degli eventi di sicurezza).

Quasi tre quarti delle organizzazioni OT hanno subito negli ultimi 12 mesi un'intrusione di malware che ha compromesso produttività, ricavi, fiducia nel marchio, proprietà intellettuale e sicurezza fisica.[1]

Il 78% delle organizzazioni OT ha una visibilità solo parzialmente centralizzata delle soluzioni di sicurezza informatica distribuite nei loro ambienti.[4]

Necessità di più visibilità, controllo e informazioni sul contesto

La superficie di attacco OT è in rapida espansione. I sistemi sensibili negli ambienti industriali e infrastrutturali critici sono esposti a nuovi rischi dovuti a cambiamenti dell'infrastruttura, come la sostituzione delle connessioni OT seriali con connessioni digitali e la rapida crescita del numero di sistemi e dispositivi connessi a Internet.

Nonostante tutte queste sfide, gli analisti delle operazioni di rete sono chiamati a garantire sempre l'operatività e la sicurezza. Per quanto riguarda la sicurezza informatica, gli ambienti OT sono stati storicamente trascurati. Questo perché, fino a poco tempo fa, un air gap (separazione completa dalla rete IT) teneva questi sistemi al riparo dalle minacce. Oggi, tuttavia, il malware può attaccare i sistemi OT attraverso le connessioni IT, ad esempio tramite campagne di phishing via email.[2,3]

La priorità della sicurezza OT ha ricevuto molta attenzione negli ultimi tempi. Tuttavia, la trasposizione delle tradizionali strategie di sicurezza IT agli ambienti OT non è una soluzione adatta ai sistemi sensibili, spesso legacy, presenti in tali ambienti. Per garantire operazioni sicure e funzionali, le organizzazioni necessitano di tre funzionalità di sicurezza critiche:

Visibilità

La protezione dei moderni ambienti OT inizia con la definizione di una visibilità continua di ogni risorsa connessa alla rete, via cavo o in modalità wireless. La soluzione di sicurezza deve tenere traccia di tutti i dispositivi connessi in tutta l'organizzazione, quando vengono aggiunti, rimossi o spostati da un luogo all'altro.

Controllo

Le organizzazioni devono essere in grado di applicare e far rispettare le policy di accesso in base all'utente e al dispositivo, per proteggere le operazioni OT da potenziali minacce provenienti da ambienti IT. Attraverso controlli dinamici, basati sui ruoli, si possono raggruppare le applicazioni, collegare i dati e limitare l'accesso a gruppi specifici per rafforzare le difese OT. Questo tipo di segmentazione, detto intent-based, offre un controllo granulare che regola l'accesso in base a una valutazione continua dell'attendibilità di dispositivi e utenti.

Informazioni sul contesto

Quando un singolo dispositivo in un ambiente OT viene attaccato, le organizzazioni necessitano di notifiche istantanee e di informazioni sul contesto delle minacce per capire rapidamente quali azioni intraprendere e dove cercare. La sicurezza OT richiede una correlazione degli eventi e una gestione del rischio unificate per aiutare a velocizzare l'analisi, automatizzare le risposte e accelerare le azioni correttive, soprattutto considerando i gravi limiti delle risorse umane nella maggior parte delle organizzazioni.

Oltre la metà (53%) delle organizzazioni non dispone di una segmentazione interna della rete per limitare la diffusione delle minacce all'interno delle reti OT.[5]

La carenza mondiale di professionisti della sicurezza informatica è aumentata fino a quasi 3 milioni di posizioni non occupate.[6]

Un'architettura di sicurezza integrata per gli ambienti OT

Il **Fortinet Security Fabric** collega diverse soluzioni di sicurezza distribuite in un ambiente OT in un ecosistema di sicurezza coordinato. Questo tipo di architettura di sicurezza integrata coordina le difese informatiche in tutta l'organizzazione per consentire visibilità, controllo e informazioni sul contesto end-to-end per proteggere gli ambienti OT di oggi. Se un dispositivo connesso mostra un comportamento sospetto, il Security Fabric assicura la copertura e le capacità necessarie per individuare e risolvere rapidamente il problema.

Negli ambienti OT, il Security Fabric comprende soluzioni Fortinet come i robusti firewall NGFW **FortiGate**, lo switching di sicurezza in **FortiSwitch** (cablato) e **FortiAP** (wireless), la protezione dei dispositivi endpoint **FortiClient** e **FortiManager** per una visibilità trasparente e una gestione centralizzata di tutti i dispositivi distribuiti nell'intera organizzazione.

Il Fortinet Security Fabric aiuta anche a controllare l'accesso ai sistemi critici senza interferire con il loro funzionamento. Tradizionalmente, i controlli degli accessi si basavano su valori di attendibilità immutabili per utenti, dispositivi e applicazioni. Ma in realtà, l'attendibilità di utenti e dispositivi può fluttuare a causa dei normali cambiamenti nelle operazioni aziendali o a seguito di minacce emergenti. La **segmentazione intent-based** collega il controllo degli accessi a livelli di attendibilità continuamente aggiornati sulla base di informazioni acquisite da fonti sia interne che esterne.

In particolare, la segmentazione intent-based Fortinet supporta un controllo degli accessi dinamico e granulare che monitora continuamente il livello di attendibilità dell'utente e adatta le policy di sicurezza di conseguenza. Le risorse IT critiche sono isolate per garantire rapidità di rilevamento e prevenzione delle minacce attraverso strumenti di analisi e automazione. Basata su **NGFW FortiGate** fisici e virtuali, la segmentazione intent-based fornisce un controllo end-to-end della rete OT sia per il traffico est-ovest che per quello nord-sud.

Ma la sicurezza negli ambienti OT è inutile se crea un qualsiasi ostacolo al corretto funzionamento di sistemi critici. L'esperienza nei sistemi OT maturata da Fortinet nel corso della sua storia si è concretizzata nell'investimento in un'architettura di sicurezza OT dedicata. Le soluzioni Fortinet sono sviluppate da esperti del settore che comprendono le particolari esigenze di sicurezza e operative di questi ambienti specifici. Il Security Fabric fornisce una soluzione architetturale completa per la protezione end-to-end, diversa dall'approccio "à la carte" di altri fornitori che propongono prodotti e servizi singoli in grado di affrontare un solo vettore di attacco alla volta.

Soluzioni per la trasparenza in profondità dei sistemi OT

Le soluzioni di protezione degli endpoint migliorano la visibilità e il controllo dei dispositivi negli ambienti OT. Tre di questi elementi del Fortinet Security Fabric che svolgono un ruolo cruciale nella protezione degli endpoint sono:

FortiSIEM

Una sicurezza OT efficace richiede sia trasparenza che informazioni sul contesto, per aiutare gli analisti delle operazioni di rete a classificare gli allarmi, tracciare i dispositivi e correggere i problemi in modo rapido. FortiSIEM è una soluzione SIEM multi-vendor unificata che offre visibilità completa, funzionalità di correlazione, risposte automatiche e azioni correttive, per alleviare il lavoro del personale e migliorare al contempo il rilevamento delle violazioni.

FortiClient

FortiClient fornisce sicurezza all'interno degli ambienti OT per le postazioni di lavoro e i dispositivi BYOD connessi. Assicura la protezione degli endpoint critici attraverso funzionalità di antivirus, antimalware, anti-exploit, Web Application Firewall (WAF) e Web Filtering. Include anche un Fabric Agent per la telemetria degli endpoint, che collega FortiClient alle funzionalità di sicurezza del firewall FortiGate NGFW.

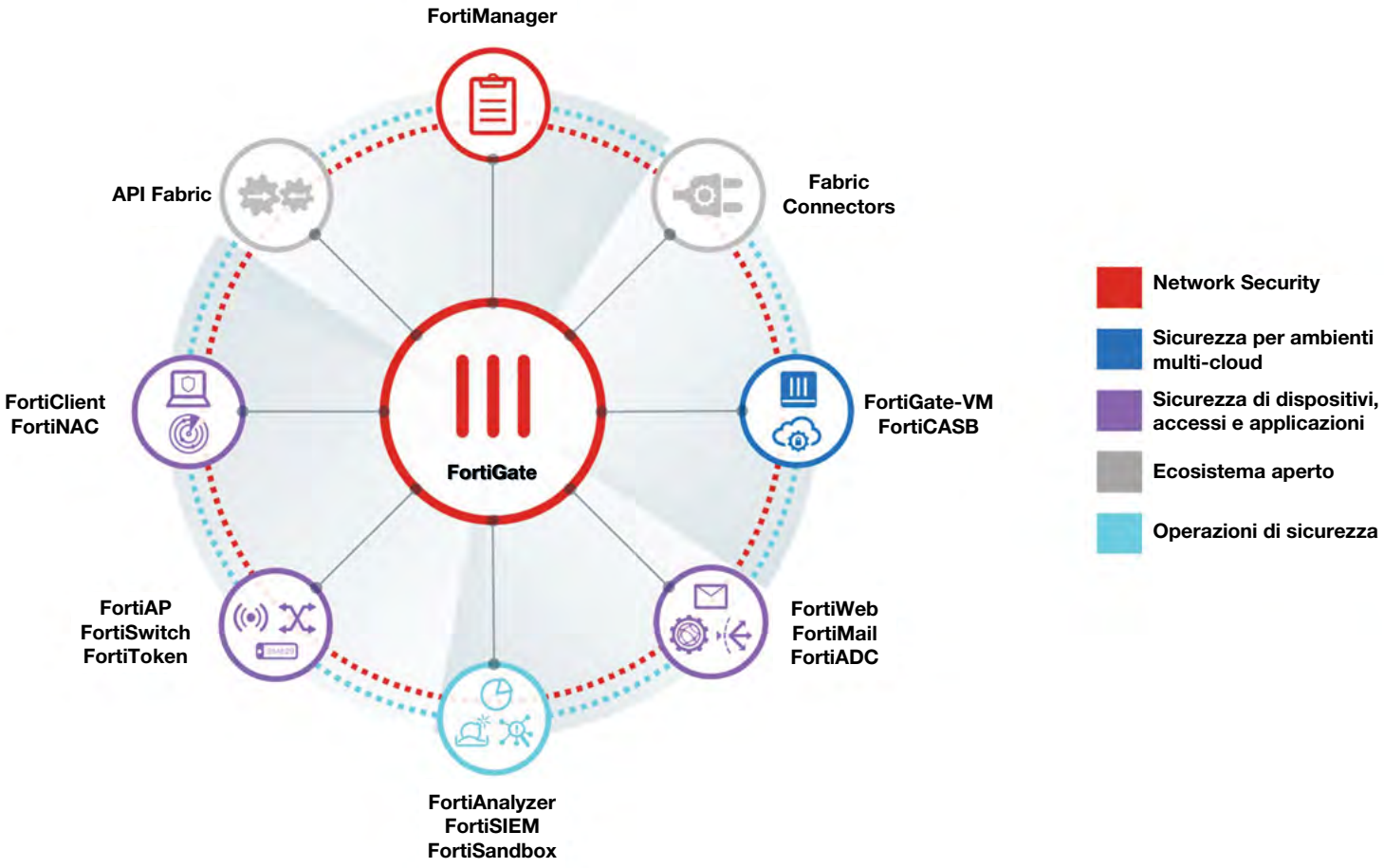
FortiNAC

FortiNAC aiuta a proteggere i dispositivi e i sistemi OT che possono non disporre di sufficienti funzionalità di sicurezza integrate, inclusi i dispositivi IoT (Internet of Things)/IIoT (Industrial Internet of Things), i controllori PLC (Programmable Logic Controller), nonché i sistemi ICS (Industrial Control System) e quelli del relativo sottoinsieme SCADA (Supervisory Control and Data Acquisition). In coordinamento con altre soluzioni del Security Fabric, FortiNAC aiuta a proteggere dalle minacce le reti OT ampiamente distribuite, rilevando gli endpoint con vulnerabilità non corrette da patch.

Per gli endpoint non critici, può rimuoverli dalla rete in modo istantaneo e automatico fino a quando non vengono applicate le patch necessarie. Può anche reintrodurre automaticamente tali endpoint in rete da una dashboard centrale. In caso di attacco multivettoriale su vasta scala (ad es. botnet) o in altre situazioni di emergenza in cui l'accesso deve essere strettamente limitato per motivi di sicurezza, FortiNAC ha la possibilità di bloccare la rete e di non consentire l'ingresso di nuovi dispositivi senza approvazione manuale.

Scegliere una soluzione di sicurezza progettata per gli ambienti OT

A causa della convergenza tra OT e IT, gli analisti delle operazioni di rete devono ora proteggere i loro vulnerabili sistemi OT da un'ondata crescente di minacce basate su Internet. Per supportare questa evoluzione, il Fortinet Security Fabric fornisce una base che assicura visibilità trasparente, controlli basati su policy e informazioni immediate sul contesto, specificamente progettata per gli ambienti OT.



Il Fortinet Security Fabric offre un'architettura di sicurezza unificata e integrata che consente l'automazione.

Il Security Fabric integra tecnologie (segmentazione, SIEM, NAC, protezione degli endpoint, switching e wireless) appositamente studiate per proteggere l'OT dalle minacce informatiche pervasive. Gli analisti delle operazioni di rete dovrebbero valutare la loro attuale soluzione di sicurezza OT ponendosi alcune domande di base:

La mia soluzione di sicurezza OT...

- Sfrutta un'architettura di sicurezza integrata che collega tutte le parti dell'infrastruttura di sicurezza in un ecosistema coeso e collettivo?
- Fornisce una maggiore visibilità per rilevare la rete OT e capire i livelli di sicurezza attuali?
- Rileva e classifica i dispositivi IoT e IIoT in base ai fattori di rischio associati, come le vulnerabilità, le classificazioni di sicurezza, nonché l'utilizzo?
- Applica la segmentazione intent-based per aumentare la resilienza delle reti OT?
- Incorpora soluzioni come SIEM e NAC per individuare utenti e dispositivi sospetti?
- Rende operativa l'intelligence per ottenere informazioni sul contesto in tempo reale senza interrompere le operazioni di base?
- Consente una gestione semplificata della sicurezza da una console unificata?

[1] "Report sullo stato dell'Operational Technology e della Cybersecurity", Fortinet, marzo 2019.

[2] "DHS Alert ICS-ALERT-14-176-02A", Cybersecurity and Infrastructure Security Agency, 22 agosto 2018.

[3] Catalin Cimpanu, "The Clever Phishing Trick Used by Hackers Targeting the US Energy Sector", BleepingComputer, 10 luglio 2017.

[4] "Report sullo stato dell'Operational Technology e della Cybersecurity", Fortinet, marzo 2019.

[5] Ibid.

[6] "Cybersecurity Skills Shortage Soars, Nearing 3 Million", (ISC)², 18 ottobre 2018.

aprile 24, 2020 12:20 PM

360483-0-0-IT

sb-network-operations-analyst