PANORAMICA SULLA SOLUZIONE

Proteggere i sistemi cyber-fisici con Fortinet OT Security Platform

Sintesi

I criminali informatici prendono sempre più di mira i sistemi cyber-fisici (CPS) nei settori della tecnologia operativa (OT) e delle infrastrutture critiche, generando cali di produzione e interruzioni dell'attività, e minacciando la stabilità delle infrastrutture critiche.[1] L'attuale aumento dei rischi ha fatto innalzare la sicurezza delle tecnologie operative (OT) a livello aziendale, e il 60% delle organizzazioni si appresta a spostare la sicurezza OT sotto la responsabilità del CISO entro 12 mesi.[2]

Fortinet OT Security Platform è il portafoglio più completo di soluzioni per la sicurezza OT, progettato per proteggere gli ambienti OT. Questa piattaforma di sicurezza comprende reti sicure, security service edge (SSE), soluzioni operative per la sicurezza (OT SecOps), intelligence dedicata alle minacce e un vasto ecosistema di alleanze tecnologiche. Tutte queste soluzioni sono integrate per unificare i vendor, centralizzare la gestione e realizzare la convergenza IT/OT al fine di semplificare le operazioni, migliorare la sicurezza di rete e ridurre il costo totale di proprietà.

OT

Fortinet OT Security Platform è stata valutata come Sole Leader del Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator.[3]

La necessità di soluzioni specifiche per l'OT

I CISO, i CIO e i team di sicurezza di rete responsabili di gestione e sicurezza degli ambienti OT devono risolvere una serie di sfide specifiche, tra cui la scelta e la gestione di un numero spesso troppo alto di vendor di sicurezza OT. Non è semplice configurare la sicurezza in un ambiente OT così complesso e gestire al contempo le priorità operative, come la sicurezza del personale e l'affidabilità della produzione. Oggi però molte organizzazioni utilizzano una piattaforma integrata per unificare i vendor, far convergere le tecnologie IT e OT e ottimizzare uno staff di cybersecurity spesso sottodimensionato. Per affrontare queste sfide, è necessaria una piattaforma di sicurezza OT che offra connettività unificata, segmentazione, SSE e soluzioni SecOps OT che si integrino bene con le soluzioni esistenti.

La piattaforma di sicurezza OT di Fortinet è una suite completa di soluzioni di rete e sicurezza progettate appositamente per l'OT, dalla connettività iniziale alle soluzioni SSE e SecOps OT avanzate.

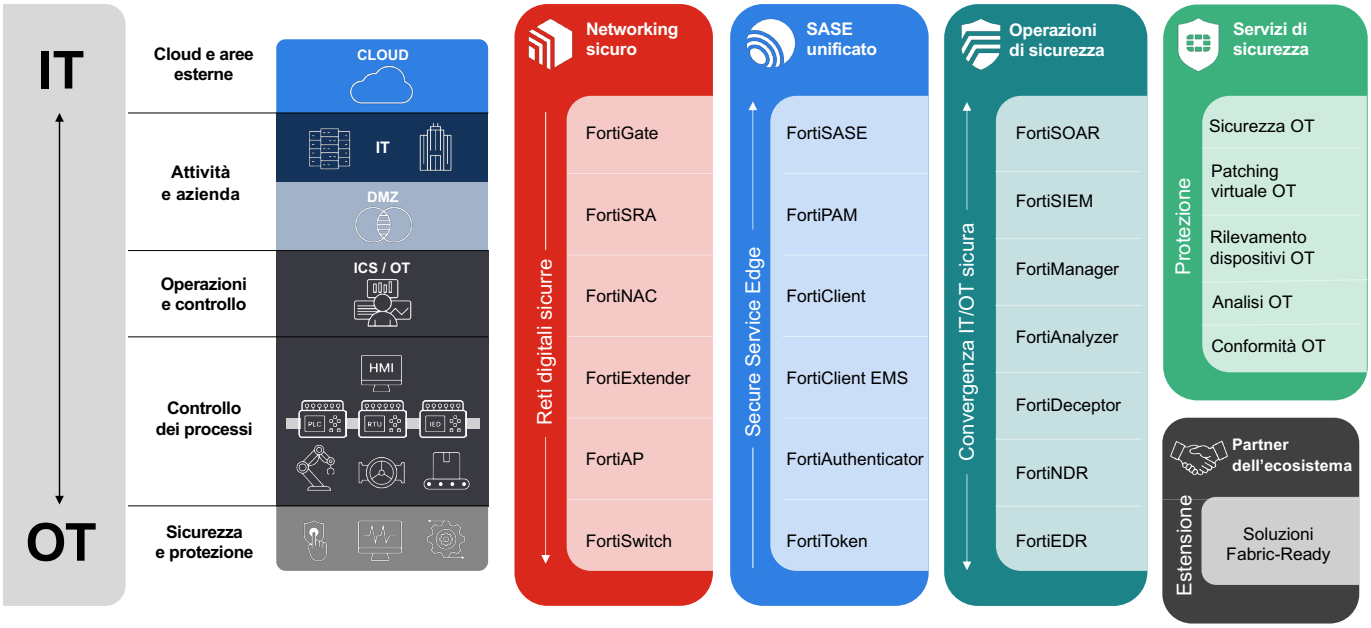

Figura 1: Fortinet OT Security Platform

Connetti e proteggi gli ambienti OT con un networking sicuro

Fortinet OT Security Platform offre ai CPS la connettività iniziale tramite il FortiGate Next-Generation Firewall (NGFW), cui segue la segmentazione fornita dal FortiSwitch di Fortinet. La soluzione di accesso remoto sicuro FortiSRA fornisce l'accesso remoto sicuro a reti e dispositivi OT con risorse limitate. Queste soluzioni di connettività e accesso critiche sono state progettate ad hoc per gli ambienti OT, e includono hardware rinforzato e servizi di sicurezza OT avanzati basati su AI.

OT Security Platform è stata progettata anche per affrontare altre sfide comuni dei team di sicurezza. I sistemi e i dispositivi OT spesso non sono protetti da patch perché il vendor non le ha predisposte o perché sono in conflitto con le priorità di produzione, quindi è essenziale implementare misure di sicurezza proattive o compensare i controlli. OT Security Platform offre controlli di sicurezza per applicazioni e protocolli OT, segmentazione e microsegmentazione della rete per le reti OT e controlli di gestione delle vulnerabilità come un motore di virtual patching. Questo motore include oltre 1.000 regole di patch virtuali per proteggere immediatamente i dispositivi OT vulnerabili perché privi di patch.

Oltre ad assicurare visibilità sugli asset e la rete, OT Security Platform include FortiGuard OT Security Service, che fornisce protezione dalle vulnerabilità per le applicazioni e i protocolli OT dei principali produttori di sistemi di controllo industriali (ICS). Le firme aggiornate e i dati di protezione delle vulnerabilità consentono a FortiGate NGFW di rilevare i tentativi di exploit delle vulnerabilità note dei sistemi OT. OT Security Service include oltre 80 protocolli di automazione industriale e sistemi di controllo, e utilizza un elenco di oltre 18.000 firme di vulnerabilità. Di queste, più di 4.000 sono focalizzate sulla sicurezza OT e basate sul motore del sistema di prevenzione delle intrusioni FortiGate.

Dato che molti dispositivi e sistemi OT non sono protetti da patch, la capacità di individuare gli exploit e prevenire gli attacchi con il patching virtuale o la protezione delle vulnerabilità è un vantaggio assoluto. Fortinet OT Security Platform offre le seguenti funzionalità:

- Controllo della sicurezza e applicazione di policy con FortiGate NGFW
- Visibilità e controllo completi di utenti e dispositivi nella rete, e supporto per la microsegmentazione di rete con o senza FortiSwitch
- Monitoraggio, logging e reporting centralizzati con FortiAnalyzer per le appliance FortiGate distribuite in reti IT e OT
- Gestione centralizzata dei dispositivi e implementazione di policy di sicurezza con FortiManager per le appliance FortiGate in reti IT e OT
- Informazioni e misure di mitigazione in tempo reale e aggiornate per affrontare minacce, vulnerabilità ed exploit zero-day tramite FortiGuard Labs

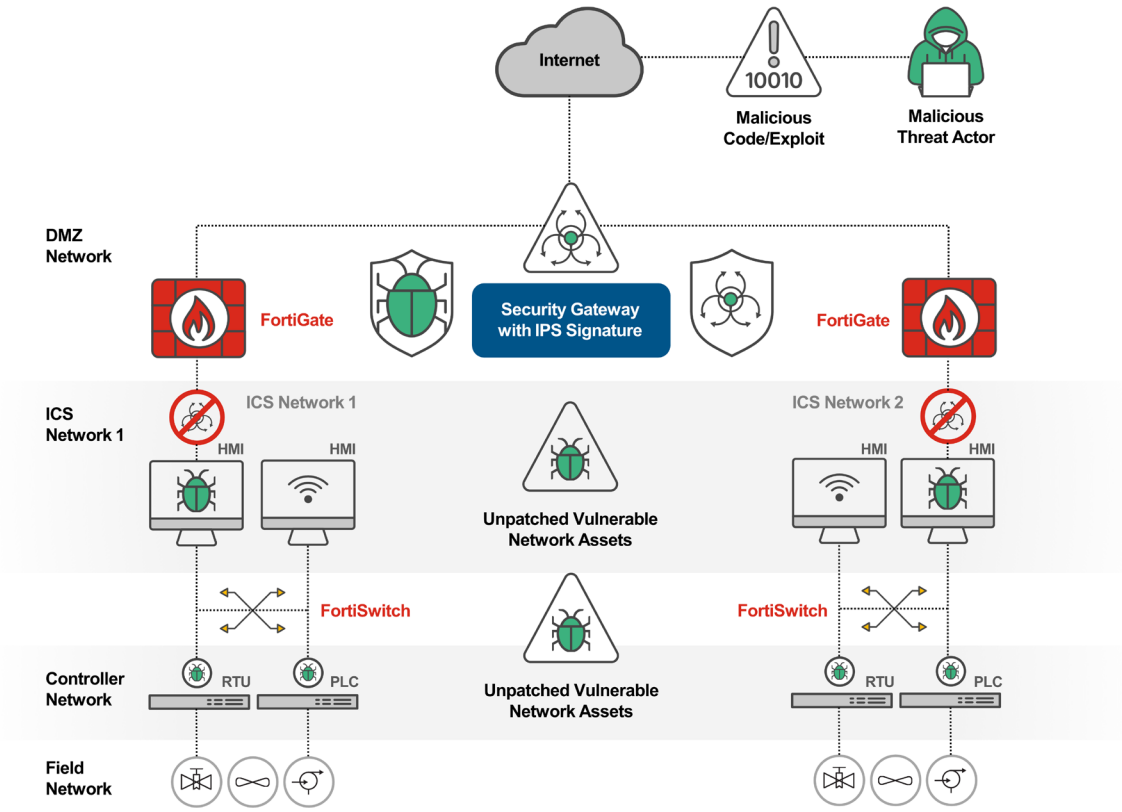

Figura 2: Patching virtuale nelle reti ICS/OT

Soluzioni SSE per l'OT

Estendere la strategia SSE alle reti OT può essere difficile a causa di priorità operative, sensibilità delle reti e dei dispositivi ICS critici e mancanza di soluzioni Zero Trust specifiche per il settore OT. Per superare queste sfide, la soluzione OT Security Platform include la gestione degli accessi privilegiati (PAM) e il controllo degli accessi alla rete (NAC).

Pur essendo efficaci già singolarmente, queste soluzioni lavorano in sinergia per convalidare chi e cosa si connette alla rete OT, limitando l'accesso alle risorse idonee in base ai ruoli del dispositivo o dell'utente. Le soluzioni Fortinet SSE connettono quindi in modo sicuro gli utenti alle applicazioni, a prescindere dalla posizione dell'utente o da dove sia ospitata l'applicazione.

Il NAC consente l'accesso degli utenti alle applicazioni in modo selettivo, identificando e proteggendo le applicazioni IT, OT e Industrial Internet of Things (IIoT). I proprietari e gli operatori degli asset hanno inoltre una visibilità completa e il controllo su ogni dispositivo connesso alla rete. FortiSRA abilita l'accesso remoto sicuro a supporto di appaltatori terzi, auditor e dipendenti remoti, proteggendo i sistemi OT critici da minacce provenienti dall'accesso remoto e dalle reti non attendibili.

Le soluzioni di gestione delle identità e degli accessi FortiPAM, FortiAuthenticator e FortiToken funzionano insieme per limitare l'accesso ai soli utenti autorizzati. Allo stesso tempo, la segmentazione FortiGate migliora ulteriormente l'accesso Zero Trust separando le reti IT/OT in base alle esigenze aziendali. Le soluzioni Fortinet SSE offrono le seguenti funzioni:

- FortiGate NGFW fornisce controllo della sicurezza e applicazione di policy.
- FortiNAC offre visibilità, controllo e risposta automatizzata per tutto ciò che è connesso alla rete.
- FortiSRA offre un accesso remoto sicuro e senza agente per gli ambienti OT.
- FortiToken offre l'autenticazione a due fattori con un'applicazione OTP (one-time password), notifiche push o un token OTP hardware a tempo.
- FortiAuthenticator offre l'accesso Single Sign-On e l'autorizzazione dell'utente che identifica gli utenti, verifica le autorizzazioni di accesso provenienti da sistemi di terzi e comunica le richieste di accesso a FortiGate NGFW per implementare policy di sicurezza basate sull'identità.
- FortiPAM offre funzionalità di gestione delle identità e degli accessi privilegiati, abilitando l'implementazione della sicurezza Zero Trust per le risorse critiche. Controlla l'accesso degli utenti alle applicazioni e ai sistemi critici, monitora e traccia l'attività degli utenti e fornisce l'accesso remoto sicuro alle risorse critiche.

Gartner ha dichiarato: "L'interesse generale verso la sicurezza CPS (e in particolare la sicurezza OT) è in crescita, come indicano non solo i sondaggi Gartner ma anche i trend delle richieste dei clienti Gartner. Ciò è dovuto sia alle iniziative degli attori delle minacce (in alcuni casi sostenuti da Stati-nazione) che puntano sempre più spesso alle infrastrutture critiche e ai sistemi industriali, sia all'espansione della superficie di attacco delle aziende generata dalle iniziative di trasformazione digitale. Contestualmente, sono aumentati anche i requisiti di conformità, come quelli relativi alla direttiva NIS2 e al Cyber Resilience Act previsti dall'UE e all'aggiornamento del NIST Cybersecurity Framework degli Stati Uniti."[4]

Migliorare la sicurezza OT con operazioni di sicurezza specifiche per l'OT

L'uso di una piattaforma specifica per le reti OT consente di integrare più fonti di dati, velocizzare i tempi di rilevamento e rendere possibile l'automazione delle risposte di sicurezza. Le soluzioni Fortinet OT SecOps sono personalizzate per far convergere le operazioni di rete e di sicurezza in un'unica piattaforma di gestione e monitoraggio per infrastrutture di rete e sicurezza OT. Infatti, includono identificazione degli asset e comunicazioni di rete con una mappa topologica che fa riferimento alla Purdue Enterprise Reference Architecture, alla matrice MITRE ATT&CK for ICS, ai playbook OT e al reporting su rischi e conformità.

I team IT e OT devono anche bilanciare le esigenze di sicurezza con le priorità operative. Quando si mitigano i rischi, è possibile rinviare le operazioni di remediation ai team operativi o di sicurezza OT per garantire la continuità della produzione e dei servizi. L'obiettivo finale è ottimizzare un centro operativo di sicurezza IT/OT convergente che usi intelligence sulle minacce, analisi, rilevamento delle minacce, tattiche di inganno o honeypot, risposta agli incidenti, ricerca delle minacce, governance e conformità senza generare interruzioni dell'ambiente OT.

Per raggiungere questo obiettivo, le soluzioni Fortinet OT SecOps includono:

- FortiGate NGFW fornisce controllo della sicurezza e applicazione di policy.
- FortiAnalyzer offre una gestione unificata dei log, oltre ad analisi e report sulla sicurezza OT, tra cui report sul rischio IT/OT, IEC 62443 e sulla conformità NERC CIP.
- FortiEDR offre rilevamento e protezione dalle minacce automatizzati e in tempo reale agli endpoint, risposta agli incidenti orchestrata e analisi forense.
- FortiSIEM acquisisce e analizza i dati di log dei sistemi IT e OT e mette in correlazione il comportamento degli attori delle minacce in entrambi gli ambienti. FortiSIEM può anche mostrare l'attività delle minacce nel framework MITRE ATT&CK per ambienti IT e ICS aziendali.
- FortiSOAR è una piattaforma personalizzabile per le operazioni di sicurezza che fornisce playbook automatizzati, triage degli incidenti e remediation in tempo reale per consentire alle aziende OT di identificare, difendersi e rispondere agli attacchi.
- FortiDeceptor offre implementazioni di honeypot (esche per dispositivi OT e protocolli) per ingannare, smascherare ed eliminare minacce esterne e interne prima che si verifichino danni significativi.
- FortiNDR offre funzionalità di rilevamento e risposta di rete basate sull'intelligenza artificiale e su reti neurali artificiali per fornire indagini in tempi inferiori al secondo. Sfrutta tecnologie di deep-learning che assistono gli analisti SOC con risposte automatizzate per rimediare a diverse tipologie di attacchi. Per ottenere questo risultato, FortiNDR include un Virtual Security Analyst in grado di identificare, classificare e rispondere rapidamente alle minacce.
- Il Security Operations Center-as-a-Service è un servizio su cloud di monitoraggio della sicurezza gestito che analizza gli eventi di sicurezza generati dai FortiGate NGFW e da altri prodotti di sicurezza. Esegue il triage degli avvisi e l'escalation delle notifiche per le minacce confermate.
- FortiRecon digital risk protection è un servizio basato su SaaS che combina tre efficaci moduli: gestione della superficie di attacco esterna, protezione del brand e intelligence focalizzata sugli aggressori. FortiRecon fornisce una visione su ciò che gli aggressori vedono, fanno e pianificano, aiutando a contrastare meglio gli attacchi in fase di ricognizione e a ridurre in modo significativo i rischi, i tempi e i costi rispetto a una mitigazione delle minacce attuata solo in un secondo tempo.

Supportare consolidamento e convergenza con OT Security Platform

La protezione dei CPS è una sfida tecnica complessa, resa spesso più difficile dalla presenza di priorità operative contrastanti. Per proteggere gli ambienti OT si inizia dal connettere in modo sicuro le reti OT al resto dell'azienda, spesso per la prima volta, per poi implementare un centro operativo di sicurezza OT con piene funzioni. Contestualmente, molte organizzazioni OT mirano a ottimizzare le operazioni tramite l'unificazione dei vendor e la convergenza delle risorse IT e OT. Fortinet OT Security Platform risolve queste sfide grazie a connettività di rete, SSE e soluzioni SecOps ad hoc per il settore OT. Fortinet OT Security Platform offre la flessibilità e le soluzioni di cui le organizzazioni hanno bisogno per proteggere le infrastrutture OT.

[1] CISA, Critical Infrastructure Sectors, accesso al 1° agosto 2024.

[2] Fortinet 2024 State of OT and Cybersecurity Report.

[3] Fortinet Named Sole Leader in 2023 IT/OT Network Protection Platforms Navigator™ Report, 27 luglio 2023.

[4] Gartner, Emerging Tech: Top Factors Driving Cyber-Physical Systems Security Growth, 26 aprile 2024.

settembre 6, 2024 3:45 PM / 123456-0-0-EN