WHITE PAPER

Soluzioni Fortinet per la sicurezza informatica nel settore petrochimico

Come proteggere le infrastrutture e le risorse critiche dalle minacce informatiche e fisiche con l'integrazione end-to-end

Panoramica preliminare

Le infrastrutture di proprietà delle aziende petrolchimiche contribuiscono non solo alla redditività di un'azienda, ma anche alla stabilità economica e geopolitica del mondo intero. Dai siti di trivellazione agli oleodotti e alle raffinerie, il processo di produzione del petrolio è soggetto a ogni tipo di rischio, e gli avversari li prendono di mira per varie motivazioni. Fortinet fornisce soluzioni di sicurezza informatica al settore petrolchimico da oltre un decennio, offrendo l'integrazione end-to-end della sicurezza informatica e fisica per le reti più lontane. Nelle sedi upstream, midstream e downstream, appliance ruggedized possono sopravvivere alle peggiori condizioni ambientali, e i livelli di sicurezza proteggono i siti remoti vulnerabili. Quanto alle sedi centrali, il Security Fabric di Fortinet permette un approccio olistico alla sicurezza. E quell'architettura di sicurezza si estende ai distributori, creando una rete sicura sino alle loro sedi e al loro interno.

Il 60% delle aziende petrolchimiche ha subito di recente un incidente significativo riguardante la sicurezza informatica.[1]

Le aziende petrolchimiche possiedono e gestiscono importanti componenti di infrastrutture critiche che sono fondamentali non solo per le attività aziendali, ma anche per il benessere economico e militare di una nazione. Le operazioni upstream, midstream e downstream sono obiettivi preziosi per i cyber-avversari, con motivazioni estremamente diversa, dal profitto personale allo spionaggio industriale sino allo sconvolgimento di un'economia.[2] Parafrasando le parole di uno scrittore, ogni elemento della catena del valore nel settore petrolchimico è attualmente esposto, e le difese statiche convenzionali non sono più sufficienti.[3]

Anche se a prima vista tale affermazione potrebbe sembrare un'iperbole, il rischio è reale. Un attacco al sistema di supervisione, controllo e acquisizione dati (SCADA) che gestisce una piattaforma offshore, un pozzo petrolifero, un oleodotto o una raffineria, o anche ai dispositivi Internet-of-Things (IoT) che forniscono dati di monitoraggio a tali sistemi, può comportare conseguenze devastanti,[4] tra cui ingenti danni alle strutture, lunghe interruzioni della fornitura e persino infortuni e perdite di vite umane per dipendenti, residenti e passanti nelle vicinanze.

Gli attacchi che prendono di mira le infrastrutture OT nel settore petrolchimico stanno diventando sempre più frequenti[5], e anche le infrastrutture aziendali sono un obiettivo. Un attacco riuscito può esporre la proprietà intellettuale, come ad esempio le indagini di esplorazione, e mettere a repentaglio la sicurezza dei dati per quanto concerne le informazioni finanziarie e relative al personale. Oltre ai problemi che tali attacchi possono creare all'attività, le aziende possono anche trovarsi esposte a rischi normativi.

Da oltre un decennio, Fortinet fornisce soluzioni di sicurezza complete per il settore petrolchimico, sia per i siti di trivellazione sulla terraferma e in mare aperto che per le raffinerie e gli oleodotti, fino al distributore all'angolo. Al centro della soluzione proposta da Fortinet vi è il suo Security Fabric, che permette l'integrazione della sicurezza end-to-end di tutte le infrastrutture in espansione gestite dalle aziende petrolchimiche.

Principali esigenze del settore petrochimico rispetto alla sicurezza informatica

Le principali esigenze del settore petrochimico rispetto alla sicurezza informatica sono:

Ottimizzazione dei costi

I mercati petroliferi sono noti per le fluttuazioni selvagge del prezzo di vendita del petrolio, della benzina e del gas naturale, una volatilità per cui un'azienda può passare facilmente da una notevole redditività a una perdita di gestione nell'arco di pochi giorni. Minimizzare i costi è sempre, dunque, una priorità per le aziende petrolchimiche, che cercano di strutturare le attività in modo da sopravvivere ai periodi in cui i prezzi sono bassi.

In questo ambiente, sostituire attrezzature costose e obsolete a causa di vulnerabilità a livello di sicurezza è a volte fuori questione. Sono pertanto necessari approcci creativi per mantenerle protette. Qualunque cosa ciò richieda, la soluzione deve essere pensata in modo da non ostacolare le attività. Molte aziende hanno più componenti infrastrutturali con questo tipo di vulnerabilità, facendo gravare un carico maggiore sui responsabili della sicurezza informatica.

La carenza di competenze nel campo della cybersecurity sta peggiorando, con una carenza stimata di oltre 4 milioni di lavoratori, rispetto ai 2,8 milioni che attualmente lavorano nel settore.[6] Ciò significa che assumere altri dipendenti per affrontare questi problemi è costoso e, a prescindere dal prezzo, potrebbe addirittura essere impossibile trovare sul mercato del lavoro determinate competenze specifiche. Peraltro, l'aggiunta di personale non risolve il problema fondamentale, ovverosia che i processi di sicurezza manuali sono inadeguati ad affrontare le minacce che si muovono alla velocità delle macchine.

Visibilità dei sistemi IT e OT

I dispositivi Industrial IoT (IIoT) hanno modificato le regole del gioco per quanto concerne la sicurezza dei sistemi SCADA (Supervisory Control and Data Acquisition) utilizzati per gestire siti di trivellazione, oleodotti e raffinerie. I sensori connessi a Internet e i dispositivi di controllo connessi eliminano l'isolamento fisico da Internet che storicamente ha mantenuto i sistemi SCADA relativamente al sicuro dagli attacchi informatici.

Ciò ovviamente espande la superficie di attacco di un'azienda. Il problema è aggravato dal fatto che molti dispositivi IIoT sono headless e, quindi, non possono essere protetti con il software di sicurezza del client o ricevere aggiornamenti del firmware. Per tappare queste falle nella sicurezza, le organizzazioni spesso distribuiscono più prodotti puntuali.[7] La sicurezza compartimentata che ne risulta crea complessità[8] e offusca la visibilità, ritardando il rilevamento, la prevenzione e la risposta alle minacce. Ciò aumenta il rischio che una minaccia in rapida evoluzione riesca a passare prima che i processi manuali la rilevino.

Efficienza operativa

Questa frammentazione architettonica aumenta anche le inefficienze operative per il team responsabile della sicurezza informatica. L'automazione dei processi di sicurezza è impossibile senza l'integrazione end-to-end di tutti gli elementi di sicurezza. Ciò richiede flussi di lavoro manuali che sprecano il tempo di tecnici della sicurezza profumatamente pagati. Aumenta inoltre la complessità della sicurezza e impone ai responsabili di avere molte competenze in termini di prodotto all'interno del team. Ad esempio, nei giorni che precedono una verifica, alcuni team devono distogliere dipendenti preposti ad altri compiti per preparare manualmente i report.

L'architettura compartimentata crea anche ridondanze nella gestione delle applicazioni e persino delle licenze software e hardware, diminuendo l'efficienza dei dipendenti dell'ufficio legale, acquisti e finanze che gestiscono tali licenze. Le organizzazioni potrebbero anche scoprire che la loro spesa tecnologica è più alta a causa dell'uso di più fornitori e della sovrapposizione di funzionalità nei diversi prodotti posseduti.

Esperienza del cliente

I distributori al dettaglio interagiscono con i clienti attraverso una serie di strumenti elettronici, tra cui infrastrutture self-service nei punti vendita (POS), app mobili e carte fedeltà. Per qualsiasi transazione POS, è necessario che siano conformi ai Payment Card Industry Data Security Standard (PCI DSS), con un reporting integrato per dimostrare la compliance. Anche le prestazioni dei sensori IoT che monitorano i livelli dei serbatoi, le temperature di refrigerazione e simili incidono sull'esperienza del cliente. Proteggere le infrastrutture di un punto vendita dalle minacce informatiche è fondamentale sia per la compliance che per il mantenimento del valore del marchio. E questo valore del marchio si riflette principalmente sui fornitori upstream, midstream e downstream, visto che il distributore generalmente espone il logo del produttore principale.

Reporting a fini di compliance

Le aziende del settore energetico sono soggette a tutta una serie di regolamentazioni e standard, dai requisiti ambientali per la trivellazione e la raffinazione alle regolamentazioni sulla sicurezza informatica. Purtroppo, un'architettura di sicurezza disaggregata rende la preparazione dei report difficile e dispendiosa in termini di tempo. La mancata dimostrazione della compliance può danneggiare la reputazione del marchio e comportare ingenti multe e sanzioni.

Casi di uso

Di seguito sono riportati alcuni dei casi di uso più prevalenti per quanto concerne la sicurezza informatica nel settore petrolchimico:

Protezione delle infrastrutture upstream

Le organizzazioni che operano nel settore dell'energia svolgendo attività estrattive devono proteggere complesse infrastrutture in luoghi remoti, sia sulla terraferma che in mare aperto. Tali siti sono obiettivi preziosi per gli hacker il cui obiettivo è l'interruzione delle attività, il terrorismo ambientale, o anche infortuni e perdite di vite umane per i dipendenti e i membri della comunità circostante.

Per proteggere questi siti, ogni aspetto della sicurezza, dai sistemi di controllo industriale alla sicurezza fisica, deve essere integrato in maniera da centralizzare la visibilità e il controllo. Le infrastrutture di sorveglianza di un piccolo sito di trivellazione dovrebbero essere protette tanto quanto quelle della sede centrale, se non di più, e dovrebbero essere ugualmente visibili al team responsabile della sicurezza.

Il **Security Fabric di Fortinet** offre al settore petrolchimico una sicurezza informatica e fisica completa e integrata. I firewall NGFW **FortiGate Rugged Series** e gli access point wireless **FortiAP Outdoor Series** forniscono una robusta protezione della sicurezza resistendo alle condizioni estreme dei siti di trivellazione ed esplorazione sulla terra ferma come in mare aperto. Questi NGFW ricevono un feed delle minacce specifico per i sistemi ICS e SCADA da **FortiGuard Labs**. **FortiCamera** e **FortiRecorder** proteggono dalle intrusioni fisiche, mentre **Fortinet Secure SD-WAN** e **Fortinet SD-Branch** creano una rete sicura sino al sito remoto e al suo interno. **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** e **FortiNAC**,, generalmente messi a disposizione dalle infrastrutture aziendali della sede centrale, garantiscono a questi siti remoti vulnerabili una sicurezza stratificata.

"Poiché i sistemi OT spesso utilizzano tecnologie più obsolete e operazioni di sicurezza meno sviluppate, la percentuale di riuscita di un attacco informatico è maggiore."[11]

"Gli Stati con elevate capacità informatiche spesso conducono operazioni di ricognizione simulando attacchi alle infrastrutture nazionali critiche per prepararsi a eventi più dirompenti."[12]

Protezione delle infrastrutture midstream

Il trasporto all'ingrosso del petrolio espande la superficie di attacco fisico di un'organizzazione di centinaia o migliaia di chilometri. Gli oleodotti sono soggetti sia a perdite accidentali che a sabotaggi fisici, e i sistemi SCADA e i dispositivi IIoT che li monitorano e li controllano sono spesso vulnerabili.[9] Un attacco riuscito può essere catastrofico, con potenziali enormi danni ambientali e perdite di vite umane.

Gli operatori midstream fanno bene a utilizzare la Purdue Enterprise Reference Architecture come standard nella progettazione delle infrastrutture elettroniche.[10] Tuttavia, se lo standard Purdue aiuta a localizzare la sicurezza nell'architettura, dà poche indicazioni su come dovrebbe essere progettata l'architettura della sicurezza informatica.

Il **Security Fabric di Fortinet** lo rende possibile con la cybersecurity integrata, la sicurezza fisica e il networking protetto. I firewall NGFW **FortiGate Rugged Series** e gli access point wireless **FortiAP Outdoor Series** garantiscono una robusta protezione della sicurezza, resistendo agli ambienti esterni remoti che gli oleodotti attraversano. **FortiCamera** e **FortiRecorder** proteggono dalle intrusioni fisiche, mentre **Fortinet Secure SD-WAN** e **Fortinet SD-Branch** forniscono una rete protetta ai distributori e altri siti remoti. Una vasta gamma di strumenti messi a disposizione dalla sede centrale garantisce una protezione stratificata. Tra questi, **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** e **FortiNAC**.

Protezione delle infrastrutture downstream

Le raffinerie trasformano il greggio in vari materiali combustibili, e questo introduce un maggiore pericolo fisico nel processo. Come le operazioni upstream e midstream, anche quelle downstream sono bersaglio di attacchi sia fisici che informatici. Entrambi i tipi di attacco possono rappresentare un notevole pericolo fisico per i dipendenti e il pubblico in generale. Gli attacchi riusciti possono anche incidere sull'economia nazionale con carenze di approvvigionamento. Le minacce possono provenire dall'esterno, dall'interno e da terzi. E se alcuni attacchi interni possono essere deliberati, altri possono essere accidentali.

Per fornire protezione in un ambiente così volatile, i team responsabili della sicurezza hanno bisogno di vedere l'intera rete e controllare le infrastrutture di sorveglianza attraverso un'unica interfaccia. Il **Security Fabric di Fortinet** protegge la sicurezza informatica e fisica in queste strutture in modo integrato e olistico. I firewall NGFW **FortiGate Rugged Series** e gli access point wireless **FortiAP OutdoorSeries** resistono a diverse sfide ambientali. **FortiCamera** e **FortiRecorder** inglobano la sicurezza fisica nel Security Fabric integrato. Un'ampia gamma di strumenti di sicurezza offre livelli di protezione, tra cui **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** e **FortiNAC**.

Protezione delle infrastrutture aziendali

Nel settore petrolchimico, le infrastrutture aziendali contengono tutta una serie di dati critici per l'attività, dai dati geologici e di esplorazione ai dati finanziari e alle informazioni personali di dipendenti e consumatori. La maggior parte delle aziende ha lavoratori remoti e in trasferta, partner terzi con accesso alle risorse aziendali e servizi in più cloud. Oltre a proteggere tali risorse dagli attacchi esterni, è fondamentale proteggerle dagli attacchi interni, siano essi opera di malintenzionati o accidentali, che espongono dati riservati.

Sebbene un'architettura di sicurezza disaggregata e la mobilità degli utenti rappresentino un ostacolo sia alla sicurezza che all'efficienza operativa, la visibilità attraverso un'unica interfaccia e il controllo centralizzato migliorano entrambi gli aspetti. L'integrazione end-to-end delle infrastrutture di sicurezza consente l'automazione del rilevamento delle minacce, la risposta e il reporting, in modo che i tecnici della sicurezza, ben pagati, possano effettivamente concentrarsi su compiti strategici.

Solo il 17% dei tecnici della sicurezza nel settore petrolchimico ritiene che sia molto probabile rilevare un attacco informatico sofisticato.[13]

Il **Security Fabric di Fortinet** fornisce un'architettura di sicurezza integrata che rende tutto questo possibile. Fortinet copre l'intera superficie di attacco, dal data center ai vari cloud, passando per il perimetro della rete, con una protezione ampia, integrata e automatizzata. Le soluzioni **Fortinet Dynamic Cloud Security** abbattono la compartimentazione tra i diversi cloud pubblici e privati, consentendo una gestione coerente delle policy. **FortiManager**, **FortiAnalyzer** e **FortiSIEM** garantiscono gestione e analisi complete. **FortiInsight** e **FortiDeceptor** aiutano a proteggere dalle minacce interne. E le aziende possono proteggere dispositivi e applicazioni, rilevando gli attacchi e rispondendovi, con **FortiWeb**, **FortiMail**, **FortiClient** e **FortiEDR.** Infine, per gli utenti mobili e i loro dispositivi, **FortiAuthenticator** e **FortiToken** consentono un accesso sicuro alla rete aziendale. La segmentazione basata sull'intent, grazie ai firewall NGFW **FortiGate**, migliora la strategia di sicurezza degli utenti remoti limitandone l'accesso ai soli dati e sistemi per i quali sia stata concessa l'autorizzazione.

Protezione dei distributori al dettaglio

Nel settore petrolchimico, i distributori al dettaglio vendono solitamente anche altri articoli, per cui sono chiamati a confrontarsi con sfide simili a quelle che si pongono ad altri dettaglianti. Utilizzano inoltre numerosi dispositivi IoT per monitorare i livelli dei serbatoi, le temperature dei frigoriferi e le telecamere IP. I serbatoi di combustibile presenti in loco aggiungono ulteriori obblighi di sicurezza e compliance che altri rivenditori non hanno, e i self-service POS esterni rappresentano un altro rischio. L'integrazione della sicurezza informatica e fisica è quindi fondamentale, così come il rispetto degli standard PCI e l'offerta di un'esperienza piacevole presso il punto vendita.

Un insieme così complesso di esigenze che riguardano l'azienda e la sicurezza rende l'integrazione end-to-end dell'architettura di sicurezza particolarmente importante per i distributori. Una siffatta infrastruttura ovvia alla necessità di processi manuali e soluzioni alternative che rallentano la risposta alle minacce distogliendo il personale dal servizio al cliente.

Le soluzioni di rete e sicurezza Fortinet aiutano a collegare diverse sedi in una catena, fornendo una robusta sicurezza di rete e automatizzando l'attività reporting a fini di compliance. I firewall **NGFW FortiGate** garantiscono una solida protezione all'intera superficie di attacco, con molte funzionalità incorporate che richiedono hardware aggiuntivo acquistabile presso altri fornitori. **Fortinet Secure SD-WAN** crea una rete sicura per tutti i punti vendita senza necessità di una costosa larghezza di banda MPLS (Multiprotocol Label Switching). E le soluzioni **Fortinet SD-Branch**, tra cui **FortiAP**, **FortiSwitch** e **FortiNAC**, estendono la sicurezza di Fortinet alle infrastrutture di ogni punto vendita.

Tali infrastrutture permettono anche di fornire servizi di sicurezza condivisi dalla sede centrale, tra cui lo strumento di gestione delle identità e degli accessi **FortiAuthenticator**, le soluzioni avanzate di sicurezza degli endpoint **FortiClient** e **FortiEDR**, l'analisi del comportamento di utenti ed entità **FortiInsight** e la deception technology **FortiDeceptor**. Inoltre, gli strumenti di gestione e analisi **FortiManager**, **FortiAnalyzer** e **FortiSIEM** consentono una visibilità attraverso un'unica interfaccia e il reporting automatico a fini di compliance rispetto a standard come il PCI Software Security Framework (SSF).[14] Le infrastrutture sono supportate da capacità integrate di intelligenza artificiale e apprendimento automatico per aiutare a rilevare e risolvere le minacce ancora ignote.

Elementi distintivi di Fortinet

Di seguito sono riportati alcuni elementi distintivi che rendono Fortinet la scelta migliore per le aziende petrolchimiche:

Architettura integrata

Il Security Fabric di Fortinet fornisce a IT e OT un'architettura di sicurezza informatica integrata, end-to-end, per ogni fase del processo di produzione, dalla protezione al rilevamento e alla risposta, in modo da garantire una maggiore visibilità e un migliore controllo.

Networking, sicurezza informatica e sicurezza fisica

Fortinet offre la possibilità di consolidare le funzioni di rete, sicurezza informatica e sorveglianza in un'unica interfaccia, che si tratti della sede centrale, di un sito di trivellazione remoto o del distributore all'angolo.

Appliance di sicurezza ruggedized

Fortinet offre un'ampia gamma di appliance ruggedized per adattarsi a tutte le esigenze ambientali e proteggere la sicurezza informatica in tutte le fasi del processo di produzione e distribuzione.

"La chiave per difendere efficacemente i sistemi SCADA è essere consapevoli dei potenziali problemi e pianificare in anticipo. Investire in una difesa efficace non è più semplicemente auspicabile. È un imperativo aziendale."[17]

Alte prestazioni

I firewall NGFW FortiGate sono in grado di operare in ambienti complessi e remoti e offrono le massime prestazioni anche con l'ispezione Secure Sockets Layer (SSL)/Transport Layer Security (TLS) attivata. Fortinet è riconosciuta leader del settore nel Gartner Magic Quadrant for Network Firewalls[15] e ha ottenuto il miglior punteggio nel NGFW Security Value Map from NSS Labs.[16]

Threat intelligence robusta

Oltre a identificare le minacce IT specifiche, FortiGuard Labs fornisce una solida threat intelligence OT specifica, frutto di 15 anni di lavoro sul campo. Per rilevare le minacce zero-day, Fortinet analizza i file da 8 anni utilizzando l'intelligenza artificiale e l'apprendimento automatico con una precisione senza precedenti.

Vasta rete di partner

Il programma Fabric-Ready Partner di Fortinet prevede la più grande rete di partner del settore con esperienza specifica nei sistemi OT e industriali.

Ampia sicurezza con dispositivi minimi

Fortinet offre un'ampia varietà di funzioni di rete e sicurezza in un'unica soluzione, laddove le soluzioni proposte dalla concorrenza spesso richiedono più dispositivi e più spese di licenza per ottenere le stesse capacità.

Conclusioni

Le aziende petrolchimiche sono responsabili di alcune delle infrastrutture più critiche al mondo, e un attacco riuscito ai danni di tali infrastrutture può comportare sconvolgimenti economici, catastrofi ambientali e persino perdite di vite umane. Fortinet offre una soluzione di sicurezza informatica e fisica ampia, integrata e automatizzata che riduce il rischio e protegge infrastrutture in espansione.

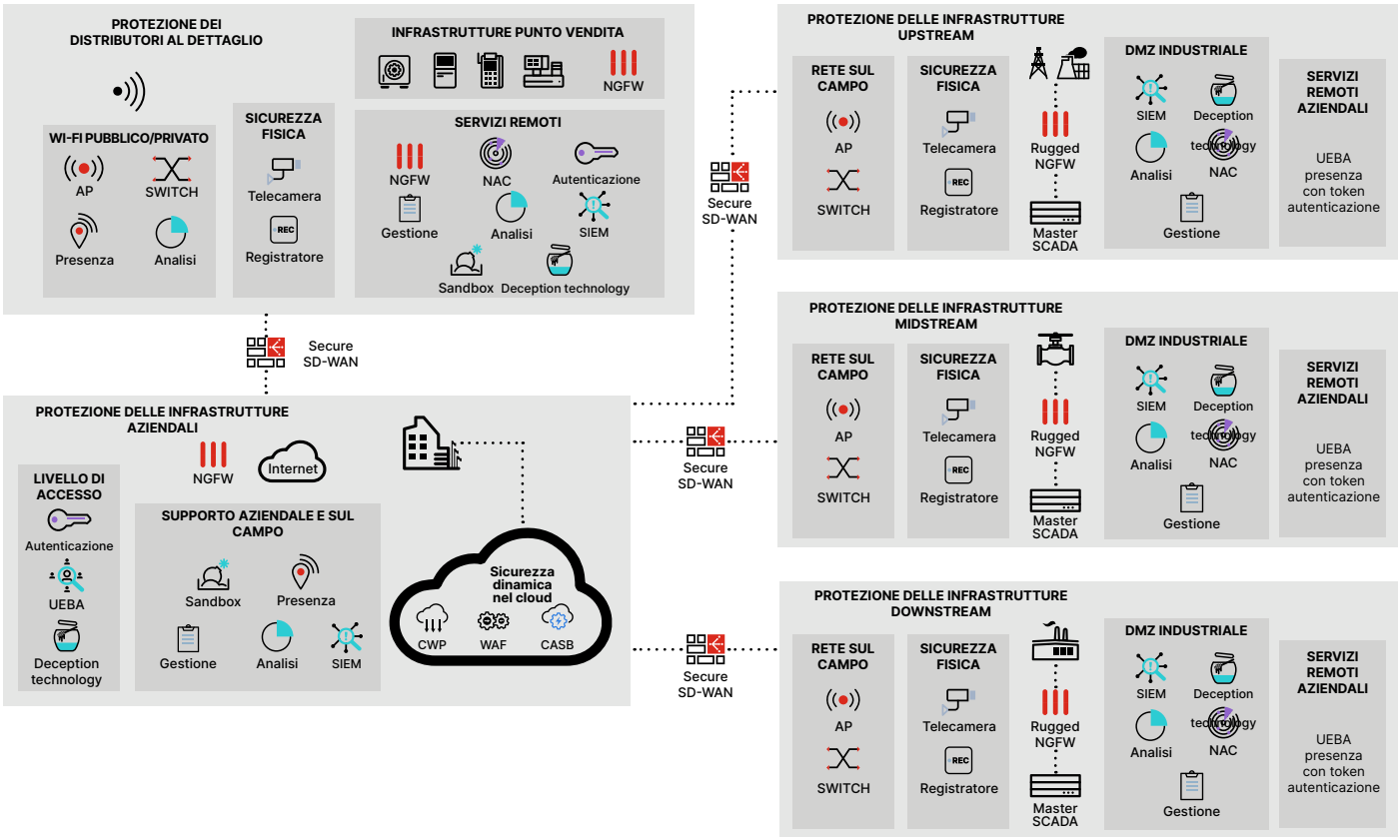

Figura 1: le soluzioni Fortinet per la sicurezza informatica nel settore petrolchimico affrontano casi di uso che abbracciano l'intero processo, dall'esplorazione alla distribuzione al dettaglio.

1 Jeff Williams, et al., "Six cybersecurity issues for oil and gas companies," EY, 12 aprile 2019.
2 "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, 28 giugno 2019.
3 Aleksander Gorkowienko, "Ensuring Oil and Gas Critical Infrastructure Security," Oil & Gas IQ, 26 giugno 2019.
4 Ibid.
5 Adlan Chaykin, "New systems, new cyber threats," Petroleum Economist, 12 novembre 2019.
6 "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019," (ISC)², 2019.
7 John Maddison, "The Problem with Too Many Security Options," Fortinet, 9 maggio 2019.
8 Vedere "Strategies That Reduce Complexity and Simplify Security Operations," Fortinet, 3 luglio 2019.
9 William T. Shaw, "SCADA System Vulnerabilities to Cyber Attack," Electric Energy Online, accesso del 21 gennaio 2020.
10 Gary Mintchell, "Purdue Enterprise Reference Architecture Meets IIoT," The Manufacturing Connection, 16 marzo 2016.
11 "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, 16 maggio 2019.
12 Adlan Chaykin, "New systems, new cyber threats," Petroleum Economist, 12 novembre 2019.
13 Jeff Williams, et al., "Six cybersecurity issues for oil and gas companies," EY, 12 aprile 2019.
14 Vedere "Complying with PCI SSF Without Sacrificing Customer Experience: What to Look for in a Security Solution," Fortinet, 24 agosto 2019.
15 "Gartner recognized Fortinet a Leader in the 2019 Magic Quadrant for Network Firewalls," Fortinet, accesso del 15 gennaio 2020.
16 "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, gennaio 2019.
17 Aleksander Gorkowienko, "Ensuring Oil and Gas Critical Infrastructure Security," Oil & Gas IQ, 26 giugno 2019.

FORTINET

www.fortinet.com

10. giugno 2022, 11:09
532367-A-1-IT