WHITEPAPER

Fortinet Cybersecurity-Lösungen für die Öl- und Gasindustrie

Wie sich kritische Infrastrukturen und Anlagen vor Cyber-Angriffen und physischen Bedrohungen mit einer End-to-End-Integration schützen lassen

Zusammenfassung

Die Infrastruktur von Öl- und Gasunternehmen trägt nicht nur zur Rentabilität eines Unternehmens bei, sondern auch zur weltweiten wirtschaftlichen und geopolitischen Stabilität. Von Bohrplätzen über Pipelines bis hin zu Raffinerien sind Förderungs- und Produktionsprozesse von Hause aus zahlreichen Risiken ausgesetzt, die Angreifer aus unterschiedlichsten Motiven ausnutzen wollen. Fortinet bietet seit über einem Jahrzehnt Cyber-Sicherheitslösungen für die Öl- und Gasindustrie an, mit denen sich durchgängige Integrationen von Cybersecurity und physischer Sicherheit für stark dezentrale Netzwerke realisieren lassen. Dazu gehören robuste Appliances für Upstream-, Midstream- und Downstream-Standorte, die selbst unter rauesten Standortbedingungen zuverlässig arbeiten und mit mehreren Sicherheitsstufen anfällige Remote-Standorte schützen. Ebenfalls ermöglicht die Fortinet Security Fabric für die Zentrale von Öl- und Gasunternehmen einen ganzheitlichen Sicherheitsansatz mit einer erweiterten Security-Architektur bis hin zur Tankstelle sowie sicheren Netzwerk-Verbindungen zwischen allen Standorten.

60 % der Öl- und Gasunternehmen erlebten kürzlich einen ernsten Cyber-Sicherheitsvorfall.[1]

Öl- und Gasunternehmen besitzen und verwalten große Teile kritischer Infrastruktur, die nicht nur für den Unternehmensbetrieb, sondern auch für die Wirtschaft und Verteidigung eines Landes von entscheidender Bedeutung sind. Upstream-, Midstream- und Downstream-Operationen sind für Cyber-Gegner aus unterschiedlichsten Gründen lohnende Ziele, die von der persönlichen Bereicherung bis hin zur Industriespionage oder dem Lahmlegen von Teilen der Wirtschaft reichen.[2] Wie ein Autor es treffend ausdrückt: „Jeder Teil der Öl- und Gas-Wertschöpfungskette ist derzeit exponiert und herkömmliche statische Abwehrmaßnahmen reichen nicht mehr aus.“[3]

Auch wenn diese Aussage auf den ersten Blick übertrieben erscheinen mag, das Risiko ist real. Ein Angriff auf das SCADA-System (Supervisory Control and Data Acquisition) einer Offshore-Bohrinsel, Ölquelle, Pipeline oder Raffinerie – oder auch auf IoT-Geräte (Internet der Dinge), die Monitoring-Daten für diese industrielle Steuerungstechnik liefern – kann verheerende Folgen haben:[4] kostspielige Schäden bei Anlagen und Standorten, längere Versorgungsunterbrechungen oder schlimmstenfalls sogar Verletzungen und Todesfälle bei Mitarbeitern, Umstehenden und Anwohnern.

Solche Angriffe auf die Infrastruktur der Betriebstechnologie (OT) werden immer häufiger[5] und die Unternehmens-infrastruktur von Öl- und Gasunternehmen ist ebenfalls ein Ziel. Erfolgreiche Angriffe können Geschäftsgeheimnisse sowie geistiges Eigentum wie Explorations- und Messdaten von Förderungsstandorten preisgeben oder auch die Datensicherheit von Finanz- und Personalinformationen gefährden. Abgesehen von den geschäftlichen Problemen, die solche Angriffe verursachen können, drohen womöglich Bußgelder oder Verfahren wegen Compliance-Verstößen.

Fortinet bietet seit über einem Jahrzehnt umfassende Sicherheitslösungen für die Öl- und Gasindustrie an. Diese Lösungen decken alles ab – von Bohrstellen an Land und Offshore-Bohrinseln bis hin zu Raffinerien, Pipelines und der „Tankstelle an der Ecke“. Im Mittelpunkt des Fortinet-Angebots steht die Security Fabric, die eine durchgängige Sicherheitsintegration von Ende zu Ende über die erweiterte Infrastruktur von Öl- und Gasunternehmen ermöglicht.

Zentrale Herausforderungen für die Cybersecurity in der Öl- und Gasindustrie

Zu den wichtigsten Herausforderungen für die Cyber-Sicherheit in der Öl- und Gasbranche gehören:

Kostenoptimierung

Der Öl- und Gasmarkt ist für seine starken Preisschwankungen bekannt. Diese Volatilität bedeutet, dass ein Unternehmen innerhalb weniger Tage seine Rentabilität einbüßen und Betriebsverluste erleiden kann. Daher hat die Kostenminimierung für Öl- und Gasunternehmen stets Priorität und Betriebsstrukturen sind darauf ausgerichtet, auch Niedrigpreis-Perioden gut zu überstehen.

In diesem Umfeld kommt der Austausch teurer, älterer Geräte wegen Schwachstellen manchmal nicht in Frage und erfordert kreative Ansätze, um diese anfälligen Geräte zu schützen. Wie auch immer so ein Schutz aussehen mag – er muss so gestaltet sein, dass die Sicherheit den Betrieb nicht behindert. Viele Unternehmen haben mehrere Infrastrukturbereiche mit solchen Schwachstellen, was das Cybersecurity-Team mit einem hohen Arbeitsaufwand belastet.

Der Fachkräftemangel im Bereich Cyber-Sicherheit wird immer schlimmer: Schätzungsweise fehlen heute über 4 Millionen IT-Experten, um die rund 2,8 Millionen Security-Mitarbeiter zu entlasten.[6] Das bedeutet, dass eine Lösung dieses Problems durch Neueinstellungen oft kostspielig ist – wenn man überhaupt einen qualifizierten Security-Experten finden kann. Doch unabhängig davon können auch Personalaufstockungen das Kernproblem nicht lösen: Mit manuellen Sicherheitsprozessen lassen sich keine der heutigen hochkomplexen Bedrohungen abwehren, die sich mit Maschinengeschwindigkeit bewegen.

Transparenz über IT- und OT-Systeme hinweg

Industrielle IoT-Geräte (IIoT) haben die Sicherheitsanforderungen von SCADA-Systemen (Supervisory Control and Data Acquisition) zum Management von Bohrstellen, Pipelines und Raffinerien grundlegend verändert. Mit dem Internet verbundene Sensoren und angeschlossene Steuerungsgeräte beseitigen das Air Gap, durch das SCADA-Systeme bislang relativ sicher vor Cyber-Angriffen aus dem Internet waren.

Dadurch erweitert sich die Angriffsfläche eines Unternehmens. Verschärft wird dieses Problem durch die fehlende Überwachung vieler IIoT-Geräte, die nicht durch Aktualisieren der Client-Security-Software geschützt werden können – manchmal sind nicht einmal Firmware-Updates möglich. Um diese Sicherheitslücken zu schließen, implementieren Unternehmen häufig mehrere Einzelprodukte.[7] Diese isolierten „Sicherheits-Inseln" führen zu Komplexität[8] und mangelnder Transparenz und verzögern so die Erkennung, Verhinderung und Abwehr von Bedrohungen. Dadurch steigt das Risiko, dass ein schnell ausgeführter Angriff die Security aushebeln kann – einfach aus dem simplen Grund, dass manuelle Reaktionen zu langsam sind.

Operative Effizienz

Eine fragmentierte Security-Architektur verringert die operative Effizienz des Cybersecurity-Teams zunehmend. Sicherheitsprozesse lassen sich nicht automatisieren, weil eine End-to-End-Integration aller Security-Komponenten fehlt. Dem Unternehmen bleibt nichts anderes übrig, als hochbezahlte Security-Experten mit manuellen Routine-Aufgaben zu betreuen. Die Security wird dadurch immer komplexer und lässt sich bestenfalls nur noch mit einem Team aus Experten in den Griff bekommen, die sich mit unterschiedlichsten Produkten sehr gut auskennen. Diese „Strategie" führt dann zu weiteren Sicherheitsproblemen, wenn das ohnehin unterbesetzte Expertenteam im Vorfeld von Audits mehrere Tage von seinen Kernaufgaben abgezogen wird, um manuell Compliance-Berichte zu erstellen.

Isolierte Bereiche in der Security-Architektur führen zudem zu Redundanzen, z. B. beim Anwendungs-Management oder bei der Software- und Hardware-Lizenzierung. Darunter leidet auch die Effizienz anderer Unternehmensbereiche, die die Lizenzierung betreuen – von der Rechtsabteilung bis hin zum Einkauf und Finanzwesen. In einigen Unternehmen steigen sogar die Technologie-Ausgaben: Aufgrund der vielen Anbieter und Security-Einzelprodukte überschneiden sich Sicherheitsfunktionen, die dann doppelt oder dreifach bezahlt werden müssen.

Kundenerfahrung

Tankstellen interagieren mit Kunden über zahlreiche Technologien – von der POS-Infrastruktur (Point-of-Sale) bis hin zu Smartphone-Apps und Kundenkarten. Alle Anwendungen für POS-Transaktionen müssen den PCI-DSS-Standard für Kreditkartenzahlungen erfüllen und integrierte Berichtsfunktionen zum Nachweis der Informationssicherheit umfassen. Die Leistung von IoT-Sensoren zur Überwachung von Dingen wie Tankfüllständen oder Kühltemperaturen wirkt sich ebenfalls auf das Kundenerlebnis aus. Der Schutz der Infrastruktur eines Tankstellenstandorts vor Cyber-Bedrohungen ist sowohl für die Compliance als auch für die Image-Pflege – Stichwort „Markenwert" – überaus wichtig. Denn der Wert einer Marke hat Einfluss auf Upstream-, Midstream- und Downstream-Anbieter, da diese Einzelhändler in der Regel die wichtigsten Öl- und Gaserzeuger präsentieren.

Compliance Reporting

Energieunternehmen unterliegen zahlreichen Vorschriften und Normen – von speziellen Umgebungsanforderungen und Cybersecurity-Standards bis hin zu Umweltvorgaben für Bohrungen und Raffinieren. Mit einer Sicherheitsarchitektur aus vielen isolierten Einzelprodukten ist die Berichterstellung schwierig und zeitaufwändig. Ist aber die Compliance nicht nachweisbar, kann dies den Ruf des Unternehmens schädigen sowie hohe Bußgelder und Strafen nach sich ziehen.

Anwendungsfälle

Im Folgenden finden Sie einige der häufigsten Cybersecurity-Anwendungsfälle für Öl- und Gasunternehmen:

Security für die Upstream-Infrastruktur

Unternehmen, die an der Energiegewinnung beteiligt sind, müssen eine komplexe Infrastruktur mit Remote-Standorten an Land und Offshore schützen. Diese Standorte sind für Hacker interessant, die es auf Betriebsstörungen, Umweltterrorismus oder schlimmstenfalls auf Verletzungen und Todesfälle bei Mitarbeitern und Anwohnern abgesehen haben.

Um solche Standorte zu schützen, muss jeder Sicherheitsaspekt – von der industriellen Steuerungstechnik bis hin zur physischen Security – so integriert werden, dass das Unternehmen eine zentrale, umfassende Transparenz und Kontrolle erhält. Auch sollte die Überwachungsinfrastruktur an einem kleinen Bohrstandort genauso stark wie die Unternehmenszentrale geschützt werden und vom Security-Team mit gleicher Transparenz einsehbar sein.

Die **Fortinet Security Fabric** bietet eine umfassende, integrierte Cybersecurity und physische Sicherheit für die Öl- und Gasindustrie. Die Next-Generation-Firewalls (NGFWs) der **FortiGate Rugged-Serie** und die drahtlosen Access Points der

FortiAP Outdoor-Serie zeichnen sich durch ihren robusten Sicherheitsschutz aus und können problemlos in den rauen Umgebungsbedingungen von Bohr- und Förderstandorten an Land und im Meer eingesetzt werden. Diese NGFWs erhalten von den **FortiGuard Labs** laufend aktuelle Bedrohungsinformationen speziell für Steuerungstechnik (ICS) und SCADA-Systeme. Mit der **FortiCamera** und dem **FortiRecorder** lassen sich Gelände und Anlagen vor unbefugtem Betreten schützen und so eine physische Zugangssicherung erreichen.
Die sichere Vernetzung des Remote-Standorts und der Schutz des internen Standort-Netzwerks erfolgen mit dem **Fortinet Secure SD-WAN** und **Fortinet SD-Branch**. **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** und **FortiNAC** werden in der Regel über die Infrastruktur der Unternehmenszentrale bereitgestellt und bieten zusätzliche Sicherheitsstufen für diese anfälligen Remote-Standorte.

„Da OT-Systeme oft veraltete Technologien nutzen und die Security Operations hier eher rudimentär ablaufen, haben Angreifer bei Betriebstechnologie eine höhere Erfolgsquote.“[11]

„Staaten mit hohen Cybersecurity-Standards testen eigene kritische Infrastrukturen regelmäßig mit Ausspäh-Aktionen (Reconnaissance Operations), um besser auf umfassende Störungen der kritischen Infrastruktur vorbereitet zu sein.“[12]

Security für die Midstream-Infrastruktur

Der Großhandelstransport von Erdöl erweitert die physische Angriffsfläche eines Unternehmens um Hunderte oder Tausende von Kilometern. Pipelines sind durch Lecks in Folge von Unfällen oder Sabotage gefährdet und werden häufig durch anfällige SCADA-Systeme (Supervisor Control and Data Acquisition) gesteuert und IIoT-Geräte (Industrielles Internet der Dinge) überwacht.[9] Ein erfolgreicher Angriff kann katastrophal sein und schlimmstenfalls zu massiven Umweltschäden und Todesfällen führen.

Midstream-Betreiber tun daher gut daran, die elektronische Infrastruktur nach der Purdue-Enterprise-Referenzarchitektur zu gestalten.[10] Allerdings deckt der klassische Purdue-Standard lediglich die physische Sicherheit ab und hilft wenig beim Design der Cybersecurity-Architektur.

Die **Fortinet Security Fabric** ermöglicht dies durch eine integrierte Cybersecurity, physische Sicherheit und Netzwerk-Security. Die NGFWs der **FortiGate Rugged-Serie** und die drahtlosen Access Points der **FortiAP Outdoor-Serie** zeichnen sich durch ihren robusten Sicherheitsschutz aus und können problemlos im Außenbereich von Remote-Standorten eingesetzt werden, um Pipelines zu schützen. Die **FortiCamera** und der **FortiRecorder** schützen das Gelände und Anlagen vor unbefugtem Betreten und schaffen eine physische Zugangssicherung, während das Fortinet **Secure SD-WAN** und **Fortinet SD-Branch** Pumpstationen und andere Remote-Standorte sicher mit dem Netzwerk verbinden. Von der Unternehmenszentrale werden zahlreiche Security-Tools bereitgestellt, die für zusätzlichen Schutz sorgen: **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** und **FortiNAC** – um nur einige zu nennen.

Security für die Downstream-Infrastruktur

Raffinerien verarbeiten Rohöl zu unterschiedlichsten Brennstoffen und sind schon allein deshalb Hochrisiko-Standorte. Zusätzlich sind Upstream-, Midstream- und Downstream-Operationen durch physische und Cyberangriffe gefährdet. Beide Arten von Angriffen können eine erhebliche physische Gefahr für Mitarbeiter und die allgemeine Öffentlichkeit darstellen. Ist ein Angriff erfolgreich, kann das Folgen für die gesamte Volkswirtschaft haben und zu Versorgungsengpässen führen. Eine Bedrohung kann von außen, aus dem Unternehmen selbst oder von Dritten ausgehen. Manche Insider-Angriffe erfolgen absichtlich, andere aus Versehen.

Um derart volatile Standorte zu schützen, benötigen Security-Teams eine zentrale Übersicht über das gesamte Netzwerk und die Überwachungsinfrastruktur. Die **Fortinet Security Fabric** schützt diese Anlagen mit einer integrierten, ganzheitlichen Sicherheit, die sowohl die Cybersecurity als auch die physische Sicherheit abdeckt. Die NGFWs der **FortiGate Rugged-Serie** und die drahtlosen Access Points der **FortiAP Outdoor-Serie** halten einer Vielzahl von Umwelteinflüssen stand, zeichnen sich durch ihren robusten Sicherheitsschutz aus und können problemlos unter schwierigen Umgebungsbedingungen eingesetzt werden. Die **FortiCamera** und der **FortiRecorder** erweitern die integrierte Security Fabric um einen zusätzlichen physischen Standortschutz. Über die Unternehmenszentrale werden zahlreiche Security-Tools bereitgestellt, die zusätzliche Sicherheit bieten: **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** und **FortiNAC**.

Sichere Unternehmensinfrastruktur

Die Unternehmensinfrastrukturen von Öl- und Gasunternehmen enthalten eine Vielzahl geschäftskritischer Daten, von geologischen, Explorations- und Finanzdaten bis hin zu persönlichen Informationen von Mitarbeitern und Verbrauchern. In den meisten Unternehmen gibt es zudem Mitarbeiter im Homeoffice, Außendienst-Teams und externe Partner, die alle auf

Unternehmensressourcen und -dienste in mehreren Clouds zugreifen müssen. Neben dem Schutz dieser Ressourcen vor externen Angriffen muss unbedingt ein Offenlegen vertraulicher Daten durch versehentliche oder böswillige Insider-Angriffe verhindert werden.

Während eine disaggregierte Security-Architektur und mobile Anwender sowohl die Sicherheit als auch die betriebliche Effizienz verschlechtern, bringen eine zentrale Transparenz und Kontrolle Verbesserungen in beiden dieser Bereiche. Eine von Ende zu Ende integrierte Security-Infrastruktur bietet Vorteile wie eine automatisierte Bedrohungserkennung, Bedrohungsabwehr und Berichterstellung und entlastet hochbezahlte Security-Experten, die sich dann auf strategische Aufgaben konzentrieren können.

Nur 17 % der Security-Experten in der Öl- und Gasindustrie halten es für sehr wahrscheinlich, dass sie einen hochkomplexen Cyber-Angriff bemerken würden.[13]

Genau das ist mit der **Fortinet Security Fabric** möglich: Unternehmen erhalten eine umfassende, integrierte und automatisierte Sicherheit für die gesamte Angriffsfläche – vom Rechenzentrum über mehrere Clouds bis hin zum Netzwerk-Rand. Mit den **Fortinet Dynamic Cloud Security**-Lösungen werden isolierte Sicherheitsbereiche abgeschafft. IT-Teams müssen nicht mehr die Sicherheits-funktionen für jede Public und Private Cloud einzeln konfigurieren, sondern können einheitliche Richtlinien im gesamten Unternehmen konsequent durchsetzen. **FortiManager**, **FortiAnalyzer** und **FortiSIEM** bieten umfassende Management- und Analytik-Funktionen, während **FortiInsight** und **FortiDeceptor** Insider-Bedrohungen abwehren. Außerdem können Unternehmen mit **FortiWeb**, **FortiMail**, **FortiClient** und **FortiEDR** sämtliche Geräte und Anwendungen schützen sowie Angriffe erkennen und darauf reagieren. Mobile Anwender und Geräte erhalten mit dem **FortiAuthenticator** und **FortiToken** einen sicheren Zugang zum Unternehmensnetzwerk. Zudem verbessert die absichtsbasierte Segmentierung mit **FortiGate** NGFWs das Sicherheitsprofil von Remote-Anwendern, indem der Zugriff auf Daten und Systeme präzise an die eingeräumten Benutzerrechte geknüpft wird.

Security für den Öl- und Gashandel

Im Öl- und Gashandel wie z. B. auf Tankstellen werden meistens auch andere Artikel angeboten. Verkaufsstandorte in dieser Branche stehen daher vor ähnlichen Herausforderungen wie andere Einzelhändler mit Ladengeschäften. In vielen Verkaufsstandorten gibt es zudem zahlreiche IP-Kameras und IoT-Geräte (Internet der Dinge), um z. B. Tankfüllungen abzufragen oder Kühlschrank-Temperaturen im Blick zu behalten. Die Anforderungen an die Sicherheit und Regelkonformität sind jedoch höher als im klassischen Einzelhandel, da sich auf dem Grundstück auch Kraftstofftanks, Selbstbedienungstechnologie wie Zapfsäulen und Verkaufsstände unter freiem Himmel befinden. Deshalb müssen nicht nur die physische Sicherheit und Cybersecurity integriert, sondern auch Normen wie der PCI-Standard für Kartenzahlungen eingehalten werden. Und natürlich muss das Einkaufserlebnis stimmen.

Aufgrund dieser komplexen Geschäfts- und Sicherheitsanforderungen ist eine durchgängige Integration der Security-Architektur für Tankstellen und andere Verkaufsstandorte des Gas- und Ölhandels besonders wichtig. Durch eine solche Security-Infrastruktur entfallen manuelle Vorgehensweisen und Workarounds, die die Bedrohungsabwehr verlangsamen und Mitarbeiter von ihrer eigentlichen Aufgabe ablenken: Kunden einen ausgezeichneten Service zu bieten.

Mit den Netzwerk- und Security-Lösungen von Fortinet können Sie verschiedene Standorte einer Kette vernetzen und erhalten zudem eine robuste Netzwerk-Sicherheit sowie automatisierte Compliance-Berichte. **FortiGate NGFWs** bieten einen robusten Schutz für die gesamte Angriffsfläche und haben bereits viele Funktionen integriert, die bei anderen Anbietern extra als Hardware zugekauft werden müssen. Mit dem **Fortinet Secure SD-WAN** erhalten Sie ein sicheres Netzwerk für alle Niederlassungen, das sich ohne eine teure MPLS-Bandbreite (Multiprotocol Label Switching) realisieren lässt. Ein weiterer Vorteil: **Fortinet SD-Branch**-Lösungen wie **FortiAP**, **FortiSwitch** und **FortiNAC** erweitern die Fortinet-Security auf die Infrastruktur jeder Tankstelle sowie anderer Geschäftsstandorte.

Diese Infrastruktur ermöglicht auch die Bereitstellung gemeinsamer Sicherheitsdienste von der Unternehmenszentrale aus, wie z. B. **FortiAuthenticator** für die Identitäts- und Zugangsverwaltung, **FortiClient** und **FortiEDR** für die erweiterte Endpunkt-Sicherheit, **FortiInsight** für Benutzer- und Entitätsverhaltensanalysen (UEBA) oder **FortiDeceptor** – eine Täuschungstechnologie, die Angreifern Fallen stellt. Zusätzlich erhalten Unternehmen mit dem **FortiManager**, **FortiAnalyzer** und **FortiSIEM** praktische Management- und Analysetools, die zentrale Transparenz und automatisierte Compliance-Berichte zur Einhaltung von Standards wie PCI SSF (Software Security Framework) bieten.[14]
Diese Infrastruktur wird durch integrierte Funktionen für künstliche Intelligenz (KI) und maschinelles Lernen (ML) unterstützt, um auch unbekannte Bedrohungen zu erkennen und abzuwehren.

Alleinstellungsmerkmale: Warum Fortinet?

Für Unternehmen aus der Öl- und Gasindustrie sprechen viele gute Gründe für Fortinet-Lösungen. Wir haben kurz die wichtigsten Alleinstellungsmerkmale zusammengestellt:

Integrierte Architektur

Die Fortinet Security Fabric bietet eine durchgängige, integrierte Security-Architektur für IT und OT. Öl- und Gasunternehmen erhalten damit eine Komplettlösung von einem einzigen Anbieter für jede Phase des Erzeugungs- und Produktionsprozesses, die vom Schutz bis zur Erkennung und Abwehr von Bedrohungen alles abdeckt. Das schafft mehr Transparenz und verbessert die Kontrolle.

Netzwerk, Cybersecurity und physische Sicherheit

Mit Fortinet lassen sich Funktionen wie Netzwerk, Cybersecurity und Überwachung konsolidieren und zentral steuern – ob in der Unternehmenszentrale, an entfernten Bohrstandorten oder in der „Tankstelle an der Ecke".

„Entscheidend für einen wirksamen Schutz von SCADA-Systemen ist, sich potenzieller Probleme bewusst zu sein und vorauszuplanen. Die Investition in eine effektive Verteidigung ist heutzutage keine Option mehr, sondern eine geschäftliche Notwendigkeit."[17]

Robuste Security-Appliances

Fortinet bietet eine breite Auswahl an robusten Geräten, um sämtlichen Umweltanforderungen gerecht zu werden und einen Cyber-Sicherheitsschutz für alle Phasen des Produktions- und Lieferprozesses zu gewährleisten.

Starke Performance

FortiGate NGFWs umfassen spezielle Funktionen für komplexe Remote-Umgebungen und bieten selbst bei aktivierter SSL/TLS-Prüfung (Deep Secure Sockets Layer/Transport Layer Security) eine hohe Leistung. Fortinet wird im Gartner Magic Quadrant für Netzwerk-Firewalls als Leader eingestuft[15] und hat in der NGFW Security Value Map der NSS Labs die höchste Punktzahl erzielt.[16]

Verlässliche Bedrohungsinformationen

Neben der Identifizierung von IT-Bedrohungen liefern die FortiGuard Labs auch zuverlässige Threat Intelligence speziell für OT-Systeme und bieten eine Fachkompetenz, in die 15 Jahre Security-Expertise einfließen. Um Zero-Day-Bedrohungen zu erkennen, analysiert Fortinet seit acht Jahren Dateien mithilfe künstlicher Intelligenz (KI) und maschinellem Lernen (ML) mit beispielloser Präzision.

Umfangreiches Partner-Netzwerk

Das Fortinet Fabric-Ready-Partnerprogramm umfasst das branchenweit größte Netzwerk von Partnern mit Fachkenntnissen zu Betriebstechnologie (OT) und Industriesystemen.

Umfassende Sicherheit mit minimaler Hardware

Fortinet bietet eine Vielzahl von Security- und Netzwerk-Funktionen als Komplettlösung an. Bei anderen Anbietern müssen Sie oft mehrere Geräte und Lizenzen kaufen, um die gleiche Funktionalität zu erhalten.

Fazit

Öl- und Gasunternehmen sind für einige der kritischsten Infrastrukturen der Welt verantwortlich. Erfolgreiche Angriffe können in diesem Sektor zu wirtschaftlichen Störungen, Umweltkatastrophen und schlimmstenfalls zu Todesfällen führen. Mit Fortinet erhält die Öl- und Gasindustrie eine umfassende, integrierte und automatisierte Security-Lösung, die mit hoher Wirksamkeit vor Cyber-Attacken und physischen Angriffen schützt, Risiken reduziert und Sicherheit für stark dezentrale Infrastrukturen bietet.

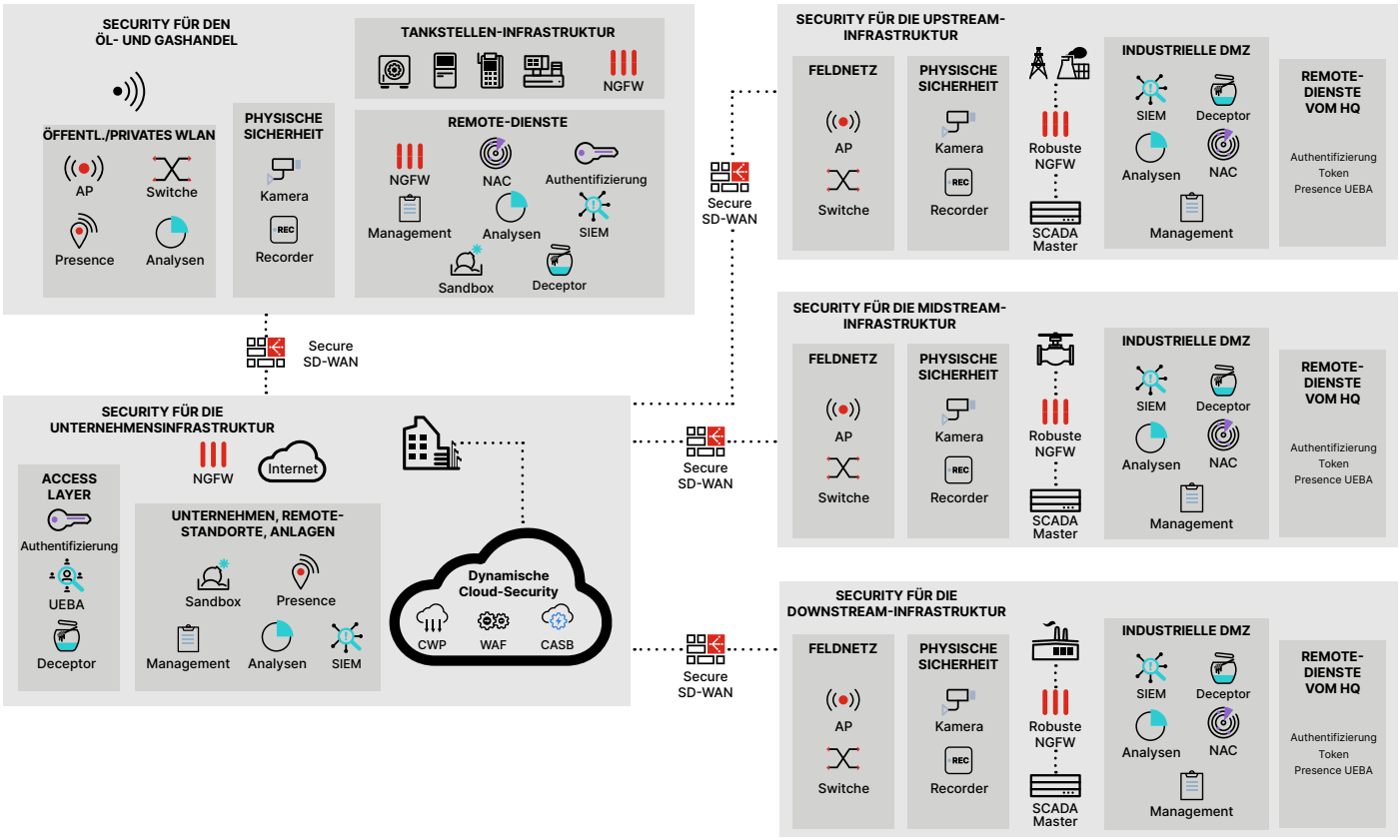

Abbildung 1: Cybersecurity-Lösungen von Fortinet für Öl- und Gasunternehmen wurden für Anwendungsfälle entwickelt, die den gesamten Prozess von der Exploration bis zur Tankstelle schützen.

1 Jeff Williams, et al.: „Six cybersecurity issues for oil and gas companies“. EY, 12. April 2019.
2 „Independent Study Pinpoints Significant SCADA/ICS Security Risks“. Fortinet, 28. Juni 2019.
3 Aleksander Gorkowienko: „Ensuring Oil and Gas Critical Infrastructure Security“. Oil & Gas IQ, 26. Juni 2019.
4 Ebd.
5 Adlan Chaykin: „New systems, new cyber threats“. Petroleum Economist, 12. November 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. Mai 2019.
8 Siehe: „Strategies That Reduce Complexity and Simplify Security Operations“. Fortinet, 3. Juli 2019.
9 William T. Shaw: „SCADA System Vulnerabilities to Cyber Attack“. Electric Energy Online, abgerufen am 21. Januar 2020.
10 Gary Mintchell: „Purdue Enterprise Reference Architecture Meets IIoT“. The Manufacturing Connection, 16. März 2016.
11 „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.
12 Adlan Chaykin: „New systems, new cyber threats“. Petroleum Economist, 12. November 2019.
13 Jeff Williams, et al.: „Six cybersecurity issues for oil and gas companies“. EY, 12. April 2019.
14 Siehe: „Complying with PCI SSF Without Sacrificing Customer Experience: What to Look for in a Security Solution“. Fortinet, 24. August 2019.
15 „Gartner recognized Fortinet a Leader in the 2019 Magic Quadrant for Network Firewalls“. Fortinet, abgerufen am 15. Januar 2020.
16 „Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests“. Fortinet, Januar 2019.
17 Aleksander Gorkowienko: „Ensuring Oil and Gas Critical Infrastructure Security“. Oil & Gas IQ, 26. Juni 2019.

FORTINET

www.fortinet.com/de

20. Juni 2022, 11:43
532367-A-1-DE