FORTINET

WHITEPAPER

Digitale Innovationen mit der Fortinet Security Fabric

Umfassend, integriert und automatisiert

Zusammenfassung

Initiativen für digitale Innovationen (DI) werden derzeit in vielen Unternehmen in rasantem Tempo umgesetzt. Die Ziele sind klar: schnellere Geschäftsabläufe, Kostensenkungen, Effizienzsteigerung und bessere Kundenerfahrungen. Die meisten Initiativen umfassen die Verlagerung von Anwendungen und Workflows in die Cloud, die Implementierung von IoT-Geräten (Internet der Dinge) im Unternehmensnetzwerk und die Erweiterung der Unternehmenspräsenz mit neuen Filialen und Niederlassungen.

Doch dieser Infrastruktur-Ausbau bringt neue Sicherheitsrisiken wie wachsende Angriffsflächen, ausgefeiltere Bedrohungen und eine komplexere Infrastruktur mit sich – gefolgt von einer Flut neuer Vorschriften. Damit digitale Innovationen halten, was sie versprechen, müssen Risiken effektiv gemeistert und Komplexitäten minimiert werden. Dies gelingt jedoch nur mit einer Cyber-Security-Plattform, die Transparenz über alle Umgebungen bietet und die Security Operations und Network Operations mit einem einfachen Management unterstützt.

Die Fortinet Security Fabric löst diese Herausforderungen mit umfassenden, integrierten und automatisierten Lösungen, die sicherheitsorientierte Netzwerke, einen Zero-Trust-Netzwerkzugang, eine dynamische Cloud-Sicherheit und Sicherheitsprozesse mit künstlicher Intelligenz (KI) ermöglichen. Zur Erweiterung des Fortinet-Angebots gibt es zudem zahlreiche nahtlos integrierbare Drittprodukte, die die Lücken in Security-Architekturen minimieren und gleichzeitig für eine maximale Kapitalrendite (ROI) von Investitionen in die Sicherheit sorgen.

84 % der Security-Manager glauben, dass das Risiko von Cyber-Angriffen steigen wird.[1]

77 % der Security-Experten berichten, dass in ihrem Unternehmen ungeachtet von Sicherheitsbedenken Anwendungen oder Infrastrukturen in die Cloud verlagert wurden.[3]

Digitale Innovationen verändern alle Branchen

Weltweit gelten digitale Innovationen (DI) in allen Branchen als Muss für das Geschäftswachstum und die Verbesserung der Kundenerfahrung. CIOs stehen ihren DI-Initiativen generell positiv gegenüber: 61 % geben an, dass sie bereits umfassend mit der Cloud, dem Internet der Dinge (IoT) und mobilen Lösungen arbeiten.[2]

Aus der Sicht der führenden Anbieter von Cloud-Plattformen und Cyber-Security bringen digitale Innovationen zahlreiche Änderungen für Netzwerk-Umgebungen mit sich. Zunehmend mobilere Benutzer greifen von Standorten und mit Endgeräten auf das Netzwerk zu, über die das IT-Team eines Unternehmens oft keine Kontrolle hat. Auch werden direkte Verbindungen zu Public Clouds hergestellt, um wichtige Geschäftsanwendungen wie Office 365 zu verwenden. Die Fülle solcher Benutzergeräte wird noch durch die Masse an IoT-Geräten übertroffen, die sich überall im Netzwerk befinden – häufig an entfernten, unüberwachten Orten. Hinzu kommen die stark dezentralen Infrastrukturen von Cloud-Anbietern mit entlegenen Standorten, die sich direkt mit der Cloud und Mobilfunknetzen verbinden und damit die Rechenzentren von Unternehmen umgehen.

Durch all diese Änderungen ist das herkömmliche Konzept der Bedrohungsabwehr am Netzwerk-Rand zum Scheitern verurteilt und verlangt vom Cloud-Anbieter eine neue mehrstufige Security-Strategie.

Migration von Anwendungen und Workloads in die Cloud

Fast jedes Unternehmen hat damit begonnen, einige Workloads und Anwendungen in die Cloud zu verlagern – oder plant dies zumindest. Diese Entscheidungen beruhen oft auf dem Wunsch, mit einer flexiblen Cloud-Lösung Kosten zu senken und die betriebliche Effizienz und Skalierbarkeit zu verbessern.

Die Auswahl an Cloud-Modellen ist groß: Unternehmen können SaaS-Anwendungen (Software-as-a-Service) und SaaS-Services wie Salesforce oder Box nutzen oder für On-Premises-Umgebungen entwickelte und implementierte Software als IaaS (Infrastructure-as-a-Service) oder PaaS (Platform-as-a-Service) über Anbieter wie Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure oder IBM Cloud bereitstellen.

Viele entscheiden sich für eine Multi-Cloud-Infrastruktur, um nicht an einen Cloud-Anbieter gebunden zu sein und die jeweils am besten geeignete Cloud für Anwendungen und Workloads zu nutzen. Der Nachteil ist jedoch, dass sich Unternehmen mit den Besonderheiten jeder Cloud-Umgebung befassen müssen. Auch erfordert jede Umgebung unterschiedliche Management- und Security-Tools. Das geht nicht nur zu Lasten der Transparenz. Auch muss beim Richtlinien-Management, Reporting und anderen Aufgaben mit mehreren Konsolen gearbeitet werden.

Fülle an Endgeräten in mehreren Umgebungen

Endgeräte sind mit Abstand die am stärksten gefährdeten Knoten im Netzwerk eines Cloud-Anbieters. Die größeren Anbieter beschäftigen Tausende von Mitarbeitern, von denen jeder mit verschiedenen geschäftlichen und persönlichen Geräten auf Netzwerk-Ressourcen zugreift. Das Sicherstellen einer Cyber-Hygiene und aktuellen Endpunkt-Security auf all diesen Geräten ist eine Mammutaufgabe. Doch eine noch größere Herausforderung stellen die unzähligen IoT-Geräte dar: Schon Ende 2019 waren es über 26,66 Milliarden Geräte – und laut Schätzungen von Experten dürfte diese Zahl 2020 auf 31 Milliarden steigen.[5]

IoT-Geräte sind in zahlreichen Geschäftskontexten vorhanden: Sie bieten Einzelhandelskunden und Hotelgästen personalisierte Erlebnisse, verfolgen den Lagerbestand in der Fertigung und Logistik und überwachen Geräte in Fabrikhallen oder Kraftwerken.

IoT-Geräte sind in der Regel robust, energieeffizient und legen den Schwerpunkt auf die Leistung – leider auf Kosten von Security-Funktionen und sicheren Kommunikationsprotokollen. Anders als die meisten Geräte im Netzwerk befinden sich IoT-Geräte häufig an entfernten Standorten, im Freien oder in unbesetzten bzw. selten besetzten Einrichtungen (wie Kraftwerken) – und übertragen von diesen unsicheren Standorten unablässig kritische, sensible Daten an On-Premises-Rechenzentren und Cloud-Dienste.

Erweiterte Geschäftspräsenz über verteilte Märkte und Regionen hinweg

Erweitern Unternehmen ihre internationale Präsenz um neue Werke, Niederlassungen und andere dezentrale Standorte, kommt es häufig zu einer eingeschränkten WAN-Bandbreite (Wide Area Network): Zwar steigern SaaS-Anwendungen, Videokonferenzen und VoIP (Voice over IP) die Produktivität und ermöglichen neue Leistungsangebote, tragen jedoch auch zu einem exponentiellen Wachstum des WAN-Traffics bei.

Seit vielen Jahren laufen WAN-Verbindungen über das hochzuverlässige Multiprotocol Label Switching (MPLS). Bei MPLS ist es jedoch schwierig, die Nutzung der WAN-Bandbreite zu optimieren und die Dienstqualität (QoS) bedarfsgerecht und flexibel für verschiedene Anwendungen anzupassen. Daher können neue Standorte und Dienste schnell die WAN-Kosten explodieren lassen.

Viele Unternehmen entscheiden sich daher für ein SD-WAN (Software-Defined WAN), das MPLS-, Internet- und sogar Telefonverbindungen effizient bereitstellen kann. Auch läuft bei einem SD-WAN der Traffic dynamisch über die jeweils am besten geeignete Verbindung.

Vier Überlegungen zur Gestaltung der Security-Architektur

Viele Unternehmen treiben digitale Innovationen mit Begeisterung voran. Die Folgen für die Netzwerk-Security werden dabei oft übersehen oder heruntergespielt: Fast 80 % der Unternehmen führen neue digitale Innovationen schneller ein, als sie diese vor Cyber-Bedrohungen schützen können.[9]

IT-Verantwortliche stehen bei der Gestaltung von sicheren Architekturen für digitale Innovationen vor vier zentralen Herausforderungen:

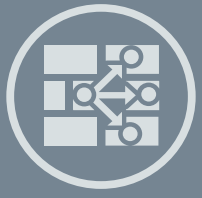
Erweiterung der Angriffsfläche

Sensible Daten können sich überall befinden – und über unterschiedlichste Verbindungen übertragen werden, über die das Unternehmen keine Kontrolle hat. Da Anwendungen in

Cloud-Umgebungen sind dynamisch: 74 % der Unternehmen haben eine Anwendung in die Cloud verlagert – und dann wieder On-Premises bereitgestellt.[4]

84 % der Unternehmen verfolgen eine Multi-Cloud-Strategie. 81 % bezeichnen die Security als große Herausforderung bei der Cloud.[6]

Von 2017 bis 2019 stieg die Anzahl der Unternehmen, bei denen es durch ungesicherte IoT-Geräte oder Anwendungen zu Datenpannen kam, um 73 %.[7]



Ein SD-WAN bietet gegenüber MPLS eine höhere Leistung und Sicherheit – zu geringeren Kosten.[8]

der Cloud dem Internet ausgesetzt sind, erweitert jede neue Cloud-Instanz die Angriffsfläche des Unternehmens. Gleiches gilt für IoT-Geräte, durch die entfernte, unbesetzte Standorte zum Sicherheitsrisiko werden. In diesen intransparenten Bereichen der Angriffsfläche können illegale Zugriffe wochen- bis monatelang unbemerkt stattfinden und so verheerende Schäden im gesamten Unternehmen anrichten. Da Anwender zwischen Unternehmensstandorten wechseln, sich im öffentlichen Raum bewegen und ins Ausland reisen, wird die Angriffsfläche durch mobile Geräte und benutzereigene Endgeräte unberechenbar. Tatsächlich sind es drei Faktoren – die umfassende Migration in die Cloud sowie die starke Nutzung von Mobil- und IoT-Geräten –, die bei einer Datenpanne die Kosten pro Datensatz auf sechsstellige Beträge schnellen lassen.[10]

Diese erweiterte, dynamische Angriffsfläche erodiert den einst klar abgegrenzten Netzwerk-Rand und die damit verbundenen Sicherheitsmaßnahmen. Angreifer können heutzutage viel leichter in Unternehmensnetzwerke eindringen und stoßen im Netzwerk auf nur geringen Widerstand, um ungehindert und unentdeckt bis zum Ziel ihres Angriffs vorzudringen. Wer auf digitale Innovationen setzt, braucht eine mehrstufige Security. Notwendig sind Kontrollen pro Netzwerk-Segment – weil man einfach davon ausgehen muss, dass es früher oder später am Perimeter zu einem erfolgreichen Angriff kommt. Wichtig ist auch ein reglementierter Zugriff auf Netzwerk-Ressourcen, der nur das unbedingt notwendige Maß an Benutzerrechten gewährt und die Vertrauenswürdigkeit eines Benutzers ständig neu bewertet.

Komplexe Bedrohungslage

Die Cyber-Bedrohungslage verschärft sich rasant angesichts von Kriminellen, die alles daran setzen, herkömmliche Abwehrmaßnahmen auszuhebeln: Bis zu 40 % der pro Tag erkannten neuen Malware ist Zero-Day-Schadsoftware oder war zuvor unbekannt.[15] Unabhängig davon, ob dies auf den vermehrten Einsatz von polymorpher Malware oder auf die Verfügbarkeit von Malware-Toolkits zurückgeht – bisher gut funktionierende, signaturbasierte Malware-Erkennungsalgorithmen können den zunehmenden Zero-Day-Malware-Angriffen wenig entgegensetzen. Auch Social Engineering ist bei kriminellen Elementen beliebt, um herkömmliche Sicherheitskonzepte mit statischen Zugriffsrechten in die Knie zu zwingen: Wie Studien zeigen, haben 85 % der Unternehmen im vergangenen Jahr Phishing- oder Social-Engineering-Angriffe erlebt.[16]

Mit zunehmender Komplexität von Cyber-Bedrohungen sind Datenschutzverletzungen schwerer zu erkennen und zu beheben: Von 2018 bis 2019 stieg die Zeit bis zur Erkennung und Eindämmung einer Datenpanne von 266 auf 279 Tage.[17] Neben der Fähigkeit, einen versuchten Angriff zu entdecken und zu verhindern, müssen Unternehmen auch in der Lage sein, einen erfolgreichen Angriff schnell zu identifizieren, zu stoppen und die Folgen zu beheben. Dass 88 % der Unternehmen nach eigenen Angaben im letzten Jahr mindestens einen Vorfall erlebten, zeigt, dass alle Unternehmen einem Angriffsrisiko ausgesetzt sind und dass die Cyber-Resilienz von entscheidender Bedeutung ist.[18]

Komplexeres Ecosystem

Für fast die Hälfte der CIOs ist die zunehmende Komplexität das größte Problem bei der wachsenden Angriffsfläche.[19] Schuld an dieser erhöhten Komplexität sind die vielen isoliert arbeitenden Einzelprodukte, die für unterschiedliche Sicherheitsfunktionen implementiert wurden: De facto gibt es in einem durchschnittlichen Unternehmen mehr als 75 verschiedene Sicherheitslösungen.[20]

Diese fehlende Security-Integration verhindert, dass Unternehmen von den Vorteilen automatisierter Sicherheitsfunktionen profitieren. Tatsächlich geben 30 % der CIOs an, dass die Anzahl der manuellen Prozesse ein zentrales Sicherheitsproblem darstellt.[21] Ohne Security-Automatisierung benötigen CIOs besser qualifizierte Cyber-Sicherheitsexperten, um das Netzwerk zu überwachen und zu sichern.

Viele Unternehmen haben jedoch Schwierigkeiten damit, geeignete Fachkräfte für die Cyber-Sicherheit einzustellen. Schätzungen zufolge sind derzeit über 4 Millionen Cyber-Security-Stellen unbesetzt – Tendenz steigend.[22] Dieser Fachkräftemangel gefährdet

61 % der CISOs geben an, dass sie bereits in weiten Teilen mit Cloud-, IoT- und mobilen Lösungen arbeiten.[11]

Bis zu 40 % der pro Tag erkannten neuen Malware ist Zero-Day-Schadsoftware oder war zuvor unbekannt.[12]

DI-Initiativen bedeuten, dass interne Security-Teams einen Schutz für 17 verschiedene Arten von Endpunkten bereitstellen müssen.[13]

Ein Drittel der Unternehmen erlebte im Vorjahr Verstöße bei geschäftskritischen Daten, für die Bußgelder erhoben werden könnten.[14]

das gesamte Unternehmen: 67 % der CIOs geben an, dass sie wegen fehlender Mitarbeiterkenntnisse zur Cyber-Security nicht mit Änderungen Schritt halten können.[23] Angreifer kennen diese Probleme sehr wohl – und nutzen sie zu ihrem Vorteil.

Fortinet Security Fabric
- Umfassend
- Automatisiert
- Integriert

FORTINET Fabric-Ready

Zunahme an gesetzlichen Vorschriften

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) und das kalifornische Verbraucherschutzgesetz (CCPA) sind zwei der bekanntesten Datenschutzbestimmungen. Sie sind jedoch bei weitem nicht die einzigen. So gibt es z. B. in einigen US-Bundesstaaten eine Meldepflicht bei Datenschutzverletzungen und viele Länder erlassen zusätzliche Bestimmungen zum Schutz der Privatsphäre von Verbrauchern. Aufgrund des politischen und gesellschaftlichen Drucks dürfte die Zahl der Vorschriften in den nächsten Jahren steigen – und mit ihnen die Höhe und Häufigkeit von Bußgeldzahlungen.

Weiter müssen Unternehmen Industriestandards einhalten, scheitern hieran jedoch häufig. Tatsächlich bestehen weniger als 37 % der Firmen das Compliance-Audit für den PCI-DSS-Standard für Kreditkartenzahlungen.[24] Da PCI DSS bald durch das PCI Software Security Framework (PCI SSF) ersetzt wird, dürften sich die Konformitätsprobleme für diese Unternehmen noch verschärfen.

Die Notwendigkeit der Einhaltung gesetzlicher Vorschriften wirkt sich stark auf den Erfolg der Security-Transformation aus. Beispielsweise haben 21 % der 71 % der Unternehmen, die cloudbasierte Anwendungen wieder zurück in On-Premises-Rechenzentren verlagerten, dies nur aus einem Grund getan: um gesetzliche Vorschriften zu erfüllen.[25]

Die Fortinet Security Fabric

Die Fortinet Security Fabric wurde speziell für die zuvor beschriebenen Sicherheitsherausforderungen entwickelt. Unternehmen erhalten damit umfassende Transparenz und Kontrolle über die gesamte digitale Angriffsfläche, um Risiken zu minimieren. Da es sich um eine integrierte Lösung handelt, verringert sich auch die Komplexität (es müssen weniger Einzelprodukte unterstützt werden) und Betriebsabläufe werden dank automatisierter Workflows beschleunigt.

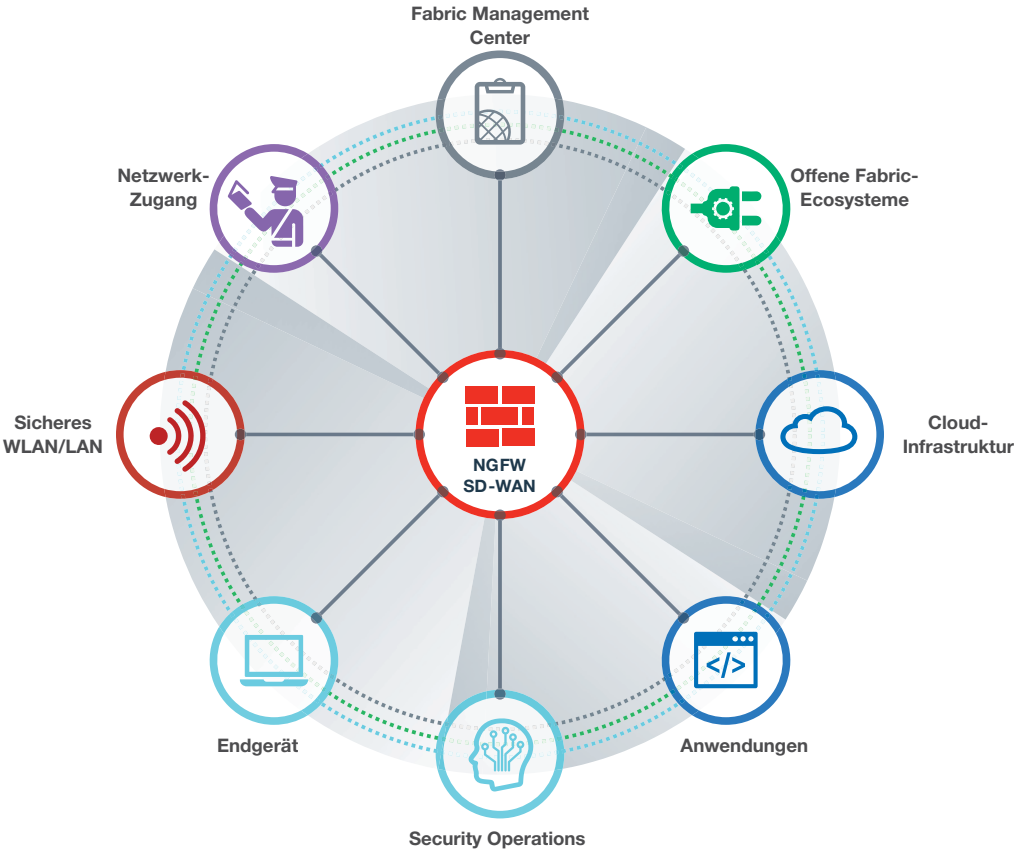


Abbildung 1: Mit der Fortinet Security Fabric können mehrere Security-Technologien nahtlos über alle Umgebungen hinweg zusammenarbeiten – unterstützt von einer einzigen Threat-Intelligence-Quelle und kontrolliert über eine gemeinsame „Schaltzentrale“. So werden Security-Lücken im Netzwerk geschlossen und Reaktionen auf Angriffe und Datenschutzverletzungen beschleunigt.

Umfassende Transparenz über die Angriffsfläche

Wird der Netzwerk-Rand infolge der Transformationen durch digitale Innovationen (DI) immer größer, wächst auch die Angriffsfläche. Die Fortinet Security Fabric begegnet dieser Problematik einer erweiterten Angriffsfläche mit einer End-to-End-Security und -Transparenz für die gesamte Netzwerk-Infrastruktur. Mit einem breitgefächerten Angebot an leistungsstarken, sicherheitsorientierten Netzwerk-Lösungen für Rechenzentren, Filialen und Kleinunternehmen sowie für alle wichtigen Cloud-Plattformen bietet die Fortinet Security Fabric Unternehmen die notwendige Flexibilität, um jedes Netzwerk-Segment zu schützen.

Alle Sicherheitskomponenten werden zentral konfiguriert, verwaltet und überwacht. Diese „Security-Schaltzentrale“ löst nicht nur isolierte Bereiche auf, die beim Einsatz punktueller Einzelprodukte zwangsläufig entstehen, sondern reduziert auch den Schulungsaufwand für personell begrenzte IT-Teams. Zudem erleichtert das zentrale Management-System die Zero-Touch-Bereitstellung von Remote-Komponenten, reduziert Außendienst-Einsätze und senkt die Betriebskosten um ein Weiteres.

Integrierte Security-Architektur

Da alle Komponenten mit FortiOS das gleiche Netzwerk-Betriebssystem verwenden, sorgt die Fortinet Security Fabric automatisch für einheitliche Konfigurationen, ein konsequentes Richtlinien-Management und eine reibungslose Echtzeit-Kommunikation innerhalb der gesamten Sicherheitsinfrastruktur. Dies minimiert Verzögerungen bei der Bedrohungserkennung und -abwehr, reduziert Sicherheitsrisiken durch Konfigurationsfehler und manuelle Dateneingaben und ermöglicht zeitnahe, korrekte Compliance-Audits.

Neben der Integration von Fortinet-Produkten und -Lösungen umfasst die Security Fabric auch vorkonfigurierte API-Verbindungen (Application Programming Interface) für mehr als 70 Fabric-Ready-Partner, die eine tiefgehende Integration aller Security-Fabric-Elemente sicherstellen.

Security-Produkte, die nicht vom Fabric-Ready-Partnernetz abgedeckt werden, können Kunden über REST-APIs (Representational State Transfer) und DevOps-Skripten (Development Operations) schnell und einfach zur Security Fabric hinzufügen.

Automatisierte Abläufe, Orchestrierung und Bedrohungsabwehr

Zusätzlich zu ihrer nahtlosen Integration ist die Fortinet Security Fabric marktführend bei der Anwendung von ML-Technologien (Machine Learning), um mit der dynamischen Cyber-Bedrohungslandschaft Schritt zu halten. Auch bietet die Fortinet Security Fabric intelligente SOAR-Funktionen (Security Orchestration, Automation und Response), eine proaktive Bedrohungserkennung, Bedrohungskorrelationen, den Austausch von Bedrohungsinformationen sowie die Erforschung und Analyse von Bedrohungen.

Für eine schnelle Reaktion auf Vorfälle muss zudem sichergestellt werden, dass das Security-Team nicht durch andere Aufgaben – wie das Sammeln von Daten oder das Erstellen von Berichten für die Einhaltung gesetzlicher Vorschriften oder das leitende Management – abgelenkt wird. Hierfür bietet die Fortinet Security Fabric eine automatisierte Log-Aggregierung, Datenkorrelation und Berichterstellung anhand integrierter Vorlagen.

Für fast die Hälfte der CISOs haben eine integrierte Security und bessere Analysen oberste Priorität bei der Technologie-Strategie im Bereich Cyber-Sicherheit.[26]

Externe Tests zeigen: FortiGate NGFWs bieten das beste Preis-Leistungs-Verhältnis beim Überprüfen von verschlüsseltem Datenverkehr. Sie erreichen eine SSL-Leistung von 5,7 Gbit/s und blockieren gleichzeitig 100 % der Umgehungsversuche.[27]

Werden Verstöße schneller erkannt und Reaktionszeiten verkürzt, sinken die Gesamtkosten einer Datenpanne um bis zu 25 %.[28]

Security-Fabric-Lösungen

Die Fortinet Security Fabric adressiert fünf Kernbereiche: Zero-Trust-Access, sicherheitsorientierte Netzwerke, dynamische Cloud-Security, KI-gesteuerte Security Operations und die Einbindung von Partnern über das Alliance Ecosystem. Für jeden dieser Sicherheitsschwerpunkte werden erstklassige, preisgekrönte Lösungen angeboten, die von unabhängigen Stellen wie den NSS Labs getestet, bewertet und empfohlen sowie von führenden Analysten wie Gartner als führend eingestuft werden.[29,30]

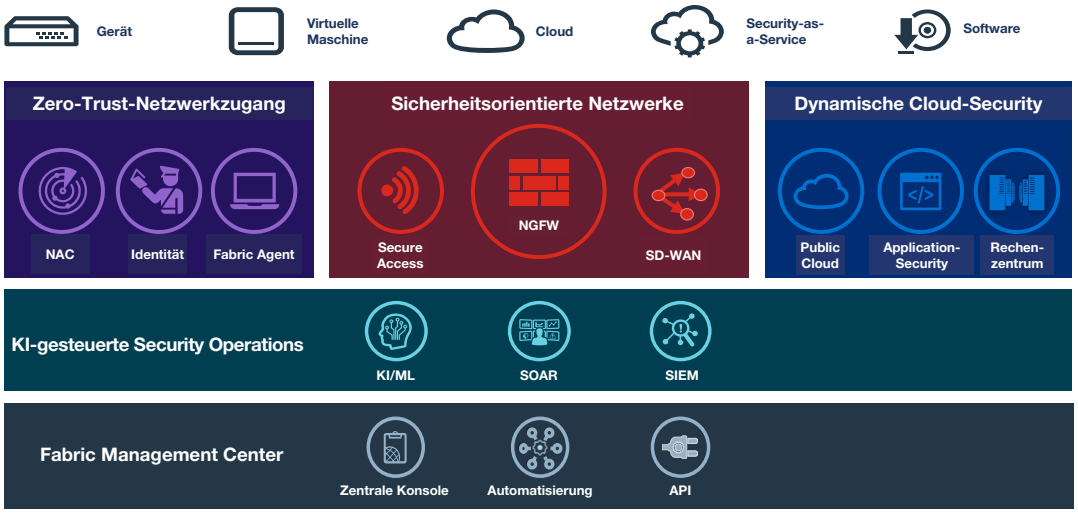


Abbildung 2: Framework-Konzept der Fortinet Security Fabric

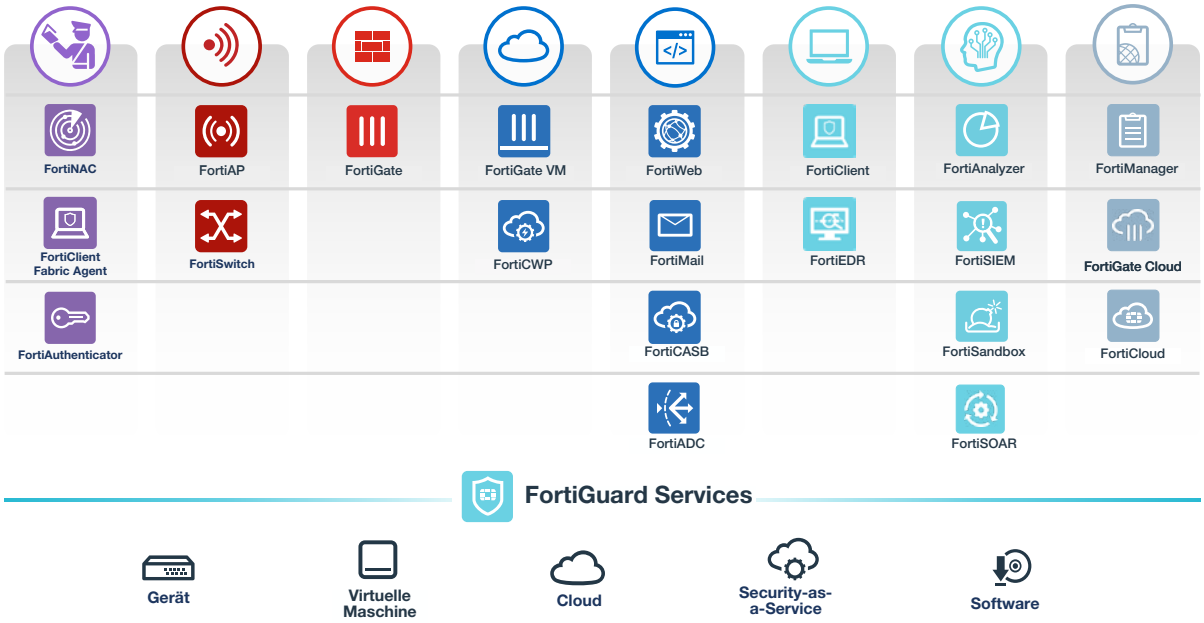


Abbildung 3: Sicherheitslösungen für jeden Bereich der Security Fabric – die wichtigsten Produkte auf einen Blick

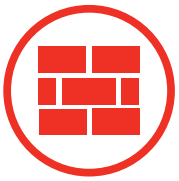
Zero-Trust-Netzwerkzugang

Mit zunehmender Komplexität von Cyber-Bedrohungen reicht ein perimeterorientiertes Sicherheitsmodell nicht mehr aus: Malware und der Diebstahl von Zugangsdaten ermöglichen externen Bedrohungen den Zugriff auf legitime Konten im Unternehmensnetzwerk. Mit der Fortinet Security Fabric können Unternehmen im gesamten Unternehmens-WAN eine Zero-Trust-Richtlinie implementieren.

Der erste Schritt bei der Durchsetzung eines Zero-Trust-Access in einem Netzwerk ist die Ermittlung der mit dem Netzwerk verbundenen Geräte. **FortiNAC**-Lösungen regeln die Netzwerk-Zugangskontrolle (Network Access Control). Sie erkennen automatisch Geräte, die eine Verbindung zum Unternehmens-WAN herstellen und unterziehen verbundene Geräte einer Sicherheitsüberprüfung. Zudem kann das Security-Team eines Unternehmens gerätespezifische Richtlinien definieren, die durchgesetzt werden müssen. Wurde einem Gerät der Zugriff auf das Netzwerk gestattet, wird es kontinuierlich überwacht. Dadurch lassen sich Anomalien im erwarteten Verhalten erkennen, die auf eine Infektion oder Missbrauch durch böswillige Akteure hinweisen können.

Kann ein Unternehmen die mit dem Netzwerk verbundenen Geräte identifizieren, lässt sich mit einem implementierten Zero-Trust-Access feststellen, wer diese Geräte verwendet. Beim FortiAuthenticator handelt es sich um einen Server für das User-Identity-Management mit integrierter Authentifizierung und rollenbasierter Zugangskontrolle (RBAC). Unternehmen können hiermit die erteilten Netzwerk-Zugriffsrechte auf ein Mindestmaß sowie nach Aufgaben begrenzen. Zusätzlich stärkt die Zwei-Faktor-Authentifizierung mit FortiToken die eindeutige Erkennung von Benutzern: Diese Multi-Faktor-Authentifizierung stellt sicher, dass kein Angreifer mit gestohlenen Anmeldedaten auf ein Benutzerkonto zugreifen kann.

Sind Geräte mit dem Unternehmensnetzwerk verbunden, lassen sich Richtlinien über das Netzwerk überwachen und durchsetzen. Dabei muss jedoch bedacht werden, dass die Anzahl der geschäftlich genutzten Mobilgeräte rasant steigt und Geräte oft auch offline oder in anderen Netzwerken verwendet werden. Um dieses Problem zu lösen, sollte der **FortiClient** installiert werden. Dieser Fabric Agent bietet Transparenz über Endgeräte und implementiert sowohl im als auch außerhalb des Unternehmensnetzwerks eine dynamische Zugangskontrolle.



Sicherheitsorientierte Netzwerke

Mit der Erweiterung von Unternehmensnetzwerken und Angriffsflächen infolge digitaler Innovationen wächst die Notwendigkeit, diese Netzwerke zu sichern. Bei sicherheitsorientierten Netzwerken sind Netzwerk-Infrastruktur und Security-Architektur eng integriert. Netzwerke können dadurch skaliert und angepasst werden, ohne die Sicherheit zu beeinträchtigen. Eine solche Integration verringert die Komplexität, weil die Anzahl isolierter Einzelprodukte auf ein Minimum reduziert wird. Unternehmen profitieren zudem stärker von Leistungsverbesserungen, da Netzwerk- und Sicherheits-Appliances für die Zusammenarbeit optimiert sind.

Die **FortiGate** Next-Generation-Firewalls (NGFWs) ermöglichen sicherheitsorientierte Netzwerke und fungieren als erste Verteidigungslinie eines Unternehmens gegen komplexere Bedrohungen. FortiGates sind jedoch viel mehr als Firewalls: Da fast ein Drittel der Datenschutzverletzungen auf Phishing-Angriffe[31] zurückgeht – bei denen mit bösartigen Links oder Anhängen Endgeräte infiziert oder Anmeldedaten gestohlen werden –, umfassen FortiGate-NGFWs auch ein sicheres Web-Gateway (SWG), das Verbindungsversuche zu bösartigen oder verdächtigen URLs identifiziert und blockiert.

FortiGate NGFWs übernehmen zudem die Entschlüsselung und Überprüfung von Paketen, die durch das SSL-Protokoll (Secure Sockets Layer) bzw. TLS (Transport Layer Security) geschützt sind. Heutzutage ist das eine wichtige Anforderung, da schätzungsweise 75 % des Netzwerk-Traffics von Unternehmen mit der SSL/TLS-Verschlüsselung übertragen werden – und etwa 82 % des bösartigen Datenverkehrs.[32,33] Speziell für diese Aufgabe besitzen **FortiGate NGFWs** eigene Security-Prozessoren (SPUs), damit die Überprüfung des SSL/TLS-Traffics nicht zu Lasten der Firewall-Leistung geht. Durch diese Integration einer extrem leistungsstarken Überprüfung des verschlüsselten Datenverkehrs direkt in der NGFW kann das Unternehmen Kosten sparen, da die Anschaffung und Implementierung von Einzelgeräten in der gesamten Netzwerk-Infrastruktur entfällt.

Werden Bedrohungen am Netzwerk-Rand nicht erkannt, muss unbedingt verhindert werden, dass sie sich quer im Netzwerk verbreiten. Mit einer absichtsbasierten Segmentierung lässt sich das leicht erreichen: Unternehmen können hiermit ihr Netzwerk basierend auf den Geschäftsanforderungen segmentieren. Verdächtige oder bösartige interne Verbindungen werden standardmäßig blockiert. Sollte nach einer Infektion eine Zero-Day-Bedrohung erkannt werden, gehen die Bedrohungsinformationen über die Security Fabric sofort an alle verbundenen Sicherheitslösungen. So wird sichergestellt, dass es zu keinen sekundären Infektionen kommt.

Damit dies funktioniert, ist eine Security-Integration im gesamten Unternehmensnetzwerk notwendig, einschließlich in entfernten Standorten. **Fortinet Secure SD-WAN** bietet für Filialen und Niederlassungen eine optimierte Netzwerk-Performance und Security-Integration. Da FortiGate NGFWs bereits in die SD-WAN-Appliances integriert sind, wird der gesamte Netzwerk-Datenverkehr automatisch überprüft. Davon profitiert die Netzwerk-Performance, da z. B. SaaS-Anwendungen und -Dienste direkt auf das Internet zugreifen können. Ein weiterer Vorteil sind die geringeren WAN-Kosten.

Die Implementierung von **Fortinet Secure SD-Branch** für Niederlassungen und Filialen erweitert auch die Transparenz und das zentrale Security-Management bis zur Vermittlungsschicht, dem Switching-Layer. Fortinet Secure SD-Branch besteht aus FortiNAC-Lösungen, FortiSwitch Secured Access Switches und **FortiAP** Wireless Access Points, die allesamt über eine FortiGate NGFW überwacht und kontrolliert werden. Die Integration der Security in das WAN vereinfacht zudem Betriebsabläufe: Redundanz wird vermieden und auf komplexe Bedrohungen kann schnell und koordiniert reagiert werden.

Dynamische Cloud-Security

Bei der Umstellung auf die Cloud ist die Erweiterung der Security-Implementierung auf cloudbasierte Ressourcen von entscheidender Bedeutung. Die Fortinet Security Fabric integriert daher mehrere cloudnative Lösungen, mit denen jede Anwendungs- und Bereitstellungsumgebung geschützt werden kann.

Sicherheitslösungen von Fortinet bieten Netzwerk-Security, Transparenz und Kontrolle für Public und Private Clouds. FortiGate NGFWs sind auch als virtuelle Maschine (VM) erhältlich. Unternehmen erhalten damit eine cloudnative Security-Automatisierung mit VPN-Verbindungen, Netzwerk-Segmentierung, Intrusion Prevention und einem SWG.

Neben dem Schutz vor bösartigen Inhalten müssen Unternehmen auch sicherstellen, dass ihre Cloud-Implementierungen richtig konfiguriert sind. Fehlkonfigurationen bei der Security sind ein gewaltiges Problem bei Public Clouds: 99 % der Sicherheitsvorfälle werden überhaupt nicht gemeldet.[34] Mit den Cloud-Security-Analysen von **FortiCWP** erhalten Unternehmen Transparenz und Kontrolle über ihren Teil der Public-Cloud-Infrastruktur mit einem integrierten Bedrohungsmanagement – einschließlich Konfigurationsüberwachung, Datensicherheit und Regelkonformität.

Nicht nur die Cloud-Infrastruktur muss geschützt werden, auch die darin ausgeführten Anwendungen. Viele Public-Cloud-Implementierungen dienen zum Hosten von Web-Anwendungen und Web-APIs, die sich mit der cloudnativen Security von **FortiWeb** WAFs sehr gut absichern lassen. Diese Web Application Firewalls schützen Web-Anwendungen mit einer Kombination aus Signaturerkennung, ML und KI vor bekannten und unbekannten Bedrohungen. Da die meisten Web-Anwendungen über APIs auf Web-Dienste zugreifen und mit weiteren Tools integriert sind, sollten Web-APIs zusätzlich mit einer Schema-Validierung und OpenAPI-Security vor potenziell bösartigen Bot-Aktivitäten – wie Scraping oder Analysen der Sicherheitsmaßnahmen – geschützt werden.

Viele Unternehmen verwenden zunehmend cloudbasierte E-Mail-Lösungen wie Google G Suite oder Microsoft Office 365. Da Phishing-Angriffe eine der Hauptursachen für Sicherheitsvorfälle und Datenpannen sind, ist die Sicherung von cloudbasierten E-Mails entscheidend. Messaging-Security-Lösungen wie **FortiMail** – erhältlich als Gerät, VM oder gehosteter Dienst – schützen E-Mail-Implementierungen On-Premises und in der Cloud. Zusätzlich zur Blockierung herkömmlicher und komplexerer E-Mail-Bedrohungen bietet FortiMail auch Backup-Funktionen, damit keine vertraulichen Informationen verloren gehen.

Neben Web-Anwendungen und E-Mails sind viele Unternehmen auf SaaS-Lösungen wie Google G Suite, Box, Microsoft Office 365, Dropbox und Salesforce angewiesen. Für das Risiko-Management von Security-Fehlkonfigurationen empfehlen sich Cloud Access Security Broker (CASBs) wie **FortiCASB**. Unternehmen profitieren mit einem CASB von zentraler Transparenz, administrativer Kontrolle und Datensicherheit in SaaS-Anwendungen und können zugleich sicherstellen, dass die Konfiguration von SaaS-Anwendungen gesetzliche Compliance-Vorschriften erfüllt.

KI-gesteuerte Security Operations

Volumen und Komplexität bösartiger Angriffe steigen ständig und überfordern herkömmliche Cyber-Sicherheitslösungen: Eine signaturbasierte Malware-Erkennung kann z. B. nur die Hälfte der Malware-Angriffe identifizieren.[35] KI- und ML-Funktionen sind daher unverzichtbar, um solche Attacken zu erkennen und zu verhindern.

Mit der künstlichen Intelligenz von **FortiGuard** AI sind Unternehmen Cyber-Kriminellen stets einen Schritt voraus. Die FortiGuard Labs erfassen weltweit Bedrohungsdaten von Millionen Sensoren und arbeiten mit über 200 internationalen Unternehmen zusammen. FortiGuard AI fragt über 5 Milliarden Knoten ab, um einzigartige Merkmale bekannter und unbekannter Bedrohungen zu identifizieren. Das Volumen, das die FortiGuard Labs täglich bewältigen, ist beeindruckend: Jeden Tag werden über 100 Milliarden Web-Anfragen verarbeitet – und pro Sekunde über 3600 bösartige URL-Anfragen blockiert.

Mit zunehmender Komplexität von Bedrohungen ist eine 100%ige Prävention nicht mehr möglich. Erweiterte Funktionen zur Bedrohungserkennung sind unverzichtbar, um Unternehmen bei der Vermeidung von Sicherheitsverletzungen zu unterstützen. Die in **FortiDeceptor, FortiSandbox** und **FortiInsight** integrierten KI- und ML-Funktionen helfen Unternehmen bei der Identifizierung unbekannter Angreifer und Malware sowie bei der Aufdeckung und Bekämpfung von Insider-Bedrohungen.

Angesichts der rasanten Entwicklung bei Cyber-Bedrohungen ist eine strategische Automatisierung nötig, um Bedrohungen schneller einzudämmen und zu beseitigen. Mit **FortiSIEM** und **FortiAnalyzer** erhält ein Unternehmen globale Transparenz über seine Netzwerk-Infrastruktur sowie KI-gesteuerte Sicherheitsanalysen. Anhand der gesammelten Daten – und mit Unterstützung von **FortiAI** Virtual Analyst – können Security-Analysten die Art und den Schweregrad von Bedrohungen ermitteln. Doch die Erkennung und Prävention von Bedrohungen allein genügt nicht: Mit **FortiSOAR** zur Orchestrierung und Automatisierung lässt sich der Schaden von Hacker-Angriffen schnell beheben – eine sinnvolle Unterstützung für überlastete SOC-Teams (Security Operations Center) bei der Skalierung, gezielten Bedrohungssuche und anderen geschäftskritischen Aufgaben.

Auch für Endgeräte sind KI-gesteuerte Ressourcen für den Incident-Response-Prozess notwendig. **FortiEDR** Endpoint Detection und Response (EDR) und FortiClient bieten einen erweiterten Endpunkt-Schutz mit neuen Möglichkeiten – von Schwachstellen-Scans, Patching und virtuellen Patches bis hin zur Verhinderung von Exploits in Online- und Air-Gapped-Umgebungen. Wird ein Endpunkt infiziert, verhindert die FortiEDR-Bedrohungserkennung auch nach einer Infektion, dass Malware mit CC-Servern (Command-Control) kommuniziert oder sich quer durch das Netzwerk verbreitet. Weiter bietet FortiEDR eine risikobasierte Bedrohungsreaktion und Online-Remediation mit Unterstützung automatisierter Anleitungen zur Fehlerbehebung – Stichwort „Remediation Recipes“.

Fabric Management Center

Die Fortinet Security Fabric vereinfacht das Management der gesamten Security-Architektur eines Unternehmens: Die Sicherheitsstruktur integriert alle bereitgestellten punktuellen Security-Produkte, damit diese zentral überwacht und verwaltet werden können.

Gemeinsam bilden der **FortiManager** als zentralisierte Management-Plattform und der **FortiAnalyzer** für das zentralisierte Logging und Reporting eine einzige „Schaltzentrale". Unternehmen erhalten damit übersichtliche Transparenz und Management in einer Lösung: Mit einer einzigen Konsole – inklusive Analysen und Workflow-Automatisierung – lässt sich die gesamte Netzwerk-Infrastruktur abdecken.

Diese Funktionalität wird durch zahlreiche API-Integrationen von Fortinet Fabric-Ready-Partnern unterstützt. Zwölf Fabric-Konnektoren ermöglichen die umfassende Integration mit Drittlösungen. API-Integrationen sind für über 135 Fabric-Ready-Partner verfügbar. Für Lösungen anderer Anbieter bietet die Fortinet Security Fabric eine REST-API und DevOps-Skripte, die eine einfache Integration sicherstellen.

Da viele Unternehmen Betriebsabläufe in die Cloud verlagern, ist eine Single-Point-of-Access- und Single-Sign-On-Lösung (SSO) erforderlich, um die Komplexität von Multi-Cloud-Implementierungen zu verringern. **FortiCloud** umfasst eine SSO-Funktion, Portale für 15 Fortinet SaaS- und MaaS-Lösungen (Metal-as-a-Service) und ein **FortiCare** Services Portal. Mit der Unterstützung aller wichtigen Public-Cloud-Anbieter vereinfacht die Fortinet Security Fabric auch Multi-Cloud-Implementierungen.

Durch die Kombination von FortiManager, FortiAnalyzer und FortiCloud kann ein Unternehmen seine On-Premises- und Cloud-Bereitstellungen vollständig integrieren. Diese Integration eröffnet die Vorteile einer Automatisierung und Orchestrierung, um das Security-Management zu vereinfachen. Mit Fabric-Konnektoren und APIs können Security-Teams zudem Informationen zur Netzwerk-Integrität in Echtzeit erhalten, das Netzwerk-Log-Management automatisieren und die Compliance-Berichterstellung vereinfachen – alles über eine einzige, zentrale Konsole.

Risiken im Griff, Chancen verfolgen

Digitale Innovationen (DI) eröffnen Unternehmen neue Effizienz- und Kosteneinsparungen sowie eine Verbesserung der Kundenerfahrung. DI-Initiativen erweitern und verändern jedoch auch die Angriffsfläche des Unternehmens und bieten damit den Nährboden für neue Cyber-Bedrohungen und Angriffsformen.

Für Vorreiter bei digitalen Innovationen ist es von größter Bedeutung, Risiken zu identifizieren, zu akzeptieren und richtig zu handhaben. Die Fortinet Security Fabric bietet die Basis dafür. Sie vereinheitlicht Security-Lösungen über eine zentrale Konsole, macht die wachsende digitale Angriffsfläche sichtbar, integriert einen KI-gesteuerten Schutz vor Datenschutzverletzungen und automatisiert Betriebsabläufe, Orchestrierung und Reaktionen. Zusammenfassend lässt sich sagen, dass sie es Unternehmen ermöglicht, mit digitalen Innovationen einen neuen Mehrwert zu schaffen, ohne die Sicherheit im Tausch für Agilität, Leistung und einfache Bedienung zu beeinträchtigen.

[1] Nick Lansing: „Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources“. Forbes und Fortinet, 2019.

[2] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[3] Jeff Wilson: „The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments“. IHS Markit, 2019.

[4] Ebd.

[5] Gilad David Maayan: „The IoT Rundown For 2020: Stats, Risks, and Solutions“. Security Today, 13. Januar 2020.

[6] „2019 State of the Cloud Report“. Flexera, 2019.

[7] Larry Ponemon: „Third-party IoT risk: companies don't know what they don't know“. ponemonsullivanreport.com, abgerufen am 4. Februar 2020.

[8] Nirav Shah: „SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019“. Fortinet, 9. September 2019.

[9] Kelly Bissell, et al.: „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“. Accenture Security und Ponemon Institute, 2019.

[10] „2019 Cost of a Data Breach Report“. IBM Security und Ponemon Institute, 2019.

[11] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[12] Laut internen Daten der FortiGuard Labs.

[13] „6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders“. Fortinet, 8. September 2019.

[14] Laut Daten aus einer internen Fortinet-Studie.

[15] Laut internen Daten der FortiGuard Labs.

[16] Kelly Bissell et al.: „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“. Accenture Security und Ponemon Institute, 2019.

[17] „2019 Cost of a Data Breach Report“. IBM Security und Ponemon Institute, 2019.

[18] Basierend auf Daten einer internen Fortinet-Studie.

[19] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[20] Kacy Zurkus: „Defense in depth: Stop spending, start consolidating“. CSO, 14. März 2016.

[21] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[22] „Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019“. (ISC)², 2019.

[23] „CIO Survey 2019: A Changing Perspective“. Harvey Nash und KPMG, 2019.

[24] „2019 Payment Security Report“. Verizon, 2019.

[25] Jeff Wilson: „The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments“. IHS Markit, 2019.

[26] „Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources“. Forbes und Fortinet, 2019.

[27] „Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests“. Fortinet, 14. Oktober 2019.

[28] „2019 Cost of a Data Breach Report“. IBM Security und Ponemon Institute, 2019.

[29] „Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests“. Fortinet, 14. Oktober 2019.

[30] „Gartner Magic Quadrant Reports“. Fortinet, abgerufen am 22. Januar 2020.

[31] „2019 Data Breach Investigations Report“. Verizon, 2019.

[32] Alex Samonte: „TLS 1.3: What This Means For You“. Fortinet, 15. März 2019.

[33] Robert Lemos: „Attackers Are Messing with Encryption Traffic to Evade Detection“. Dark Reading, 15. Mai 2019.

[34] Charlie Osborne: „99 percent of all misconfigurations in the public cloud go unreported“. ZDNet, 24. September 2019.

[35] Robert Lemos: „Only Half of Malware Caught by Signature AV“. Dark Reading, 11. Dezember 2019.

FORTINET

www.fortinet.com/de

29. Juni 2020, 13:26 Uhr

570099-0-0-DE