WHITEPAPER

Fortinet Security Fabric unterstützt die digitale Transformation

Umfassend, integriert und automatisiert

Zusammenfassung

DX bietet neue Geschäftsvorteile und Unternehmen setzen zunehmend auf digitale Technologien, um ihr Geschäft zu beschleunigen, bessere Kundenerfahrungen zu bieten, Kosten zu senken und ihre Effizienz zu verbessern. Unternehmen migrieren Workloads und Anwendungen in die Cloud, was zu einer Explosion von IoT-Geräten über mehrere Umgebungen hinweg und einer Ausweitung der Geschäftspräsenz in allen Märkten und Regionen führt.

DX bringt aber auch neue Security-Herausforderungen, die eine ernsthafte Gefahr für Unternehmen darstellen – wie etwa eine erweiterte Angriffsfläche, eine sich entwickelnde komplexe Bedrohungslandschaft oder erhöhte Komplexität. Die Fortinet Security Fabric löst diese Herausforderungen, indem sie umfassende Sichtbarkeit der gesamten digitalen Angriffsfläche bietet, KI-gesteuerten Schutz vor Datenschutzverletzungen integriert und Abläufe, Orchestrierung und Reaktionen automatisiert.

78 % der CIOs sind der Meinung, dass ihre digitale Strategie nur mäßig effektiv ist – oder schlechter.[1]

Einleitung

Angetrieben von dem Wunsch, auf globaler Ebene schneller zu agieren und die Kundenerfahrungen zu optimieren, überdenken Unternehmen ihre Geschäftsabläufe – und dabei steht die digitale Transformation (DX) im Vordergrund. Trotz der weitreichenden Geschäftsvorteile, die DX bietet, bringt sie auch neue Herausforderungen mit sich. Da DX unzählige technologische Aspekte berührt und sich vom Rechenzentrum und Firmengelände bis zu den Rändern des Netzwerks und die Cloud erstreckt, löst sich die Netzwerkgrenze praktisch auf. Dadurch werden zusätzliche Risiken geschaffen und die Komplexität einer ohnehin komplexen Security-Architektur wird erhöht.

Anwendungen können jetzt überall installiert sein und Mitarbeiter können an jedem beliebigen Ort und jederzeit arbeiten. Diese erweiterte Angriffsfläche macht traditionelle Tools zur Verwaltung und Sicherung einer definierten Netzwerkgrenze wirkungslos. Die von den Netzwerk- und Security-Verantwortlichen eingesetzten zusätzlichen Security-Produkte für die erweiterte Angriffsfläche erhöhen jedoch die Komplexität des Risiko- und Compliance-Managements immer weiter. Angriffe nehmen an Volumen, Geschwindigkeit und Raffinesse zu und sind schwer zu erkennen und abzuwehren.

Digitale Transformation bringt neue Geschäftsprobleme hervor

Für die für IT- und Cyber-Sicherheit Verantwortlichen schaffen DX-Initiativen Veränderungen der Geschäftsabläufe, die zu neuen technologischen Realitäten führen. Diese gliedern sich grob in drei Kernbereiche:

Migration von Workloads und Anwendungen in die Cloud

Fast jedes Unternehmen evaluiert und/oder durchläuft Workload- und Anwendungsmigrationen zu cloudbasierten Implementierungen. Die Treiber dafür sind oft der Wunsch, Kosten zu senken und in einem immer anspruchsvolleren Geschäftsumfeld schneller zu agieren. Dies erfolgt entweder durch Software-as-a-Service-(SaaS-)Anwendungen (z. B. Salesforce, Box) oder durch das Übertragen von Anwendungen, die einst in lokalen Rechenzentren liefen, in Infrastructure-as-a-Service -(IaaS-) und Platform-as-a-Service-(PaaS-) Modelle, wie Amazon Web Services (AWS), Google Cloud Platform (GCP) und Microsoft Azure.

Es gibt Unternehmen, die in den nächsten Jahren eine vollständige Migration aller Anwendungen und Dienste in die Public Cloud anstreben. Häufiger entscheiden sich Unternehmen jedoch dafür, genauer zu unterscheiden, was tatsächlich migriert werden soll und auf welcher Plattform. Sie folgen damit einer Hybrid Cloud-Strategie, die sowohl Private Clouds (vor Ort) als auch Public Clouds umfasst. Diese Multi Cloud-Umgebungen erweitern jedoch nicht nur die Angriffsfläche, sondern sie sind auch isoliert und schaffen Komplexität. Sie erhöhen zudem die Risikoexposition durch eine mögliche Fehlkonfiguration von SaaS-Anwendungen, Cloud-Infrastruktur und Plattformen.

Explosion von IoT-Geräten über mehrere Umgebungen hinweg

Internet-of-Things-(IoT-)Geräte nehmen in allen Unternehmensumgebungen weiterhin zu. Obwohl die Schätzungen unterschiedlich sind, prognostizieren die meisten Analysten, dass innerhalb des nächsten Jahres mehr als 30 Milliarden Geräte im Einsatz sein werden.[3] Die Geschäftsmöglichkeiten des IoT sind enorm, und viele glauben, dass wir uns noch in den frühen Phasen der IoT-Innovation und -Akzeptanz befinden.

Die Liste der IoT-Geräte ist umfangreich – vom Lichtschalter über Drucker, Medizinvorrichtungen bis hin zu Geldautomaten. Doch wenn es um die Sicherheit geht, stellen diese verbundenen Geräte aufgrund fehlender integrierter Sicherheitsfunktionen eine große Herausforderung dar. Bedingt durch ihre begrenzten Speichermöglichkeiten sind traditionelle Endgeräte-Security-Lösungen zu groß oder ressourcenintensiv, um auf vielen IoT-Geräten ausgeführt werden zu können. Darüber hinaus übertragen und speichern IoT-Geräte, die sich gewöhnlich am Rande des Netzwerks befinden, wichtige Informationen, die sie mit lokalen und Cloud-Diensten teilen.

Erweiterte Geschäftspräsenz über verteilte Märkte und Regionen hinweg

Unternehmen sind zunehmend dezentral, wobei das Verkehrsaufkommen in den Filialen aufgrund von SaaS-Anwendungen, Video und Voice over IP (VoIP) exponentiell zunimmt. Dies bietet Möglichkeiten für eine höhere Produktivität und Zusammenarbeit und auch für reduzierte Kosten. Geografisch verteilte Netzwerkumgebungen haben jedoch nur eine begrenzte Kontrolle und Sichtbarkeit der Benutzer, Maschinen und Geräte an entfernten Standorten. Da auch Niederlassungen sich mit der Zentrale verbinden und häufig die gleichen Systeme und Anwendungen nutzen, können Leistungs- und Verfügbarkeitseinbußen an einem einzigen Standort einen Dominoeffekt im gesamten Unternehmen haben.

Für Unternehmen, die softwaredefinierte Wide Area Networks (SD-WAN) einsetzen, die den Datenverkehr nicht mehr durch das Rechenzentrum, sondern über öffentliche Internet-Verbindungen leiten, können die Auswirkungen auf die Sicherheit sehr gravierend sein. Da der Netzwerkverkehr nicht mehr an MPLS-Verbindungen und die Verfügbarkeit und Skalierbarkeit des Rechenzentrums gebunden ist, erhält die Anwendungsleistung bei SD-WAN eine andere Dynamik.

83 % der Workloads von Unternehmen werden bis 2020 in der Cloud liegen, und 63 % der IT-Experten sehen Security als das größte durch diesen Trend ausgelöste Problem.[2]

Cyber-Kriminelle haben IoT-Geräte und ihre Schwachstellen direkt im Blick. Schätzungsweise 25 % aller Angriffe werden bis 2020 auf IoT-Geräte abzielen.[4]

Ein wesentliches Merkmal von SD-WAN ist seine Fähigkeit, die Kosten-Nutzen-Vorteile von internetbasierten VPNs mit der Leistung und Agilität von MPLS-VPNs zu liefern.[5]

Drei Herausforderungen für Security-Verantwortliche

Die oben genannte Geschäftsdynamik führt zu drei zentralen Sicherheitsherausforderungen:

Erweiterung der Angriffsfläche

Sensible Daten können nun über mehrere Clouds hinweg und in Reichweite einer wachsenden Anzahl von bereitgestellten IoT-Geräten gespeichert werden. Der Datenverkehr läuft über das öffentliche Internet anstelle von privaten Netzwerken und erstreckt sich bis an die Netzwerkgrenzen – von mobilen Geräten und drahtlosen Access Points bis hin zur Betriebstechnologie (Operational Technology, OT). Diese erweiterte, dynamische Angriffsfläche löst den einst gut definierten Netzwerkrand und die damit verbundenen Sicherheitsmaßnahmen auf.

Um die neuen Schwachstellen zu beheben, die durch diese neue Netzwerkrealität entstehen, setzen viele Unternehmen eine Reihe von weitgehend disaggregierten isolierten Security-Einzelprodukten ein. Mehr als drei Viertel der Unternehmen geben zu, dass ihre Sicherheitsarchitekturen aufgrund nicht integrierter Security-Produkte nicht miteinander verbunden sind.[6] Diese de facto-Sicherheitsarchitektur ist nicht miteinander verbunden, was zu mehreren Sicherheits- und Compliance-Lücken und Ineffizienzen führt, die ironischerweise den ganzheitlichen Schutz beeinträchtigen.

Disaggregierte Sicherheit verschwendet auch Personalressourcen, da sie manuelle Arbeitsabläufe und Administration erforderlich macht. Schlimmer noch, sie erhöht das Risiko für Unternehmen. Es kommt zu einer Ablenkung von strategischen Prioritäten, da Sicherheitsvorfälle einen „All-Hands-on-Deck"-Ansatz zur Behebung erfordern.[7] Infolgedessen befinden sich die Security-Teams in einem ständigen Reaktionsmodus gegenüber den aktuellen Bedrohungen, sodass sie nicht in der Lage sind, in der nahen Zukunft bevorstehende Angriffe zu antizipieren und entsprechend zu planen.

Komplexe Bedrohungslandschaft

Volumen und Geschwindigkeit von Bedrohungen nehmen weiter zu. So stiegen beispielsweise im vergangenen Quartal die Unique Exploits um 5 % und die pro Unternehmen erkannten Exploits um 10 %.[9] Es gibt viele Gründe für dieses explosive Wachstum, angefangen bei der Tatsache, dass der Zugriff auf Malware aufgrund der Verfügbarkeit von Malware-as-a-Service (MaaS) und anderen On-Demand-Diensten im Darknet einfacher ist denn je.

Komplexe Bedrohungen werden dazu immer ausgefeilter. Viele sind nun Multi-Vektor-Angriffe, die gleichzeitig und koordiniert verschiedene Punkte auf der erweiterten Angriffsfläche anvisieren. Ein Angriff kann ein Unternehmen gleichzeitig vom zentralen Rechenzentrum bis hin zum Netzwerkrand gefährden und auf ein ganzes Spektrum von Endgeräten und Anwendungen in lokalen und Cloud-Umgebungen abzielen. Einige Exploits sind zu „lebenden Organismen“ geworden, die polymorphe Malware einsetzen, um die neuesten Signaturen und Patches zu umgehen.[10]

Diese Fortschritte erschweren auch die Erkennung von Datenschutzverletzungen und die Reaktion auf sie. So stieg beispielsweise im letzten Jahr die durchschnittliche Dauer bis zur Identifizierung eines Datenschutzverletzungs-Incidents von 191 Tagen auf 197 Tage – ein Hinweis darauf, dass höhere Komplexität die Erkennung von Bedrohungen erschwert.[11] Und es geht nicht mehr nur um Erkennung und Schutz. Cyber-Resilienz – die Fähigkeit, einen Verstoß schnell abzuwehren und zu beheben – ist von entscheidender Bedeutung, da vier von fünf Unternehmen im vergangenen Jahr mindestens einen erfolgreichen unbefugten Zugriff gemeldet haben.[12]

Höhere Komplexität

Die Breite der isolierten Security-Produkte und die zunehmende Disaggregation der Security-Architektur erhöhen die Komplexität des Security Managements für Unternehmen. Mehr als 75 verschiedene Sicherheitslösungen werden von einem durchschnittlichen Unternehmen verwendet, von denen viele auf ein einziges neues Element der Angriffsfläche oder der Compliance-Anforderungen gerichtet sind.[14] In dieser weitgehend disaggregierten Security-Architektur kommunizieren diese unterschiedlichen Lösungen typischerweise nicht miteinander.

Neue und sich ändernde branchenspezifische und gesetzliche Vorschriften wie die Datenschutzgrundverordnung (DSGVO) der Europäischen Union und die Annahme von Sicherheitsstandards wie dem Cybersecurity Framework des Center for Internet Security (CIS) und des National Institute of Standards and Technology (NIST) erschweren das Bild für IT- und Security-Verantwortliche zusätzlich. Das Geschäftswachstum durch Fusionen und Übernahmen sowie flexible Betriebsvereinbarungen mit Auftragnehmern und Service Providern schaffen zusätzliche Stufen der Geschäftskomplexität und Schwachstellen im Hinblick auf das Geräte- und Benutzerzugangs-Management.

Die zunehmende Komplexität, die sich aus diesen unterschiedlichen Problemen ergibt, führt zu einer Überlastung der Cyber-Security-Teams. Der Bedarf zusätzlicher Mitarbeiter zur Steuerung der daraus resultierenden manuellen Arbeitsprozesse kann nicht durch einen höheren Personalbestand gelöst werden. Tatsächlich war es noch nie so schwierig, Cyber-Security-Experten mit den erforderlichen Fähigkeiten zu finden und zu halten. Heute sind weltweit fast 3 Millionen Security-Positionen unbesetzt – eine Zahl, die in den kommenden Jahren voraussichtlich weiter zunehmen wird.[15]

Nahezu 80 % der Unternehmen führen digitale Innovationen schneller ein als ihre Fähigkeit, diese vor Cyber-Angriffen zu schützen.[8]

Bis zu 40 % der an einem bestimmten Tag erkannten neuen Malware ist heute Zero-Day oder war zuvor unbekannt.[13]

65 % der CIOs geben an, dass ein Mangel an Cyber-Security-Nachwuchskräften ihre Unternehmen behindert.[16]

Die Fortinet Security Fabric

Die Fortinet Security Fabric adressiert die drei oben genannten Sicherheitsherausforderungen, indem sie eine breite Sichtbarkeit der gesamten digitalen Angriffsfläche, eine integrierten, KI-gesteuerten Schutz vor Datenschutzverletzungen sowie automatisierte Abläufe, Orchestrierung und Reaktionen bereitstellt.

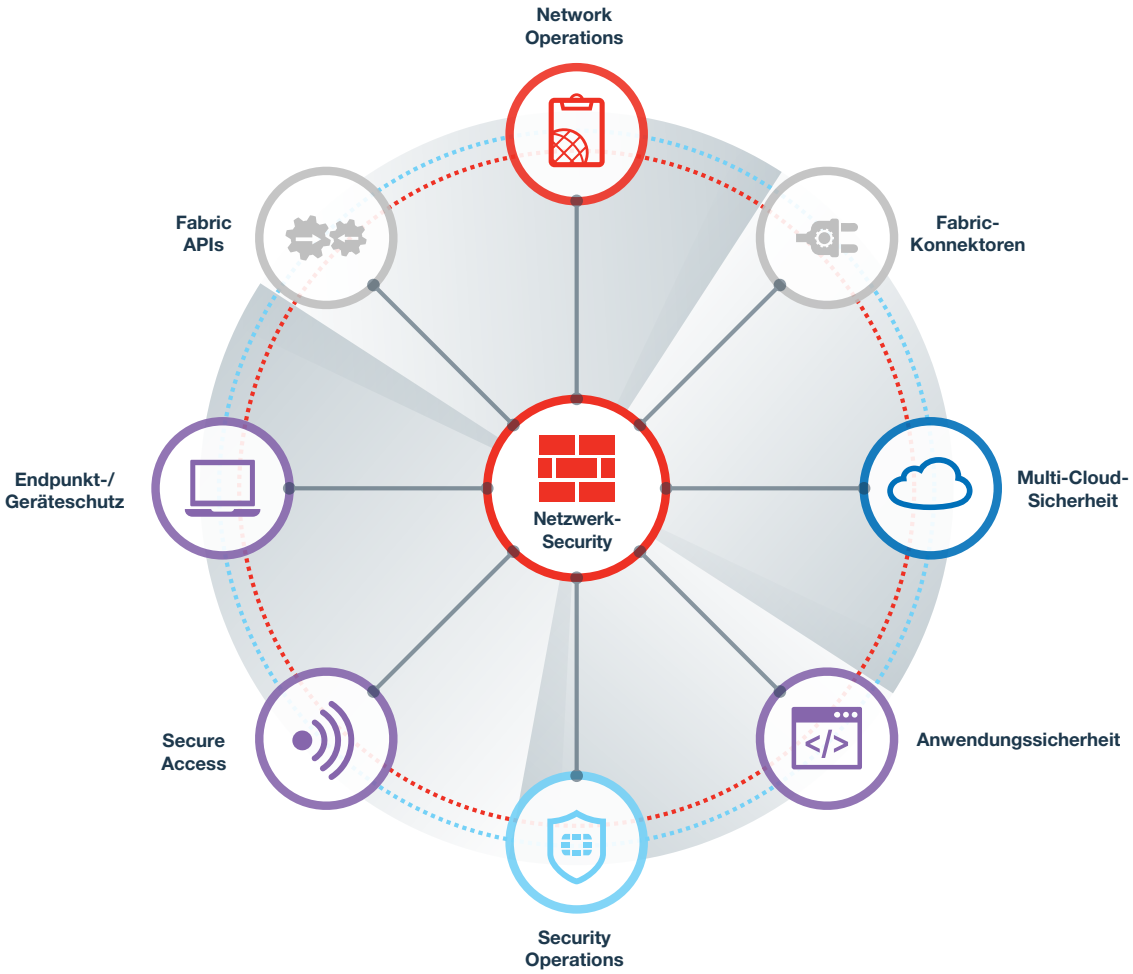


Abbildung 1: Die Fortinet Security Fabric

Die Fortinet Security Fabric ermöglicht es, dass mehrere Security-Technologien nahtlos zusammenarbeiten, über alle Umgebungen hinweg und unterstützt von einer einzigen Threat Intelligence-Quelle. Dadurch werden Security-Lücken im Netzwerk geschlossen und Reaktionen auf Angriffe und Datenschutzverletzungen beschleunigt.

Die in die Security Fabric integrierte absichtsbasierten Segmentierung von Fortinet überwacht kontinuierlich die Vertrauensstufe von Benutzern, Geräten und Anwendungen und steuert den Zugriff dynamisch, basierend auf Geschäftsabsicht, Verhalten und Risiko. Dadurch wird die Angriffsfläche drastisch verkleinert, weil es Eindringlingen erschwert wird, Schwachstellen zu finden und auszunutzen, da ihre seitliche (Ost-West-) Bewegung durch das Netzwerk verhindert wird.

Neben der Integration von Fortinet-Produkten und -Lösungen umfasst die Security Fabric vorgefertigte API-(Application Programming Interface-)Verbindungen für mehr als 70 Fabric-Ready-Partner, die eine tiefe Integration über alle Elemente der Security Fabric hinweg gewährleisten. Darüber hinaus können Security-Produkte, die nicht Teil des Fabric-Ready-Partner-Ökosystems sind, mithilfe von REST-APIs und DevOps-Skripten von Kunden einfach und schnell der Security Fabric hinzugefügt werden.

Eine effektive Segmentierung muss die Geschäftsabsicht nutzen, um das Wo, Wie und Was für eine effektive Sicherheit festzulegen.

Integrierter, KI-gesteuerter Schutz vor Datenschutzverletzungen

Da die Security Fabric die gesamte Angriffsfläche und jedes Security-Element vollständig integriert, kann sie auch globale Threat Intelligence-Daten von den FortiGuard Labs über neu erkannte Zero-Day-Angriffe, komplexe Bedrohungen, Botnets, Indicators of Compromise (IOCs) und mehr teilen.[17]

Um Bedrohungen zu erkennen und Richtlinien durchzusetzen, scannen FortiGate NGFWs den verschlüsselten SSL-(Secure Sockets Layer-) / TLS-(Transport Layer Security-) Datenverkehr. Da verschlüsselter Datenverkehr heute 72 % des gesamten Netzwerkverkehrs ausmacht und 50 % der Cyber-Angriffe verbirgt, ist die Überprüfung des verschlüsselten Datenverkehrs unabdingbar.[18, 19] Im Gegensatz zu anderen Firewall-Lösungen, die dramatische Leistungseinbußen verzeichnen, verwenden FortiGate NGFWs speziell entwickelte Sicherheitsprozessoren (SPUs), um negative Auswirkungen auf die Leistung zu minimieren. Auf diese Weise können Unternehmen vermeiden, ihre Firewall-Infrastruktur nachzurüsten und um weitere Appliances zu erweitern – egal ob im Rechenzentrum oder am Netzwerkrand.

Das Volumen und die Geschwindigkeit bösartiger Angriffe, gepaart mit ihrer zunehmenden Komplexität, machen es für Cyber-Security-Abwehrsysteme schwierig, Schritt zu halten. Die Blockade bekannter Bedrohungen reicht heute nicht mehr aus. Mehr als drei Viertel der erfolgreichen Angriffe nutzen unbekannte oder polymorphe Malware oder Zero-Day-Angriffe.[21] Künstliche Intelligenz (KI) und maschinelles Lernen (ML) bieten Unternehmen die Möglichkeit, Cyber-Kriminellen einen Schritt voraus zu sein. Leider nutzen nur etwas mehr als ein Drittel der Security-Anbieter KI- und ML-Funktionen in ihren Lösungen.

Fortinet hat die Bedeutung dieser Vorgehensweise bereits vor Jahren bei der Entwicklung von FortiGuard AI erkannt. Insbesondere verwendet FortiGuard Labs KI-gesteuerte Funktionen, einschließlich ML, die 4,4 Millionen Sensoren weltweit nutzen. Darüber hinaus bestehen Partnerschaften mit über 200 globalen Unternehmen. Diese KI/ML-gesteuerte Threat Intelligence verwendet 5 Milliarden Knoten, um einzelne bösartige oder saubere Funktionen für bekannte und unbekannte Bedrohungen zu identifizieren. Insgesamt verarbeitet FortiGuard Labs täglich mehr als 100 Milliarden Web-Anfragen und blockiert jede Sekunde 2600 bösartige URLs.[22] Fortinet AI/ML-Funktionen sind auch in FortiWeb und FortiInsight integriert, sodass Unternehmen mit FortiWeb Fehlalarme drastisch reduzieren und forensische Analysen auf Benutzer-, System- und Netzwerkebene nutzen können, um Insider-Bedrohungen mit FortiInsight zu erkennen und zu verhindern.

Andere Funktionen wie Sandboxing und der Einsatz von Ködern spielen ebenfalls eine entscheidende Rolle, wenn es darum geht, komplexe Bedrohungen zu stoppen, bevor sie den Betrieb beeinträchtigen oder zu einer Datenschutzverletzung führen. Insbesondere sind sowohl FortiSandbox[23] als auch FortiDeceptor[24] vollständig in die Security Fabric integriert, sodass sie ihre Threat Intelligence-Daten in Echtzeit über alle Security-Elemente hinweg automatisch teilen können.

Automatisierte Abläufe, Orchestrierung und Reaktionen

Die Anzahl und die Geschwindigkeit von DX-Projekten erschweren es Unternehmen, sich vor komplexen Bedrohungen zu schützen. Fast 80 % der Unternehmen geben zu, dass sie DX mit einem Tempo einführen, das schneller ist als ihre Fähigkeit, sie vor Cyber-Angriffen zu schützen.[26] Dazu kommen neue und sich ändernde Vorschriften, die Einführung von Sicherheitsstandards sowie die Tatsache, dass Bedrohungen schneller und komplexer denn je sind und die Komplexität der Security nimmt exponentiell zu.

Automatisierte Workflows und Orchestrierung – von der Erkennung über den Schutz bis hin zu Reaktionen – werden zur Voraussetzung für jedes Unternehmen, das in dieser komplexen Welt des Security Managements erfolgreich sein will. Hier liefert die Security Fabric greifbare Vorteile.

Die Automatisierung des Netzwerkbetriebs hilft DevOps-Teams, sich auf die Markteinführung zu konzentrieren, verbessert die betriebliche Effizienz durch Zero-Touch-Bereitstellung und liefert Echtzeit-Informationen über die Leistung des Filialnetzwerks zu Problemen wie Spikes, Skalierung und Prioritäts-Routing des Datenverkehrs. Die Automatisierung von Sicherheitsabläufen reduziert das Risiko durch die proaktive Erkennung von Bedrohungen, Bedrohungskorrelationen, Warnmeldungen zum Informationsaustausch sowie durch Bedrohungsforschung und -analyse.

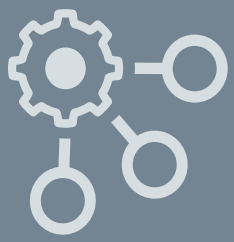
FortiGate NGFWs bieten in Vergleichstests beim Scannen von verschlüsseltem Datenverkehr das führende Preis-Leistungs-Verhältnis. Die Ergebnisse umfassen das Blockieren von 100 % der Umgehungen.[20]

Automatisierung, künstliche Intelligenz und maschinelles Lernen werden nur von 38 % der Unternehmen genutzt. Dies stellt nicht nur eine verpasste Gelegenheit dar, sondern setzt Unternehmen auch komplexen Bedrohungen aus, die herkömmliche Security-Modelle nicht bewältigen bzw. mit denen sie nicht mithalten können.[25]

77 % der Unternehmen verlassen sich bis zu einem gewissem Maße auf nicht integrierte, isolierte Security-Einzelprodukte – und schaffen so Lücken in der Security-Effektivität.[27]

Die Unvermeidlichkeit von erfolgreichen unerlaubte Zugriffen und Datenschutzverletzungen beschert der Cyber-Resilienz erhöhte Aufmerksamkeit.[28] Die Integration von IT Service Management-(ITSM-)Tools ermöglicht die Automatisierung von Ereignisanalysen und -reaktionen. Dies verringert die Reaktionszeiten von Tagen auf Minuten oder sogar Sekunden.

Die Security Fabric nutzt Automatisierung auch, um Compliance-Audits, Tracking und laufende Berichterstellung über Branchenvorschriften und Sicherheitsstandards hinweg zu transformieren. Letztere umfasst Dashboards für den CISO, CIO, CEO und sogar den Vorstand. Dies erspart den Security-Teams unzählige Stunden bei der manuellen Protokollaggregation und -korrelation – einer besonders mühsamen Aufgabe, da es einer disaggregierten Security-Architektur an Transparenz und zentralen Kontrollen mangelt.



Die Automatisierung von Security-Workflows und Threat Intelligence-Daten ermöglicht es auch überlasteten Security-Teams, mit ihren vorhandenen Fähigkeiten und Ressourcen mehr zu erreichen.

Lösungselemente der Security Fabric

Die Security Fabric umfasst acht verschiedene Lösungsbereiche. Jede dieser Bereiche beinhaltet erstklassige, prämierte Lösungen, die von führenden unabhängigen Testorganisationen wie NSS Labs empfohlen und von führenden Analysten wie Gartner anerkannt sind.[29, 30]

Netzwerk-Security

Netzwerk-Security

Die Netzwerksicherheit erstreckt sich vom Rechenzentrum und dem Firmengelände bis an die Grenzen des Netzwerks. Einige der Kernfunktionen der Netzwerksicherheit sind:

SD-WAN-Architekturen können verteilten Unternehmen helfen, schnellere Konnektivität, Kosteneinsparungen und eine verbesserte Cloud-Anwendungsleistung im Vergleich zu herkömmlichen WAN-Umgebungen zu erreichen. Die FortiGate NGFWs beinhalten Fortinet Secure SD-WAN, das Filialnetzwerke und Firewall-Sicherheit in einer einzigen, einheitlichen Lösung vereint. In Kombination mit FortiManager unterstützt Fortinet Secure SD-WAN die Sichtbarkeit und Kontrolle von Anwendungen, die Bereitstellung von hochwertigen Sprach- und Videodaten sowie die konsolidierte Verwaltung von Netzwerken und Sicherheit für Filialnetzwerke. Fortinet SD-Branch integriert Secure SD-WAN-Funktionen in das lokale Netzwerk (LAN) und erweitert die Sicherheit auf der Zugriffsebene.

NGFWs vereinfachen die Komplexität der Sicherheit und bieten Einblick in Anwendungen, Benutzer und Netzwerke. FortiGate NGFWs nutzen speziell entwickelte Security-Prozessoren und Threat-Intelligence-Dienste von FortiGuard Labs, um erstklassige Sicherheit und leistungsstarken Schutz vor Bedrohungen zu bieten (z. B. Intrusion Prevention, Web Filtering, Anti-Malware, Application Control). Die automatisierten, richtlinienbasierten FortiGate NGFW-Reaktionen beschleunigen die Zeit bis zur Problembehebung.

Absichtsbasierte Segmentierung übersetzt die Geschäftsabsicht effizient in eine feinkörnige Zugriffskontrolle, die auf der Grundlage der kontinuierlichen Gefahrenbewertung von Benutzern, Geräten und Anwendungen angepasst wird. Die tiefe Integration in die Fortinet Security Fabric-Lösungen ermöglicht die absichtsbasierte Segmentierung, die das Verteidigungsprofil eines Unternehmens verbessert, Risiken abwehrt, Compliance unterstützt und die betriebliche Effizienz steigert.

Management- und Analyse-Tools ermöglichen es Security-Teams, mit begrenzten Ressourcen mehr zu erreichen. Fortinet Management- und Analyselösungen (z. B. FortiAnalyzer, FortiCloud, FortiManager, FortiSIEM) bieten effiziente Verwaltung, transparente Sichtbarkeit, Informationen und Echtzeit-Erkenntnisse über die gesamte Security Fabric hinweg. Sie vereinfachen Management-Workflows, verkürzen die Implementierungszeiten und verringern die Wahrscheinlichkeit von Fehlkonfigurationen durch menschliche Fehler.

Cloud-Sicherheit

Cloud-Sicherheit

Fortinet-Lösungen für Cloud-Sicherheit bieten hervorragende Transparenz, Schutz und Kontrolle über Public, Private, SaaS- und Hybrid Cloud-Umgebungen. Fortinet Cloud-Security bietet Sichtbarkeit durch eine zentrale Konsole und einheitliche Sicherheit über mehrere Cloud-Implementierungen hinweg. Zu den Kernbereichen der Lösung gehören:

Lückenlose **Transparenz und Kontrolle** für Public Clouds wird durch den FortiCASB Cloud Access Security Broker (CASB) für die Überwachung und Konfiguration von Cloud-Implementierungen und SaaS-Anwendungen ermöglicht. FortiGate-VM bietet erweiterten Schutz für den Client-Server-(Nord-Süd-)Datenverkehr in einer virtualisierten Umgebung wie einer Private Cloud oder einem Software-Defined Datacenter (SDDC). Es ermöglicht zentralisierte Transparenz und Kontrolle sowie die vollständige Automatisierung von Sicherheitsprozessen in Verbindung mit anderen Security-Elementen innerhalb der Security Fabric. FortiGate-VM ermöglicht auch Deep Packet Inspection – sowohl von verschlüsseltem als auch von unverschlüsseltem Datenverkehr – von Server-Server-(Ost-West-)Anwendungen und Benutzerdatenverkehr zwischen virtuellen Maschinen. FortiSIEM, FortiManager und FortiAnalyzer bieten Cloud-Erkenntnisse durch Management- und Analysefunktionen und liefern gleichzeitig umfassende Cloud-Compliance-Tracking und Berichterstellung.

Die **Anwendungssicherheit** für Cloud-Bereitstellungen nutzt die Mikrosegmentierung mit FortiGate-VM, um Workloads voneinander zu isolieren und individuell zu sichern, wodurch die seitliche (Ost-West-)Bewegung bösartiger Angriffe eingeschränkt wird. Fortinet bietet auch Sicherheit, die in den Anwendungslebenszyklus von Containern integriert werden kann. FortiGate-VM verbindet sich mit der Containerverwaltungsstufe und lernt die Labels verschiedener Container. FortiWeb dient als Container-Image, das es Entwicklern ermöglicht, Sicherheitskontrollen entlang ihres Anwendungsentwicklungs-Lebenszyklus einzuführen und die Anwendungssicherheit zusammen mit anderen Anwendungsdiensten während des gesamten Anwendungslebenszyklus zu portieren. FortiSandbox-VM reduziert das Risiko, das durch agile Entwicklungsmethoden entsteht, durch die Integration in Anwendungscontainer.

Sichere Konnektivität ermöglicht Hochgeschwindigkeits-VPN-Funktionen für den sicheren Datentransfer über hybride Infrastrukturen hinweg. Dank der Security Fabric verfügen Unternehmen über transparente Sichtbarkeit, einheitliche Kontrollen und eine zentralisierte Durchsetzung von Richtlinien in allen Cloud-Umgebungen. Sie können auch vorkonfigurierte Instanzen von FortiGate-VM global über alle Clouds hinweg bereitstellen und haben über den nächstgelegenen Zugangspunkt im Netzwerk immer eine Verbindung zu den Geschäftsanwendungen.

Anwendungs-sicherheit

Anwendungssicherheit

Angriffe, die auf Anwendungen abzielen, erfordern zusätzliche Schutzmaßnahmen, die eine Firewall oder ein Intrusion Prevention System (IPS) nicht bieten kann. Unternehmen benötigen Web Application Firewalls, Application Delivery Controller und Sandboxing, um den neuesten Bedrohungen zu begegnen. Innerhalb der Security Fabric erhalten webbasierte Anwendungen mehr Schutz als bei der Verwendung von Security-Einzelprodukten.

Web-Anwendungslösungen bieten einheitliche Sicherheit, um die mit cloudbasierten Anwendungen verbundenen Risiken abzuwehren. Dies ermöglicht es der Security Fabric, den Schutz anfälliger Systeme zu optimieren und eine umfassende Sichtbarkeit webbasierter, öffentlich zugänglicher Anwendungen zu erhalten. Fortinet unterstützt auch die Compliance für regulierte Anwendungen, einschließlich Vorlagen zur Vereinfachung der laufenden regulatorischen Anforderungen und Abläufe – wie beispielsweise für den Payment Card Industry Data Security Standard (PCI DSS).

E-Mails erfordern eine dedizierte erweiterte Bedrohungserkennung. Die Security Fabric enthält Lösungen zur Sicherung von cloudbasierten E-Mails über SaaS, Public Cloud oder API-basierte Implementierung (als Ergänzung zu den integrierten Funktionen von Microsoft Office 365 oder Google G Suite). Dazu gehört auch die konsolidierte E-Mail-Sicherheit über ein umfassendes Secure Email Gateway-(SEG-)Angebot.

Security Operations

Security Operations

Die Security Fabric bezieht Netzwerkelemente außerhalb der Fortinet-Produktfamilie (d. h. bereits vorhandene Infrastruktur) in den Kontext mit ein, um den Sicherheitsbetrieb zu verbessern. Dies bietet Unternehmen einen umfassenden Schutz, der sowohl das IT- als auch das Security-Risiko-Management im gesamten Unternehmen abdeckt. FortiSIEM, FortiAnalyzer und FortiManager sowie FortiGuard Threat Intelligence-Daten erfüllen diese Anforderungen gemeinsam.

Verhindern Sie Cyber-Bedrohungen, indem Sie mit der sich entwickelnden Bedrohungslandschaft Schritt halten. Kuratierte Threat-Intelligence-Feeds für Dinge wie bösartige Dateien und IP-Adressen helfen, Angriffe weit vor ihrem Eintreten zu stoppen. Konsolidierte Sicherheit über mehrere Disziplinen hinweg mit FortiAnalyzer teilt Informationen in Echtzeit und ermöglicht koordinierte, absichernde Verteidigungsreaktionen.

Erweiterte Funktionen zur Bedrohungserkennung, unterstützt von den FortiGuard Labs, sichten Bedrohungen wie neue Malware-Varianten. FortiSandbox ist in allen Formfaktoren verfügbar, integriert sich in alle Elemente der Security Fabric und ermöglicht es Unternehmen, bekannte und unbekannte Bedrohungen zu identifizieren, bevor sie sich auf das Unternehmen auswirken. FortiDeceptor setzt Köder ein, die zur Analyse von Bedrohungsaktivitäten und zum Austausch von Informationen in der gesamten Security Fabric verwendet werden.

Automatisierte Reaktionen auf Security Incidents verkürzen die Zeit bis zur Problemlösung bei Erkennung, Schutz und Gegenmaßnahmen. Die Automatisierungsfunktionen der Security Fabric umfassen flexible Workflows, die richtlinienbasierte Ereignisauslöser, Reaktionsmaßnahmen und Genehmigungen kombinieren, um Bedrohungen schnell einzudämmen.

Compliance-Unterstützung in der Security Fabric umfasst Out-of-the-Box-Berichterstellung für PCI DSS und andere regulatorische Kontrollen, die den Berichts- und Auditaufwand für unterbesetzte Security Teams reduzieren. Die Security Fabric ermöglicht auch die automatisierte Bewertung von Kontrollen anhand von NIST, CIS und anderen Security Best Practices. Darüber hinaus bietet sie quantifizierte Risikobewertung, sowohl intern über Zeiträume hinweg als auch im Vergleich mit ähnlichen Unternehmen über den Security Rating Service.

Schulungsunterstützung umfasst öffentliche Module für Mitarbeiter und Führungskräfte, die sich auf Bedrohungen, Security-Technologien und Lösungen konzentrieren. Technische Schulungen werden über ein offizielles achtstufiges Network Security Expert-Zertifizierungsprogramm für Fortinet-Produkte und -Lösungen angeboten.

Secure Access

Secure Access

Unternehmen mit verteilten Niederlassungen sehen sich in einer Welt von Multi und Hybrid Cloud-Bereitstellungen mit Komplexität konfrontiert. Sie setzen Technologien wie SD-WAN ein, um Performance-Probleme zu lösen, und ermöglichen den Netzwerkverkehr über das öffentliche Internet. Aber diese Art von Datenverkehr birgt Risiken, und es ist unerlässlich, dass die Sicherheitsstrategien der nächsten Generation in Multi-Path-WAN-Implementierungen integriert werden.

Die Fortinet SD-Branch-Lösung integriert Fortinet Secure SD-WAN mit dem LAN an jedem Standort und umfasst gemeinsame Verwaltungstools in einer einzigen Konsole. Mit SD-Branch haben Unternehmen eine verbesserte Sichtbarkeit auf Filial- und Unternehmensebene und können Security- und Netzwerkprozesse nutzen. Das Ergebnis ist, dass die Security auf die Zugriffsebene ausgedehnt wird und globale Sicherheitsrichtlinien automatisch auf Filialebene angewendet werden können.

Benutzer, Endpunkt und Zugriff

Benutzer, Endpunkt und Zugriff

Die Fortinet Security Fabric unterstützt auch umfassende Sicherheit für Geräte und Endanwender mit folgenden Funktionen:

FortiClient bietet Advanced Threat Protection zum Schutz vor Exploits und fortschrittlicher Malware, basierend auf Threat Intelligence-Daten der FortiGuard Labs, um eine wachsende Anzahl von **IoT-Geräten** zu schützen, denen es oft an integrierter Security mangelt. FortiClient kann mit anderen Security Fabric-Lösungen wie FortiSandbox über Fabric Connectors integriert werden und bietet so Schutz vor bekannten und unbekannten Bedrohungen. FortiClient bietet auch ein Schwachstellen-Dashboard, das Administratoren bei der Verwaltung der Angriffsfläche und der Durchführung von On-Demand-Schwachstellenüberprüfungen unterstützt.

Endpunkt-Sichtbarkeit und -Schutz bedeuten, dass ein Administrator eine umfassende Sicht auf jedes mit dem Netzwerk verbundene Gerät hat. Die Endpunkt-Telemetrie- und Compliance-Lizenz für FortiGate NGFWs bietet eine einheitliche Sicht auf alle Elemente der Security Fabric und ermöglicht die zentrale Durchsetzung von Sicherheitsrichtlinien für Endgeräte.

Identitäts- und Zugangs-Management mit FortiAuthenticator unterstützt die absichtsbasierte Segmentierung durch die Zentralisierung von Benutzeridentitätsinformationen und hilft Unternehmen, der richtigen Person zur richtigen Zeit den richtigen Zugriff sicher bereitzustellen. Fortinet Single Sign-On (SSO) ermöglicht einen nahtlosen Schutz für den Endanwender. Die Zwei-Faktor-Authentifizierung wird durch FortiToken ermöglicht, das FortiGate NGFWs als Authentifizierungsserver für eine skalierbare Lösung mit geringen Einstiegskosten und niedrigen Gesamtbetriebskosten (TCO) nutzt. Und mit der FortiInsight Benutzer- und Entitätsverhaltensanalyse (User and Entity Behavioral Analysis, UEBA) können Unternehmen den Schutz vor Insider-Bedrohungen verbessern, indem sie Verhaltensanomalien erkennen, die auf eine Bedrohung hinweisen könnten.

Fabric API

Fabric-Konnektoren

Offenes Ökosystem

Das offene Ökosystem der Fortinet Security Fabric vereint Security-Lösungen und ermöglicht es ihnen, zu kommunizieren und zusammenzuarbeiten. Die Integration umfasst die folgenden Elemente:

Die **Fabric-API** ermöglicht es Technologieanbietern, Integrationen für ihre Produkte mit der Fortinet Security Fabric zu entwickeln. Dutzende von Fabric-Ready-Partnern decken ein breites Spektrum an Technologien ab und ermöglichen Unternehmen den integrierten, einheitlichen Schutz einer sich ständig erweiternden Angriffsfläche. Für Kerntechnologiebereiche können Kunden von Fortinet validierte Integrationen oder gemeinsame Lösungen mit Partnern nutzen.

Fabric-Konnektoren ermöglichen eine tiefere, API-basierte Integration für verschiedene Plattformen im Ökosystem eines Unternehmens und eine nahtlose Verbindung mit der Fortinet Security Fabric. Sie lassen sich leicht mit einem einfachen Klick auf die grafischen Benutzeroberfläche implementieren und erfordern keine Hard- oder Software-Änderungen an bestehenden Systemen. Fabric-Konnektoren ermöglichen einen automatisierten, konsistenten Security-Schutz in einer komplexen Hybridumgebung.

DevOps-Skripte automatisieren das Security Provisioning und das Konfigurations-Management von Fortinet unter Verwendung der offenen Architektur der Fortinet Security Fabric. Fortinet, seine Partner und Kunden haben verschiedene Skripten entwickelt, die Unternehmen dabei unterstützen, unterschiedliche Security-Lösungen in das einheitliche Fabric Framework zu integrieren. Sie helfen Unternehmen, mit den schnellen Veränderungen sowohl der IT-Infrastruktur als auch der Bedrohungslandschaft Schritt zu halten. DevOps-Skripte sind einfach auszuführen und befinden sich im Fortinet Developer Network und auf GitHub.

Network Operations

Network Operations

Die Fortinet Security Fabric ermöglicht einen reibungslosen Netzwerkbetrieb und erlaubt es dem Network Operations Center (NOC), die gleiche Management-Konsole wie das Security Operations Center (SOC) zu nutzen.

Management über eine zentrale Konsole bedeutet, dass alle Netzwerkbetriebsabläufe zentral überwacht werden, wobei neue Ressourcen per Zero-Touch-Provisioning bereitgestellt werden, um die Komplexität zu reduzieren. Auch die Konfigurationen werden für alle Geräte zentral verwaltet und Revisionen gesichert. Administratoren haben die volle, zentralisierte Kontrolle mit sofort einsatzbereiten Workflows und Skripten sowie der offenen Fortinet-API für unternehmensspezifische Anforderungen.

Best-Practice-Compliance ermöglicht es Unternehmen, nicht nur Vorschriften und Standards einzuhalten, sondern auch das Risiko entsprechend der Risikotoleranz zu steuern, die von den Compliance-Anforderungen abweichen kann. Der Security Rating Service bietet einen objektiven Risiko-Score anhand anerkannter Benchmarks und im Vergleich zu Marktbegleitern sowie fundierte Ratschläge, wie ein besseres Risiko-Management-Profil erreicht werden kann. FortiManager unterstützt Unternehmen bei der Verfolgung von Richtlinienänderungen über das gesamte Netzwerk hinweg, registriert, wer sie vorgenommen hat, und hilft bei der Bewältigung der Komplexität, indem ungenutzte Richtlinien eliminiert und konsolidiert werden.

Automatisierung und Orchestrierung optimieren den Betrieb über das gesamte Unternehmen hinweg. Die Workflow-Optimierung bietet Workflow-Kontrollen zur Richtlinienänderung, um die Möglichkeit der Benutzer einzuschränken, Richtlinien auf eine Weise zu ändern, die die Sicherheit einschränken könnte. Fabric-Ready Workflow-Tool-Integrationen rationalisieren den Betrieb und reduzieren das Risiko. Und für die DevOps-Umgebung können Unternehmen eine schlüsselfertige Verwaltung mit Skripten und Playbooks für ihre Continuous Integration-(CI-) / Continuous Delivery-(CD-) Integrationen implementieren.

Risiken verwalten, Chancen verfolgen

DX ist eine Chance für nahezu jedes Unternehmen, mehr Flexibilität und Kosteneffizienz für sich selbst und bessere Erfahrungen für seine Kunden zu erzielen. Gleichzeitig erhöht DX die digitale Angriffsfläche, bietet Hackern innovative Möglichkeiten, immer ausgefeiltere Angriffe zu generieren, und trägt zu einer wachsenden Komplexität von Vorschriften und Security-Lösungen bei.

Dies wird aufstrebende Führungskräfte nicht aufhalten – diejenigen, die eine Grundlage für das Risiko-Management schaffen, die es ihren Unternehmen ermöglicht, bei der Umsetzung von DX schneller als andere zu sein. Die Fortinet Security Fabric bietet die Basis dafür. Sie vereinheitlicht Security-Lösungen über eine zentrale Konsole, macht die wachsende digitale Angriffsfläche sichtbar, integriert den KI-gesteuerten Schutz vor Datenschutzverletzungen und automatisiert Betriebsabläufe, Orchestrierung und Reaktionen. Zusammenfassend lässt sich sagen, dass sie es Unternehmen ermöglicht, mit DX neuen Mehrwert zu schaffen, ohne die Sicherheit im Tausch für Agilität, Leistung und einfache Bedienung zu beeinträchtigen.

[1] „CIO Survey 2018: The Transformational CIO“, Harvey Nash and KPMG, 25. May 2018.

[2] Louis Columbus, „83% Of Enterprise Workloads Will Be In The Cloud by 2020,“, Forbes, 7. Januar 2018.

[3] „Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)“, Statista, letzter Zugriff 20. März 2019.

[4] „25% Of Cyberattacks Will Target IoT In 2020“, Retail TouchPoints, letzter Zugriff 21. März 2019.

[5] Zeus Kerravala, „Understanding Virtual Private Networks [and why VPNs are important to SD-WAN]“, Network World, 13. April 2018.

[6] „State of the CIO and Security Report“, Fortinet, April 2019.

[7] „2018 Data Breach Investigations Report“, Verizon, 10. April 2018.

[8] Kelly Bissell, et al., „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“, Accenture and Ponemon, 6. März 2019.

[9] „Quarterly Threat Landscape Report: Q4 2018“, Fortinet, Februar 2019.

[10] Kevin Williams, „Threat Spotlight: Advanced polymorphic malware“, SmarterMSP.com, 13. Juni 2018.

[11] „2018 Cost of a Data Breach Study“, Ponemon, Juli 2018.

[12] „The CISO and the State of Cybersecurity Report“, Fortinet, April 2019.

[13] Laut internen Daten von FortiGuard Labs.

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

[15] „Cybersecurity Skills Shortage Soars, Nearing 3 Million“, (ISC)², 18. Oktober 2018.

[16] „CIO Survey 2018: The Transformational CIO“, Harvey Nash and KPMG, 25. Mai 2018.

[17] „FortiGuard Labs“, Fortinet, letzter Zugriff 22. März 2019.

[18] John Maddison, „Encrypted Traffic Reaches A New Threshold“, Network Computing, 28. November 2018.

[19] „Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity“, Lifeline Data Centers, letzter Zugriff 21. März 2019.

[20] „Fortinet Receives Recommended Rating in Latest NSS Labs NGFW Report, Delivers High SSL Performance Suited for Encrypted Cloud Access“, Fortinet, 17. Juli 2018.

[21] Charlie Osborne, „Zero-days, fileless attacks are now the most dangerous threats to the enterprise“, ZDNet, 16. Oktober 2018.

[22] „Threat Intelligence with Integrated AI and ML Reduces Risk and Supports Performance“, Fortinet, 29. September 2018.

[23] „Mapping the Requirements of Next-Generation Sandboxing to Address the Advanced Threat Landscape“, Fortinet, 13. Juni 2018.

[24] „FortiDeceptor Enables a New Breach Protection Approach“, Fortinet, *in Kürze erscheinend*.

[25] Kelly Bissell, et al., „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“, Accenture and Ponemon, 6. März 2019.

[26] Ibid.

[27] Patrick E. Spencer, „Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study“, Scalar Security Blog Post, 20. Februar 2019.

[28] „State of the CIO and Security Report“, Fortinet, April 2019.

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

[30] „2018 Gartner Magic Quadrant Reports“, Fortinet, letzter Zugriff 21. März 2019.

FORTINET

www.fortinet.de

Copyright © 2019 Fortinet, Inc. Alle Rechte vorbehalten. Fortinet®, FortiGate®, FortiCare® und FortiGuard® sowie bestimmte andere Marken sind eingetragene Marken von Fortinet, Inc. Bei anderen hier aufgeführten Namen von Fortinet kann es sich ebenfalls um eingetragene und/oder Gewohnheitsmarken von Fortinet handeln. Alle weiteren Produkt- und Unternehmensnamen sind u. U. Marken ihrer jeweiligen Eigentümer. Leistungs- und andere hierin enthaltenen Kennzahlen stammen aus internen Labortests unter idealen Bedingungen. Die tatsächliche Leistung und andere Ergebnisse können davon abweichen. Keine der hierin enthaltenen Angaben stellt eine verbindliche Verpflichtung durch Fortinet dar und Fortinet lehnt alle ausdrücklichen oder implizierten Garantien ab. Ausnahme: Fortinet geht einen verbindlichen, schriftlichen Vertrag mit einem Käufer ein, der vom Leiter der Rechtsabteilung von Fortinet unterzeichnet wird und der eine ausdrückliche Garantie dafür gewährt, dass ein bestimmtes Produkt entsprechend den genau angegebenen Leistungskennzahlen bestimmungsgemäß funktioniert. In diesem Fall sind ausschließlich die in diesem verbindlichen, schriftlichen Vertrag aufgeführten spezifischen Leistungskennzahlen für Fortinet bindend. Jede diesbezügliche Garantie beschränkt sich einzig auf die Leistung unter den gleichen idealen Bedingungen wie bei den internen Labortests von Fortinet. Fortinet lehnt dementsprechend jegliche ausdrücklichen oder implizierten Verpflichtungen, Zusagen und Garantien ab. Fortinet behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu bearbeiten, zu übertragen oder anderweitig zu überarbeiten. Es gilt die jeweils aktuellste Fassung der Veröffentlichung.

September 10, 2019 11:29 vorm.

381915-0-1-DE

E:\PRACE\ARGOS\2019\09 2019\A-344888-924139\de-DE\FSF-FortiOS 6.2\wp-security-fabric-A4_de-DE