STRATEGIES BRIEF

Strategien zum Schutz der Enterprise Cloud

Das Fortinet-Konzept für die Cloud-Security

Zusammenfassung

Unternehmen setzen zunehmend Cloud-Plattformen ein, um im Rahmen digitaler Innovationsinitiativen (DI) ihre Investitionskosten zu senken und mehr Agilität zu gewinnen. Ungeachtet der Vorteile führt dies jedoch dazu, dass geschäftskritische Daten und Dienste immer mehr über Clouds und Rechenzentren verteilt sind. Die Folge ist eine erweiterte Angriffsfläche, die mit erhöhten Sicherheitsrisiken einhergeht.

Einige Unternehmen stoßen dabei unwissentlich auf ein neues Sicherheits-paradigma: das Modell der geteilten Verantwortung. Dieses Modell basiert auf der Annahme, dass die Cloud-Infrastruktur vom Cloud-Anbieter geschützt wird, während die Security für in der Cloud verwendete Dienste in der Verantwortung des Unternehmens liegt.

Die Fortinet Security Fabric wurde eigens entwickelt, um diese cloudbedingten Sicherheitslücken zu schließen. Als Sicherheitsstruktur bietet sie eine native Integration in Public-Cloud-Infrastrukturen, eine breite Palette von Security-Diensten und -Produkten, ein cloudübergreifendes Security-Management sowie umfassende Tools für die Automatisierung und Analyse.

Unternehmen nutzen durchschnittlich 61 verschiedene Cloud-Anwendungen.[1]

Einleitung

Fortinet geht davon aus, dass die digitale Transformation zu einer massiven Zunahme der Cloud-Anwendungen führen wird. Durch die Heterogenität der so entstehenden Cloud-Umgebungen wird die gesamte Angriffsfläche vergrößert, was den Schutz von Anwendungen zunehmend erschwert. Obwohl das allgemeine Vertrauen in die Cloud im letzten Jahrzehnt stark gewachsen ist, ruft der Sicherheitsaspekt nach wie vor große Bedenken bei Führungskräften und IT-Experten hervor. Es ist daher unerlässlich, dass Security-Elemente nicht nur ein integraler Bestandteil bei der Gestaltung einzelner Cloud-Lösungen sind, sondern auch bei der Gesamtstrategie für die Umstellung auf dynamische Multi-Cloud-Infrastrukturen von Anfang an implementiert werden.

Eine komplexe Palette von Security-Ansätzen

Cloud-Anbieter unternehmen größte Anstrengungen, um ihre Infrastruktur zu schützen. Dennoch unterscheiden sich die Ansätze, wie native Cloud-Security-Funktionen implementiert und verwaltet werden. Häufig führen unterschiedliche Cloud-Anbieter dieselben Security-Dienste unter Verwendung unterschiedlicher Tools und Ansätze aus.

Amazon Web Services (AWS) erweitert seine Security-Richtlinien zum Beispiel basierend auf Sicherheitsgruppen, die Cloud-Ressourcen zugewiesen sind. Dagegen setzt die Google Cloud Platform (GCP) Firewall-Regeln ein, die die gleiche Funktionalität bereitstellen, aber über andere Schnittstellen verwaltet werden. Viele dieser Unterschiede gehen auf anbieterspezifische Ansätze für die Abläufe in der Cloud zurück sowie darauf, wie die der Cloud zugrunde liegende Architektur strukturiert ist.

Für Kunden, die mit mehreren Clouds arbeiten, ist eine heterogene Architektur ohne zentrale Transparenz oder Kontrolle und somit ohne konsequente Durchsetzung und Verwaltung der Security leider der „Sicherheitsstandard“. In diesem Kontext wird jede Public und Private Cloud – ebenso wie On-Premises-Rechenzentren – zu isolierten Systemen in einer fragmentierten Security-Infrastruktur.

Das Cloud-Modell der gemeinsamen Verantwortung

Das Modell der gemeinsamen Verantwortung definiert die Rollen von Cloud-Anbietern und Kunden bei der Security für cloudbasierte Anwendungen und Daten. Bei diesem Modell sind Cloud-Anbieter für den Schutz der zugrunde liegenden Infrastruktur vor illegaler Nutzung, Intrusion und Missbrauch sowie für die Trennung einzelner Kunden verantwortlich, während Kunden die Sicherung der Ressourcen und Dienste in der Cloud-Umgebung übernehmen.

Es gibt verschiedene Modelle der gemeinsamen Verantwortung, die von der Art der Kunden-Implementierung abhängen. Je nach Cloud-Dienst variiert, wie die Zuständigkeiten im Detail zwischen Kunde und Cloud-Anbieter aufgeteilt werden.

Bei SaaS-Bereitstellungen (Software-as-a-Service) verfügen Kunden lediglich über grundlegende Sicherheitskontrollen. So liegt beispielsweise der Schutz von Office 365 in der Verantwortung von Microsoft: Der Software-Hersteller muss dafür sorgen, dass seine Anwendung nicht kompromittiert werden kann und dass Kunden sicher auf die Software zugreifen können. Kunden hingegen sind für die Konfiguration der Plattform, die Verfolgung von Sicherheitsvorfällen und ihre Daten verantwortlich.

Bei Implementierungen, die auf einer Public Cloud basieren – wie IaaS (Infrastructure-as-a-Service) oder PaaS (Platform-as-a-Service) –, muss der Kunde stärker bei der Sicherheit einbezogen werden. Denn diese umfassen größere Infrastrukturen, die sicher konfiguriert und verwaltet werden müssen. Zwar bieten einige Public-Cloud-Provider eigene Security-Tools an, doch die Auswahl, Konfiguration, Verwaltung und Anpassung der Sicherheitslösungen liegt weiterhin beim Kunden. In solchen Fällen ist der Kunde verantwortlich für die Plattformkontrolle und -konfiguration, die Transparenz über Sicherheitsvorfälle, die Zugangskontrolle, die Datenverschlüsselung und die Anwendungssicherheit, die z. B. über eine Web Application Firewall (WAF) bereitgestellt werden kann. Weiter trägt der Kunde die Verantwortung für die Sicherheit sämtlicher On-Premises-Elemente von hybriden Anwendungen.

Lösungen von Security-Anbietern wie Fortinet gewährleisten die umfassende Sicherheit, die Kunden für einen effektiven Schutz von allem, was sie in der Cloud erstellen, bereitstellen oder speichern, benötigen.

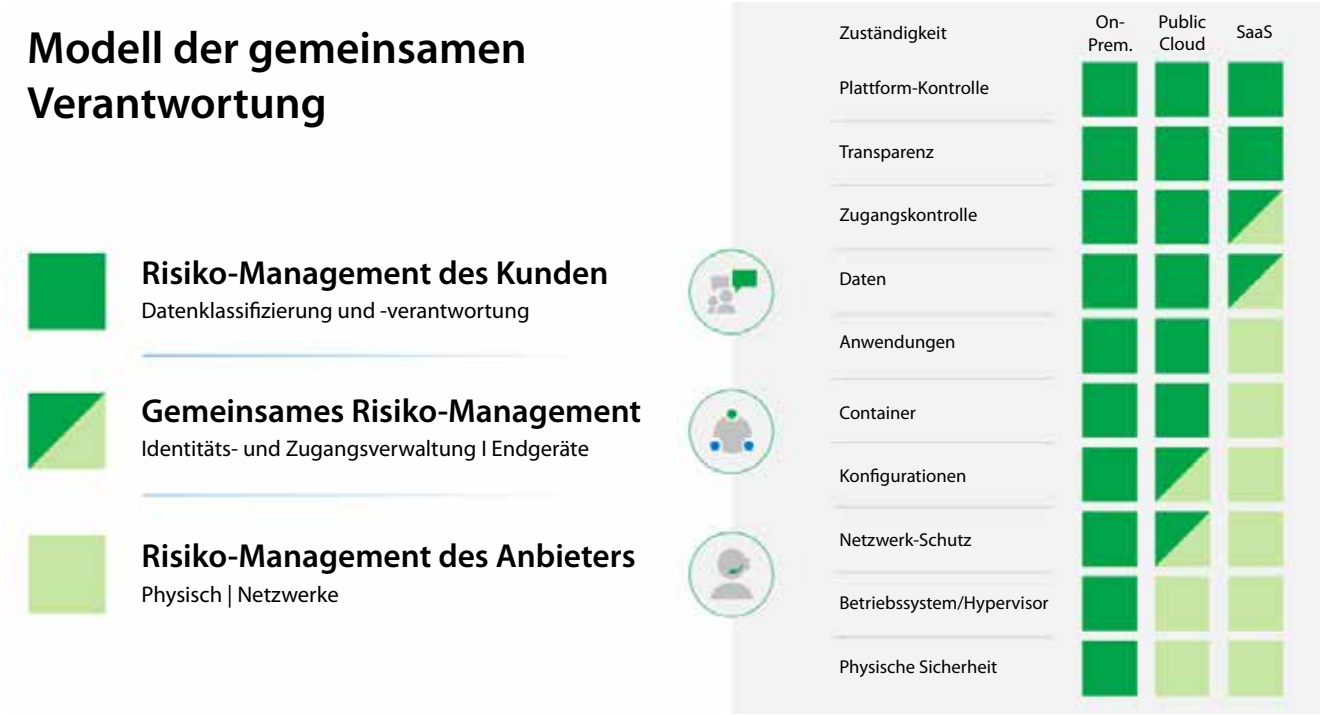

Abbildung 1: Beim Modell der gemeinsamen Verantwortung sind Kunde und Cloud-Anbieter für den Schutz unterschiedlicher Ressourcen verantwortlich.

Elemente einer umfassenden Security

Die heutige Bedrohungslage erfordert einen konsequenten, einheitlichen Ansatz für die Cloud-Sicherheit. Fortinet folgt drei übergreifenden Grundsätzen bei der Entwicklung einer effektiven Multi-Cloud-Sicherheitslösung:

1. Native Integration
2. Umfassender Schutz
3. Management und Automatisierung

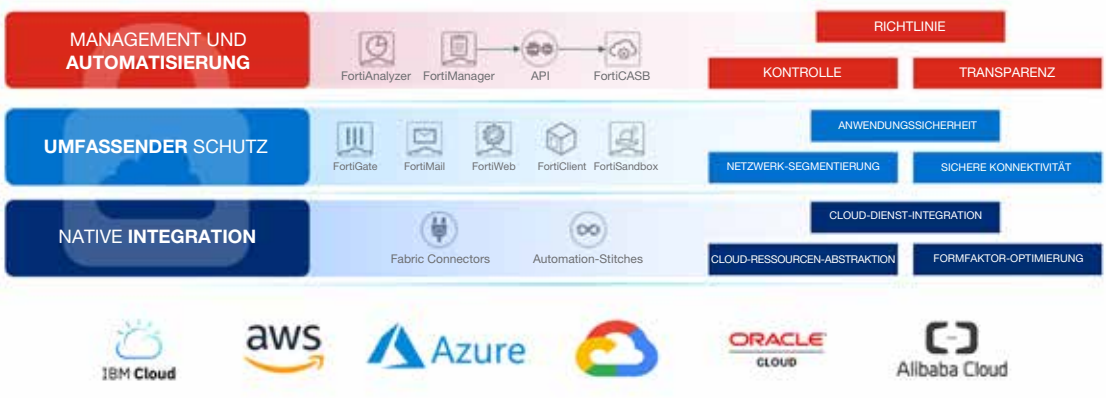

Abbildung 2: Ansatz von Fortinet für die Multi-Cloud-Security

Eine effektive Sicherheitslösung für die Cloud muss unter Berücksichtigung dieser drei Elemente entwickelt werden, um einen optimalen Schutz für ein dynamisches Cloud-Unternehmen zu bieten. Wie die Grafik zeigt, sind diese Prinzipien bei Cloud-Security-Lösungen von Fortinet bereits von Grund auf integriert.

1. Native Integration

Fortinet unterscheidet sich von anderen Cloud-Security-Anbietern durch eine breite, native Integration in Public-Cloud-Plattformen. Eine native Integration unterstützt Lösungen dabei, die Klassifikation cloudbasierter Informationen für ein umfassendes Richtlinien-Management und Funktionen zur Bedrohungsabwehr zu nutzen. Auch können native Cloud-Dienste zur Automatisierung, Bedrohungsüberwachung und Nachverfolgung eingesetzt werden. Im Folgenden wird näher auf einige der wichtigsten Funktionen der vollständig integrierten Cloud-Security-Lösung von Fortinet eingegangen:

Fabric Connectors: Security-Lösungen von Fortinet lassen sich programmatisch in eine Cloud-Plattform integrieren, um maximale Sicherheit ohne operativen Mehraufwand zu gewährleisten.

Da Cloud-Ressourcen gewöhnlich Metadaten und Labels nutzen, um ihre logische Funktion anzugeben oder ihre Informationen zu klassifizieren, und IP-Adressinformationen keine zuverlässige Grundlage für Sicherheitsentscheidungen bieten, können Fabric Connectors zur Normalisierung der verschiedenen Arten von Ressourcen-Metadaten über mehrere Clouds hinweg verwendet werden. Das vereinfacht die Entwicklung und Durchsetzung einheitlicher Sicherheitsrichtlinien übergreifend über Regionen und Clouds.

Komplexere Fabric-Connector-Implementierungen erfassen sämtliche Cloud-Ressourcen und stellen sie umfassend in einer Netzwerk-Topologie dar. Das erleichtert Security-Teams die Überprüfung ihres Cloud-Sicherheitsprofils und die Implementierung effektiver Richtlinien.

Optimierung: Während einige Anbieter ihr Hardware-Betriebssystem einfach auf eine virtuelle Instanz portieren, wurden Fortinet-Lösungen von Grund auf für die Implementierung in der Cloud entwickelt. Fortinet-Lösungen erfüllen eine Vielzahl unterschiedlichster Ressourcen- und Leistungsanforderungen – von Images mit geringem Speicherbedarf bis hin zu umfassenden Lösungen. Schlanke Lösungen sind ideal für Scale-out-Architekturen, da sie sich ganz nach Bedarf bereitstellen lassen. Umfassende Lösungen ermöglichen dagegen den Einsatz leistungsstarker Netzwerk-Treiber auf verschiedenen Cloud-Plattformen wie Azure Accelerated Networking, AWS-C5n-Instanzen oder die Arbeit im nativen Modus von Oracle.

Automatisierung: Fortinet vereinfacht die Automatisierung von Routine-Aufgaben wie Reaktionen auf verschiedene Arten von Bedrohungen mit Automation-Stitches, Automatisierungsvorlagen und einer robusten Unterstützung für das programmatische Management über RESTful-APIs. Mit Automation-Stitches lassen sich häufig ausgeführte Aktionen über eine grafische Benutzeroberfläche automatisieren – ohne Programmierkenntnisse oder große Erfahrung mit Cloud-Domains. Für flexiblere, leistungsfähigere Automatisierungsfunktionen bietet Fortinet zudem eine umfassende Dokumentation zu verfügbaren APIs.

Hochverfügbarkeit (HA): Fortinet-Lösungen können in verschiedenen HA-Modi eingesetzt werden. Jede Cloud unterstützt die Hochverfügbarkeit mit unterschiedlichen Funktionen. Wichtig ist, dass die zugrunde liegenden Security-Komponenten in jeder einzelnen Cloud-Umgebung eine konsequente, vorhersehbare Durchsetzung der Sicherheit gewährleisten. Hierzu müssen verschiedene Aktiv/Aktiv- oder Aktiv/Passiv-Strategien bereitgestellt werden, die nativ in jede Cloud integriert sind und die Verfügbarkeit geschäftskritischer Systeme unterstützen.

Auto-Skalierung: Zu den größten Vorteilen einer Cloud-Infrastruktur zählen ihre Elastizität und On-Demand-Funktionen. Unternehmen profitieren hiermit z. B. von einem Up- oder Down-Scaling von Diensten, damit nur für das gezahlt wird, was wirklich genutzt wird. Fortinet unterstützt eine native Integration mit den Auto-Skalierungsfähigkeiten der Cloud. Das bedeutet, dass sich die Security-Infrastruktur an die Skalierung der Cloud-Infrastruktur je nach Volumen und Bedarf anpassen lässt. Diese flexible Security stellt sicher, dass Anwendungen ständig geschützt sind.

Konfigurationsvorlagen: Mit Vorlagen lassen sich sowohl Fehler reduzieren als auch wichtige Prozesse wie die automatische Skalierung von Cloud-Implementierungen automatisieren. Die Konfigurationsvorlagen von Fortinet unterstützen eine Vielzahl von Frameworks, darunter AWS CloudFormation Templates (CFT), Azure Resource Manager (ARM), HashiCorp Terraform und Ansible. Security-Administratoren können so Lösungen schnell und korrekt über verschiedene Plattformen hinweg und abgestimmt auf unterschiedliche Cloud-Workload-Implementierungen bereitstellen. Konfigurationsvorlagen tragen auch dazu bei, das Risiko menschlicher Fehler zu verringern, schneller Security-Komponenten für neue Workloads hinzuzufügen und somit die sichere Bereitstellung neuer Workloads durch Security-Administratoren zu gewährleisten.

Dienst-Integration: Cloud-Plattformen stellen Software- und Hardware-Dienste bereit, die die Nutzung verschiedener Funktionen vereinfachen. Damit entfällt die Notwendigkeit, dass Anwender den Umgang mit neu eingeführten Technologien erst lernen müssen. Entscheidend ist, dass sich Sicherheitslösungen in jede Cloud-Plattform integrieren lassen und Security-Funktionen als Teil des nativen Security-Nutzungsmodells angeboten werden. Eine solche Integration erweitert diesen grundlegenden Schutz für eine größere Zahl von Anwendungsfällen und Diensten. Abgedeckt werden auch Test-Environments und Umgebungen, die noch nicht Teil einer weiter gefassten Routine im Security-Management-Lifecycle sind.

2. Umfassender Schutz

Fortinet bietet das breiteste, umfassendste Security-Portfolio der Branche. Dazu gehören Lösungen für die Netzwerk- und Anwendungssicherheit der Enterprise-Klasse sowie Secure-Access-Produkte für den sicheren Netzwerk-Zugang. Das Besondere an den Lösungen und Produkten von Fortinet ist, dass sie Informationen austauschen und in einer kooperativen Sicherheitsstruktur zusammenwirken: der Fortinet Security Fabric. Diese kombiniert ein intuitives Betriebssystem, eine mehrstufige Bedrohungserkennung und angewandte Threat Intelligence, um Sicherheit, Transparenz und Kontrolle zu gewährleisten.

Abbildung 3: Die drei Säulen der Multi-Cloud-Security

Security-Teams erhalten eine integrierte Transparenz, um die Angriffsfläche zu verringern und zu kontrollieren. Auch lassen sich Sicherheitsverletzungen mit künstlicher Intelligenz (KI) verhindern und die Komplexität durch automatisierte Abläufe und Orchestrierung reduzieren. Im Folgenden wird genauer erläutert, wie der umfassende Fortinet-Schutz für die Cloud funktioniert:

Schutz vor Zero-Day-Bedrohungen: Fast täglich werden neue, bisher unbekannte Zero-Day-Bedrohungen gefunden, die sowohl die Cloud- als auch auf On-Premises-Implementierungen gefährden. Da Angreifer zunehmend Technologien wie künstliche Intelligenz (KI) und maschinelles Lernen (ML) verwenden, wird die Anzahl der Zero-Day-Bedrohungen wahrscheinlich steigen.

Fortinet bietet verschiedene Technologien zum Erkennen und Stoppen von Zero-Day-Bedrohungen. Dazu gehören z. B. Sandbox-Analysen, mit denen potenzielle Malware in einer simulierten Umgebung beobachtet wird. So wird geklärt, ob eine Datei sicher ausgeführt und mit Tools zur Verhaltensanalyse auf bösartige Absichten untersucht werden kann.

Sandbox-Analysen sind jedoch zeit- und ressourcenintensiv und können die Leistung ausbremsen, wenn ein Großteil des Datenverkehrs nicht vorgefiltert wird. Fortinet verwendet deshalb künstliche Intelligenz (KI) und maschinelles Lernen (ML) zur Bedrohungserkennung, um viele Threats schon vor der Sandbox abzufangen. Das Implementieren von Sandboxing-Technologien – ob in einer IaaS-VM oder SaaS-Anwendung – ist eine unentbehrliche Funktionalität, die Teil jeder Multi-Cloud-Security-Strategie sein sollte.

SSL und IPsec VPN: Die Erweiterung einer sicheren Konnektivität in die Cloud sowie zwischen Clouds ist ein wichtiges Element jedes Sicherheitskonzepts. Da Datenverkehr häufig über das Internet und Cloud-Umgebungen hinweg verläuft, ist die Traffic-Isolierung und die Vorgabe konsequenter Netzwerk-Security-Richtlinien für die gesamte Infrastruktur ein Schlüsselelement, um heterogene Cloud-Umgebungen zu vereinheitlichen. Die Unterstützung von IPsec-VPNs zwischen Standorten einerseits und VPNs über virtuelle Cloud-Netzwerke hinweg anderseits ist für eine konsequente Sicherung und Isolierung des Datenverkehrs unerlässlich. Auch müssen VPN-Implementierungen mit verschiedenen Cloud-VPN-Lösungen interoperabel sein und Flexibilität für unterschiedliche Unternehmen und Bereiche bieten. Weiter ist die Fähigkeit, sehr schnelle VPN-Verbindungen bereitzustellen, entscheidend. FortiGate VM wurde speziell dafür optimiert, eine sichere Konnektivität mit hohem Durchsatz bereitzustellen, ohne cloudbasierte Anwendungen zu verlangsamen.

Kontrolle über Anwendungen: Die Application Control mit FortiGuard-Diensten erhöht die Sicherheit für internetbasierte Anwendungen. Unternehmen erhalten hiermit eine Möglichkeit, schnell Richtlinien zu erstellen, um den Zugriff auf Anwendungen zuzulassen, zu verweigern oder einzuschränken. Dieser Dienst bietet Security-Teams Transparenz und Kontrolle über Tausende von Anwendungen und kann um benutzerdefinierte Apps erweitert werden. Auch lassen sich Sicherheitsrichtlinien pro Anwendungstyp feinabstimmen und Bandbreiten mit einem anwendungsgesteuerten Traffic-Management optimieren.

Sicheres SD-WAN: Fortinet hat den SD-WAN-Markt mit seiner erstklassigen Next-Generation-Firewall (NGFW), einer SD-WAN-Lösung, erweitertem Routing und Funktionen für die WAN-Optimierung neu definiert. Mit dem einheitlichen FortiGate-Angebot lassen sich sicherheitsorientierte Netzwerke für die WAN-Edge-Transformation erfolgreich realisieren. Eine sichere Cloud-Verbindung ist ebenfalls wichtig, um nahtlose Security-Abläufe zu unterstützen. Fortinet erfüllt all diese Anforderungen – und noch mehr: Im SD-WAN-Gruppentest der NSS Labs wird Fortinet als empfehlenswert bewertet und bietet mit Fortinet Secure SD-WAN von allen acht verglichenen Anbietern die niedrigsten Gesamtbetriebskosten (TCO) pro Mbit/s.[2]

Zero Trust: Wird ein Netzwerk so gestaltet, dass die Vertrauensstufe nur einmalig grundsätzlich vergeben wird, können sich Daten und Anwendungen innerhalb des Netzwerks einfacher bewegen. Der Nachteil ist jedoch, dass dies oft zu unentdeckten Sicherheitslücken führt und den Diebstahl kritischer Daten durch böswillige Insider ermöglicht. Vor solchen Szenarien schützt die FortiGate VM NGFW mit einer dynamischen Segmentierung. Dabei wird anhand logischer Attribute von Daten und Anwendungen über mehrere Standorte und die Cloud hinweg eine konsistente Isolierung von Ressourcen gewährleistet. Reine Annahmen über die Vertrauensstufe gehören der Vergangenheit an: Jede Verbindung – unabhängig vom VLAN oder Ursprungsnetzwerk – wird grundsätzlich überprüft.

NGFW: Da Unternehmen mehr geschäftskritische Anwendungen in der Cloud erstellen, besteht ein größerer Bedarf an verbesserten Security-Funktionen. Virtuelle FortiGate-Appliances für die Ingress- und Egress-Sicherheit bieten für die Cloud dieselbe Sicherheitsfunktionalität wie On-Premises. Zudem sind diese Lösungen tief in verschiedene Cloud-Plattformen integriert und für eine hohe Leistung in Cloud-Infrastrukturen optimiert.

Web Application Firewall (WAF): Mit dem zunehmenden Fortschritt digitaler Innovationen (DI) für geschäftskritische Software werden immer mehr Anwendungen als Web Applications bereitgestellt. Die FortiWeb WAF bietet eine Bot-Abwehr sowie einen Bedrohungsschutz für kritische Web-Anwendungen und APIs, der auf maschinellem Lernen (ML) basiert. So lassen sich Web-Security-Richtlinien feinabstimmen und Fehlalarme vermeiden. FortiWeb unterstützt Unternehmen dabei, die Anforderungen von Risiko-Management-Richtlinien und Vorschriften beim Schutz von Endanwender-Informationen zu erfüllen und einen kontinuierlichen Geschäftsbetrieb sicherzustellen.

E-Mail-Sicherheit: E-Mails sind nach wie vor der häufigste Angriffsvektor für Malware – besonders wenn Unternehmen ihre E-Mail-Systeme zunehmend in die Cloud verlagern und sich auf die Cloud als Backup-System verlassen. Bis Ende 2022 werden voraussichtlich 87 % aller geschäftlichen E-Mail-Konten über die Cloud bereitgestellt werden.[3] Die E-Mail-Security-Lösungen von Fortinet bieten einen Komplettschutz vor E-Mail-Bedrohungen in der Cloud und On-Premises und eignen sich ideal zur Unterstützung der Cloud-Migration.

3. Management und Automatisierung

Die Vereinheitlichung der Security-Infrastruktur eines Unternehmens vereinfacht nicht nur das Management, sondern auch die konsequente Einhaltung von Sicherheitsrichtlinien – und das überall, wo Anwendungen ausgeführt, Daten gespeichert und Infrastrukturen angelegt werden. Auch können so Management-Prozesse für den Security-Lebenszyklus automatisiert und Compliance-Vorschriften besser erfüllt werden. Mit diesen Funktionen lassen sich unternehmensweit Cloud- und On-Premises-Infrastrukturen auf ähnliche Weise verwalten, da überall das gleiche Maß an Transparenz und Kontrolle gegeben ist. Ein zentrales Management und eine Automatisierung trägt entscheidend dazu bei, dass Unternehmen ihre Ziele für das Risiko-Management und die Compliance erreichen.

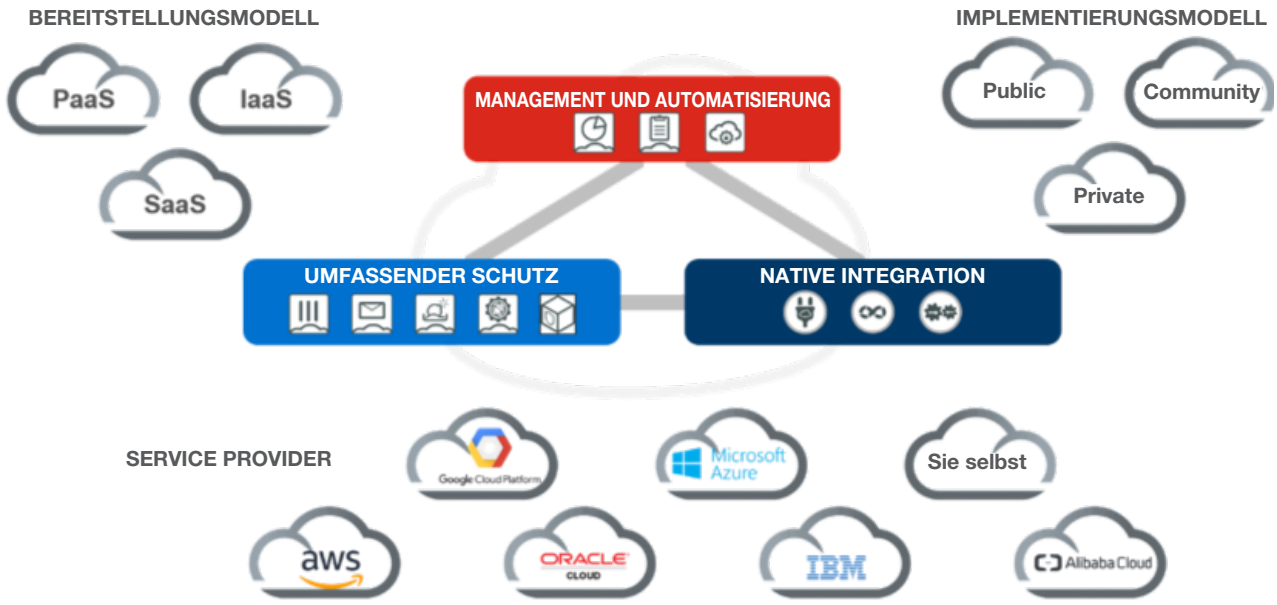

Abbildung 4: Eine umfassende Lösung, die für verschiedene Bereitstellungsmodelle, Implementierungsmodelle und Service Provider funktioniert

Die effektive Verwaltung und Automatisierung von Security-Komponenten umfasst vier Grundelemente: Transparenz, Kontrolle, Richtlinien und Compliance. Fortinet erfüllt diese Anforderungen mit Management-Produkten wie FortiManager, FortiAnalyzer, FortiCASB und FortiCWP Cloud Workload Protection (CWP).

Transparenz: Die Möglichkeit, alle Anwendungen, Netzwerke, Infrastrukturen, Sicherheitsereignisse und Logs in einer Multi-Cloud-Umgebung einheitlich anzuzeigen, ist ein Grundpfeiler für die Bewertung des Sicherheitsprofils. Diese Beurteilung dient als

Ausgangspunkt und ist zugleich ein fortlaufender Prozess des Security-Managements. Unternehmen müssen in der Lage sein, über die Infrastruktur verteilte Ressourcen zu identifizieren und Datenströme zuzuordnen. Auch muss die Verwendung von Anwendungen nachvollziehbar sein und das Unternehmen muss wissen, welche Daten im Netzwerk übertragen werden. Der FortiAnalyzer bietet Inline-Transparenz über alle Fortinet-Systeme mit tiefgehenden Analyse-Funktionen, während FortiCWP mit cloudspezifischen APIs für Transparenz über den gesamten Public-Cloud-Stack sorgt.

Anhand dieser Informationen lässt sich überprüfen, ob die Security-Richtlinien effektiv greifen oder ob zusätzliche Richtlinien notwendig sind. In einer Multi-Cloud-Umgebung, in der Anwendungen über verschiedene Infrastrukturen hinweg kommunizieren, bietet eine zentrale Nachverfolgung des Datenverkehrs und der Abfolge von Ereignissen über jede Cloud-Umgebung hinweg oft einen besseren Einblick, als mit Standard-Security-Tools möglich wäre. Auch lassen sich Abläufe mit einer zentralen Konsole vereinfachen, die die Cloud-Infrastruktur transparent in die Security-Infrastruktur einbindet.

Kontrolle: Besitzt ein Unternehmen eine vollständige Security-Transparenz, ist der nächste Schritt die Kontrolle relevanter Funktionen. Hierzu müssen Konfigurationsänderungen durchgeführt und relevante ressourcenbezogene Informationen über das Multi-Cloud-Sicherheitsprofil in die Security-Infrastruktur eingebunden werden. Security-Management-Tools sollten dafür mit konsequenten Kontrollmechanismen sämtliche Security-Funktionen abdecken.

Dieser Kontrollrahmen muss auch die nativen Security-Funktionen der einzelnen Cloud-Plattformen einbeziehen. Administratoren können dann Sicherheitsmaßnahmen innerhalb der gesamten Infrastruktur ändern – unabhängig von der zugrunde liegenden Technologie. FortiManager unterstützt Administratoren dabei, einheitliche Richtlinien für alle Infrastrukturen anzuwenden.

Richtlinien: Mit der Transparenz und den Kontrollfunktionen der Fortinet Security Fabric erhalten Unternehmen ein einheitliches Security-Management und können Sicherheitsrichtlinien konsequent durchsetzen. Da Infrastruktur-Änderungen – bedingt durch den Lebenszyklus von Anwendungen – regelmäßig notwendig sind, verringert sich so der Arbeits- und Zeitaufwand, um die Folgen von Anwendungsänderungen für die Infrastruktur abzuschätzen. Stattdessen können IT-Security-Teams die Sicherheitseinstellungen an Ereignisse im Anwendungs-Lebenszyklus anpassen, um einheitlichere Security-Richtlinien umzusetzen.

FortiCWP hilft bei der Identifizierung von falsch konfigurierten Richtlinien und Compliance-Verstößen: Mit Bedrohungsinformationen und einer nativen Integration lassen sich Konfigurationen bewerten, Aktivitäten in Cloud-Konten sowie der Cloud-Netzwerkverkehr überwachen, Daten analysieren und scannen und auch Compliance-Berichte erstellen.

Mit einer zentralen Konsole zur Verwaltung sämtlicher Fortinet-Geräte unterstützt FortiManager das Management von Multi-Cloud-Richtlinien. Unternehmen erhalten damit optimierte Bereitstellungs- und Automatisierungs-Tools für vollständige Transparenz über das Netzwerk.

Security-Teams können mit diesen Funktionen ein strategisches Sicherheitsprofil realisieren, indem Richtlinien umgehend auf einer zentralisierten Plattform implementiert werden, um Updates schneller anzuwenden.

Compliance: Durch die Aufrechterhaltung eines einheitlichen Sicherheitsprofils und die Automatisierung von Sicherheitsabläufen lassen sich Compliance-Anforderungen besser erfüllen. Mit einem zentralisierten Security-Management, automatisierten Workflows und gemeinsam genutzten Bedrohungsdaten können Unternehmen schnell auf neue Gefahren reagieren und Risiken über die gesamte Angriffsfläche hinweg effektiver abwehren – ohne hochkomplexe Security-Abläufe. FortiCWP und FortiCASB identifizieren Konformitätsprobleme und liefern Berichte zum Compliance-Status, damit Unternehmen behördliche Vorgaben jederzeit erfüllen.

Security und Threat Research

In diesem Dokument werden die Hauptelemente der Implementierung effektiver Lösungen für eine konsequente Hybrid-Cloud-Security mit nativer Integration, umfassendem Schutz sowie Management und Automatisierung umrissen. Mit Technologie allein ist es jedoch nicht getan: Eine erstklassige Cloud-Sicherheitslösung muss auch Security-Intelligence-Dienste enthalten, die Daten zur Bedrohungserkennung für Geräte und Lösungen liefern. Diese Dienste sollten von qualifizierten Sicherheitsexperten überwacht werden – ausgestattet mit den richtigen Ressourcen, um der dynamischen Entwicklung der Cyber-Security Herr zu werden.

Mit Experten auf der ganzen Welt verfügen die FortiGuard Labs über eines der größten Security-Research- und Analysten-Teams der Branche. Diese engagierten Experten sind stets auf der Suche nach aktuellen Bedrohungen und neuen Techniken. Sie untersuchen alle kritischen Bereiche der Bedrohungslandschaft, einschließlich Malware, Botnetze, Sicherheitslücken bei Mobilgeräten und Zero-Day-Schwachstellen.

Darüber hinaus unterhält FortiGuard Labs ein integriertes Intelligence-Ecosystem mit über 200 Security-Intelligence-Partnerschaften und -Kollaborationen. Mit dieser Kombination aus einem branchenführenden Forschungs- und Analysten-Team und einem umfassenden Security-Intelligence-Ecosystem bietet Fortinet eine marktführende Bedrohungserkennung und Sicherheit, die ihresgleichen sucht: Unternehmen erhalten eine leistungsstarke Lösung, um neue Bedrohungen zu verhindern, zu erkennen und sofort „im Keim zu ersticken“.

Cloud-Security – Anwendungsfälle

Bei der Entwicklung einer Cloud-Security-Strategie sollten verschiedene Anwendungsfälle für die Umstellung auf die Cloud und die Sicherheit berücksichtigt werden, wobei die geeigneten Anwendungsfälle für verschiedene Cloud-Initiativen variieren. Viele Unternehmen verfolgen eine der folgenden drei Initiativen:

- Einbindung von SaaS-Anwendungen
- Entwicklung cloudnativer Anwendungen
- Migration oder Erweiterung von Anwendungen in die Cloud

Alle drei Initiativen erfordern unterschiedliche Security-Lösungen, um ein sehr gutes Sicherheitsprofil und ein leistungsstarkes Betriebsmodell aufrechtzuerhalten. Das Modell der geteilten Verantwortung bietet hierfür Orientierung mit der Konsequenz, dass die meisten Unternehmen die Transparenz und Kontrolle für die gesamten Cloud erweitern müssen – unabhängig von der Art der geplanten Cloud-Initiative.

Während das übergeordnete Ziel, die Transparenz, Kontrolle und den Schutz von Anwendungen in der Cloud zu verbessern, bei allen drei Initiativen von größter Bedeutung ist, unterscheiden sich die Anwendungsfälle und spezifischen Produkte, um jedes Ziel zu erreichen. Die drei von Fortinet angebotenen Lösungsfamilien für die Cloud-Security sind: (1) Transparenz und Kontrolle, (2) Anwendungssicherheit und (3) sichere Konnektivität. Im folgenden Abschnitt wird genauer auf die verschiedenen Anwendungsfälle eingegangen, die mit jeder Lösung verbunden sind.

Fortinet Cloud Security – Anwendungsfälle

1. Transparenz und Kontrolle

- SaaS-Transparenz und -Kontrolle
- Transparenz und Kontrolle über die Cloud-Infrastruktur
- Compliance für die Cloud
- Cloudbasiertes Security-Management und Analytics

2. Anwendungssicherheit

- Sicherheit von Web-Anwendungen
- Logische (absichtsbasierte) Segmentierung
- Container-Security
- Sicherstellen der Produktivität
- Schutz von Cloud-Workloads

3. Sichere Konnektivität

- Schutz für Hybrid Clouds
- Cloud Security Services Hub
- Sicherer Fernzugriff

1. Transparenz und Kontrolle

SaaS-Transparenz und -Kontrolle

Als flexible, skalierbare und kostengünstige Möglichkeit zur Bereitstellung geschäftskritischer Anwendungen erfreut sich SaaS bei IT-Teams und Führungskräften großer Beliebtheit. Das Problem ist, dass der zunehmende Einsatz von SaaS oft weder reguliert noch gut gesichert erfolgt. Eine effektive Cloud-Security muss jedoch alle SaaS-Aktivitäten überwachen und sich in Sicherheitslösungen integrieren lassen, um konsequente Sicherheitsrichtlinien für herkömmliche und SaaS-basierte Anwendungen durchzusetzen.

Fortinet bietet eine zentralisierte Steuerung von SaaS-Anwendungen, damit Unternehmen allgemeine Best Practices für die Compliance und Governance bereitstellen können. Auch lassen sich so sensible Anwendungsdaten vor komplexen Bedrohungen schützen, Schatten-IT-Anwendungen kontrollieren und einheitliche Application-Control-Richtlinien an allen Standorten umsetzen. Das verbessert nicht nur die Sicherheit, sondern reduziert auch Latenzzeiten und erfüllt die Leistungserwartungen von Anwendern.

FortiCASB bietet eine zentrale, detaillierte Übersicht über die Verwendung aller SaaS-Anwendungen. So können Unternehmen einheitliche Richtlinien für die Application Control und Security implementieren, vertrauliche Daten vor komplexen Bedrohungen schützen und die Einhaltung von Sicherheits-, Compliance- und Governance-Vorgaben fördern.

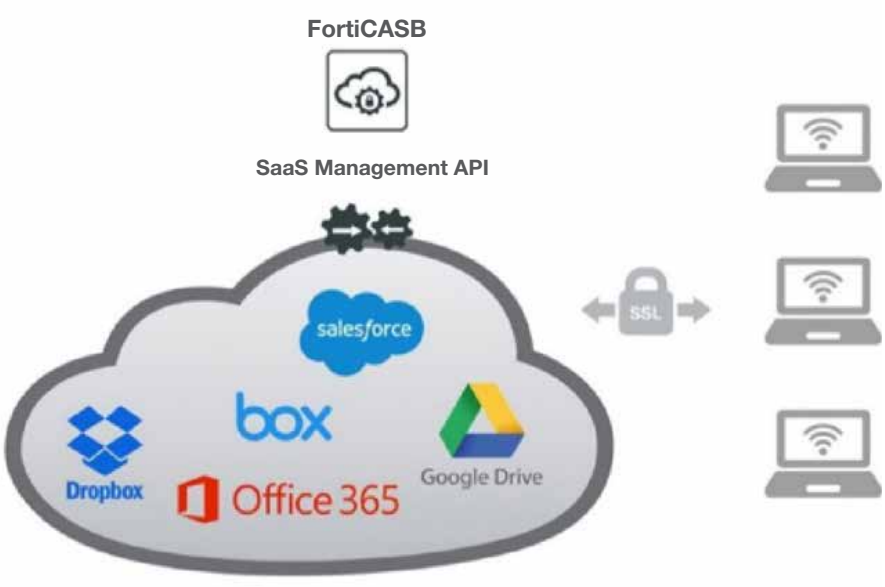

Abbildung 5: Public Cloud Security – Anwendungsfälle

Transparenz und Kontrolle über Ihre Cloud-Infrastruktur

Mit zunehmender Cloud-Nutzung steigt auch die Wahrscheinlichkeit von Fehlkonfigurationen. Da die Nutzung von Public Clouds nicht immer überwacht wird, können Sicherheitslücken leicht übersehen werden.

FortiCWP nutzt die Public-Cloud-Management-API zur Überwachung der Aktivität und Konfiguration mehrerer Cloud-Ressourcen. Konfigurationen aller Regionen und Public-Cloud-Typen werden kontinuierlich bewertet, was eine einheitliche Transparenz gewährleistet. FortiCWP vereinfacht auch die Meldung von Verstößen gegen gesetzliche Compliance-Bestimmungen und verbessert die Regelkonformität mit Empfehlungen für bewährte Security Best Practices.
Weiter gibt es Tools für die Bedrohungsabwehr und das Risiko-Management, mit denen sich Fehlkonfigurationen einfacher bis zu ihrer Quelle zurückverfolgen lassen. FortiCWP unterstützt AWS, Google Cloud Infrastructure und Microsoft Azure.

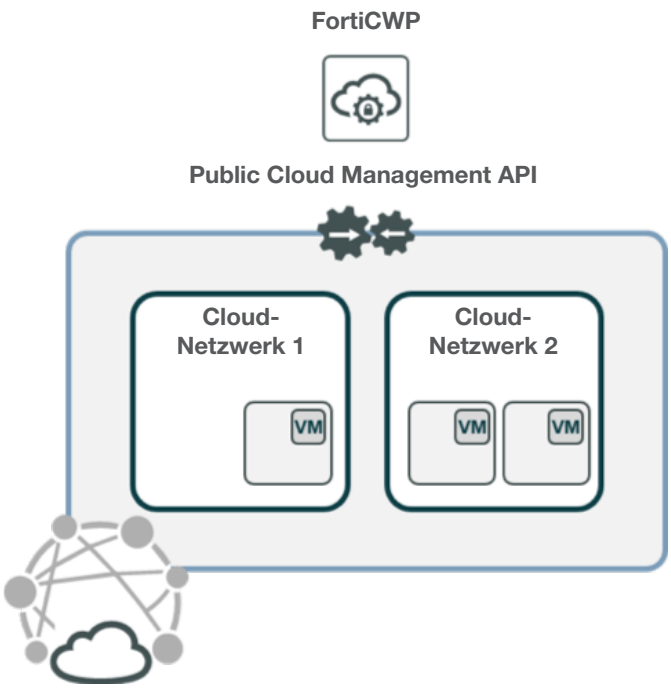

Abbildung 6: FortiCWP verwendet native APIs für die Public Cloud, um die Sicherheitsaktivität und -konfiguration cloudübergreifend zu überwachen.

Compliance für die Cloud

Das Einhalten von PCI DSS, HIPAA, SOX, GDPR und anderen behördlichen Auflagen kann eine zeitaufwändige Belastung sein, die durch die Migration in eine oder mehrere Clouds noch erhöht wird. Mit diesen Fortinet-Lösungen lässt sich die Cloud-Compliance sicherstellen:

FortiCWP aggregiert Sicherheitsinformationen aus mehreren Cloud-Diensten und APIs und stellt diese in aussagekräftigen Berichten zur Regelkonformität und in Live-Compliance-Dashboards bereit.

FortiSIEM bietet einen umfassenderen Überblick über die Compliance – übergreifend über mehrere Clouds, Fortinet Security Fabric-Produkte und Produkte von Drittanbietern. Compliance-Berichte lassen sich mit nur einem Klick erstellen.

FortiAnalyzer sammelt Logs von Fortinet Security Fabric-Elementen, während der FortiManager für Audits, Überprüfungen, Genehmigungen und Implementierungen von Änderungen dient. Gemeinsam schließen sie Compliance-Lücken zur Schadensminderung. Alle Systeme unterstützen automatisierte Prozesse, um das Management und den Workflow von Compliance-Richtlinien zu vereinfachen und das Risiko bei Richtlinien-Änderungen zu senken.

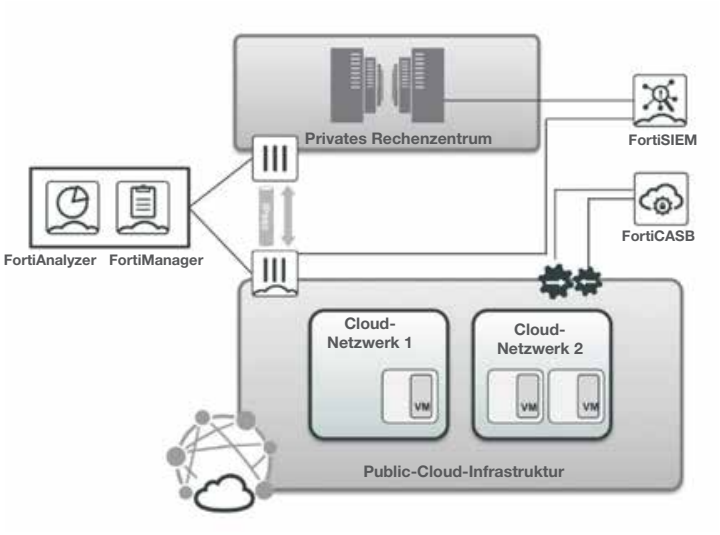

Abbildung 7: Fortinet-Lösungen für die Cloud-Compliance

Cloudbasiertes Security-Management und Analytics

Die gemeinsame Verwendung älterer Management-Tools und neuer Technologien führt zu komplexen Inkompatibilitäten, insbesondere bei der Verwaltung über die Cloud.

Um diese Herausforderungen zu meistern, können Unternehmen von der internationalen Präsenz führender Cloud-Infrastrukturanbieter profitieren und das Security-Management sowie Analytics-Systeme weltweit zentral über die Cloud bereitstellen. Werden FortiManager-VM, FortiAnalyzer-VM und FortiSIEM-VM in die Cloud implementiert, erhalten Unternehmen Möglichkeiten zur Skalierung und Globalisierung mit entscheidenden Vorteilen:

- zentrales, einheitliches Security-Management und Transparenz
- erweitertes Audit- und Compliance-Reporting
- schnellere Reaktion auf Vorfälle – Stichwort „Incident Response“
- bessere Betriebs- und Kosteneffizienz zur Verringerung des Risikos
- einfachere Automatisierung des Security-Managements

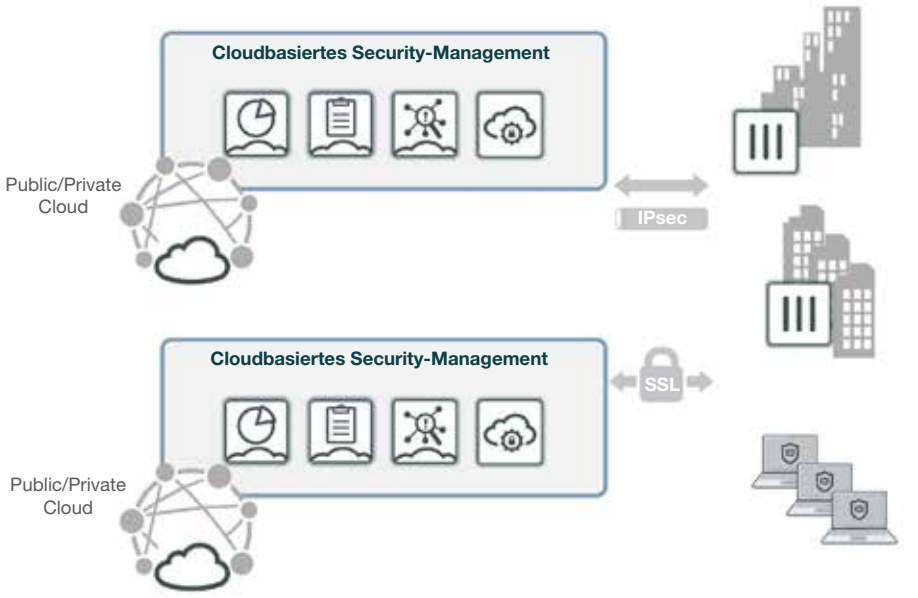

Abbildung 8: Fortinet-Lösungen für cloudbasiertes Security-Management und Analytics

2. Anwendungssicherheit

Sicherheit von Web-Anwendungen

Cloudbasierte Anwendungen verwenden häufig Web Services für die interne und externe Kommunikation, was Anwendungen anfällig für verschiedene Bedrohungen macht. Dazu kommen zusätzliche Compliance-Anforderungen für Web-Anwendungen, deren Erfüllung oft eine zusätzliche Belastung darstellt.

Fortinet bietet eine Vielzahl von Lösungen für die Web Application Security, die ideal für Kunden mit cloudbasierten Netzwerken sind. FortiWeb VM ist eine marktführende WAF, die auf allen großen Cloud-Plattformen läuft und Web Services APIs und Front-End-Webanwendungen gleichermaßen schützt. Integriert mit FortiWeb können FortiGate-VMs Sicherheitsrichtlinien zentral durchsetzen und für mehr Transparenz sorgen. Zudem bietet der Fortinet Sandbox-Dienst eine dynamische Analyse, um bislang unbekannte Malware zu identifizieren.

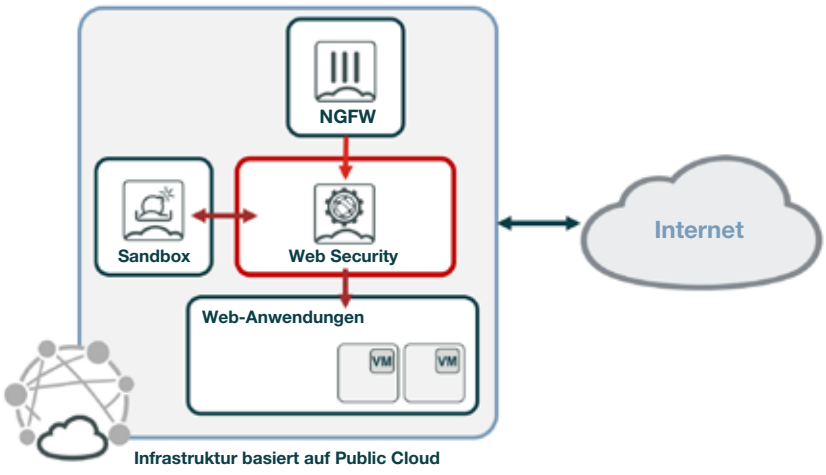

Abbildung 9: Fortinet schützt Anwendungen vor bekannten und unbekannten Bedrohungen.

Logische (absichtsbasierte) Segmentierung

Die Segmentierung von Cloud-Umgebungen ist alles andere als einfach, da bei einer dynamischen Bereitstellung ständig die IP-Adressen wechseln. Eine Netzwerk-Segmentierung anhand statischer IP-Adressen kann folglich nicht funktionieren.

FortiGate-VMs bieten eine absichtsbasierte Segmentierung, bei der Zugriffsregeln und Segmente auf Grundlage der Benutzeridentität oder Geschäftslogik erstellt werden. Diese Regeln werden dynamisch angepasst, wofür ihre Vertrauenswürdigkeit kontinuierlich neu bewertet wird. FortiGate-VMs nutzen Metadaten oder Tags, die cloudbasierten Ressourcen in mehreren Clouds zugeordnet sind und zur Durchsetzung von Sicherheitsrichtlinien dienen. So wird intuitiv definiert, welche Workloads und Elemente in der Cloud mit anderen Workloads und Elementen kommunizieren dürfen – unabhängig davon, ob sich diese innerhalb oder außerhalb der Cloud befinden.

Container-Security

Container sind mittlerweile aus dem Cloud Computing nicht mehr wegzudenken. Ihre Beliebtheit verdanken sie vor allem der Möglichkeit, dass sich damit eine Anwendung samt aller abhängigen Elemente als Paket zusammenfassen und einfach zwischen Computer-Umgebungen verschieben lässt. Container isolieren die Software vom Betriebssystem und der zugrunde liegenden Hardware und stellen so sicher, dass eine Anwendung überall reibungslos funktioniert.

Die Container-Security schützt nicht nur die zugrunde liegenden Container, sondern auch die Container-Pipeline, die Infrastruktur, auf der ein Container ausgeführt wird, sowie die Befehle und Datenebenen, die die Container unterstützen.

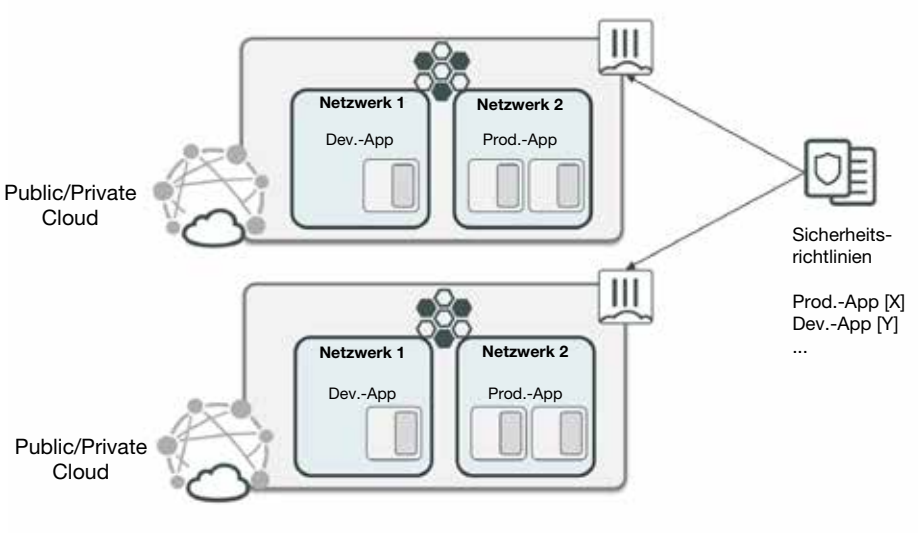

Abbildung 10: Logische Segmentierung

Die Container-Security-Lösung von Fortinet umfasst vier sich ergänzende Schutzbereiche: Der Fabric Connector bietet eine Container-aware Security zur Erkennung von Container-Labels bei der Definition von Sicherheitsrichtlinien, mit einer FortiGate lässt sich der Nord-Süd-Verkehr in und aus Containern effektiv schützen und FortiGate NGFWs bieten Fabric Connectors für weit verbreitete Container-Orchestrierungssysteme – wie native Kubernetes, AWS EKS, GCP GKE, Azure AKS und OCI OKE –, um Metadaten für Sicherheitsrichtlinien-Objekte zu nutzen.

FortiWeb kann als Container-Image in die Anwendungskette eingebunden werden. Dank dieser containerintegrierten Security lassen sich Fortinet-Lösungen dynamisch in Kubernetes-Cluster integrieren und in die Anwendungskette einfügen. So sind auch containerbasierte Apps durch die Web Application Security abgedeckt.

FortiSandbox bietet Sicherheit für die Container-Registry und überprüft vorkonfigurierte Container-Images auf bösartigen Code und Zero-Day-Bedrohungen. FortiNAC sorgt dafür, dass nur Benutzer mit den richtigen Rollen und Berechtigungen auf eine Anwendung und deren Container zugreifen können.

Sicherstellen der Produktivität

Das IT-Management von Produktivitäts- und E-Mail-Anwendungen wird zunehmend ausgelagert, wodurch Unternehmen an Transparenz und Kontrolle über diese Anwendungen einbüßen. Security-Teams müssen jedoch auch in Multi-Cloud-Umgebungen eine einheitliche, sinnvolle Sicherheit durchsetzen können.

Gemeinsam bieten FortiMail, FortiSandbox und FortiCASB-SaaS wichtige Schutzfunktionen für geschäftliche Produktivitätsanwendungen wie Microsoft Office 365. Mit der Security Fabric erhalten Unternehmen eine tiefgehende Transparenz über den Datenverkehr von Anwendungen, während Zero-Day-Angriffe und komplexe persistente Bedrohungen von Fortinet Security-Diensten und der Sandbox-Technologie erkannt und blockiert werden.

Schutz von Cloud-Workloads

In die Cloud integrierte oder migrierte Anwendungen müssen vor herkömmlichen und neuen Internet-Bedrohungen geschützt werden, die sich über Workloads verbreiten und über API-Schnittstellen ins Unternehmen gelangen können.

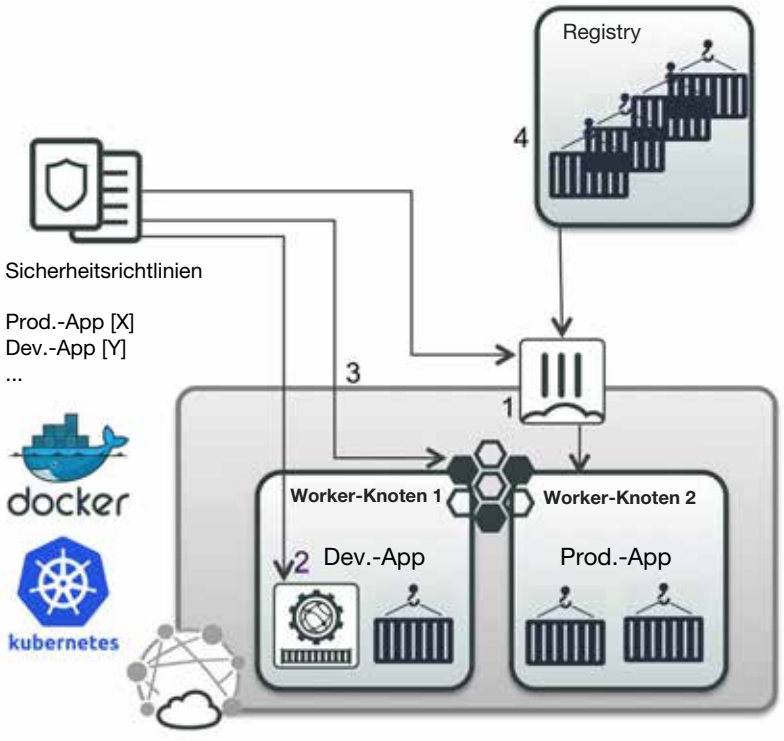

Abbildung 11: Container-Security

Durch die Kombination aus einem Inline-Schutz für den Nord-Süd-Datenverkehr, einem hostbasierten Schutz für den Ost-West-Datenverkehr und einem Schutz für Cloud-API- und Konfigurationsrisiken erhalten Unternehmen eine engmaschige Sicherheitslösung für die Cloud: Eine FortiGate-VM schützt virtuelle Cloud-Netzwerke vor Bedrohungen aus dem Internet und gewährleistet sichere Verbindungen zwischen Clouds. Durch die Installation von FortiClient auf VMs können Unternehmen die Security innerhalb der Cloud erweitern und die Compliance und Connectivity sicherstellen. Unerwünschte oder unkontrollierte Konfigurationen von Cloud-Konten lassen sich zudem mit FortiCASB-Cloud verhindern.

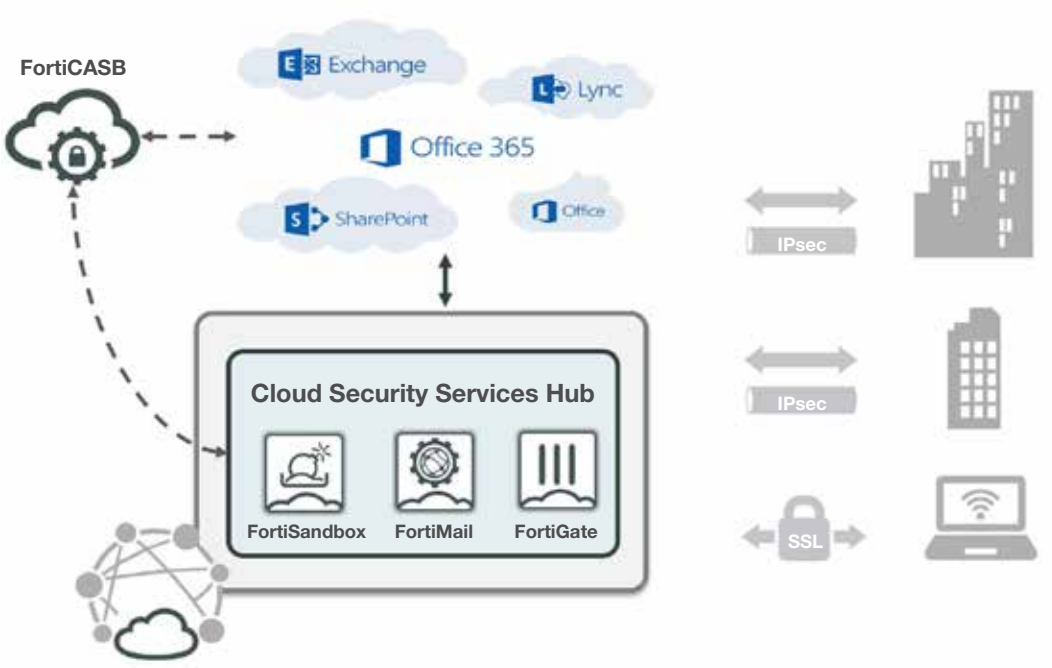

Abbildung 12: Fortinet stellt die Produktivität in der Cloud sicher.

3. Sichere Konnektivität

Schutz für Hybrid Clouds

Viele Unternehmen nutzen neben On-Premises-Rechenzentren auch Public Clouds als Teil der IT-Infrastruktur. Oft werden neue Anwendungen nur in der Public Cloud implementiert, manchmal aber auch parallel über Public und Private Clouds bereitgestellt.

Es ist wichtig, dass eine Lösung sowohl Public- als auch Private-Cloud-Technologien unterstützt. Zudem muss sie schnelle, leistungsstarke Security-Funktionen bieten, die hochvolumige Datenübertragungen bewältigen können. Ebenso wichtig ist die konsequente Verwaltung der Richtlinien. Dies verringert den Migrationsaufwand beim Infrastrukturwechsel und somit die Gefahr menschlicher Fehler, die die Sicherheit gefährden können. Auch müssen die Security-Komponenten die gesamte Angriffsfläche abdecken und skalierbar sein, um eine Anpassung an kontinuierliche Änderungen zu ermöglichen.

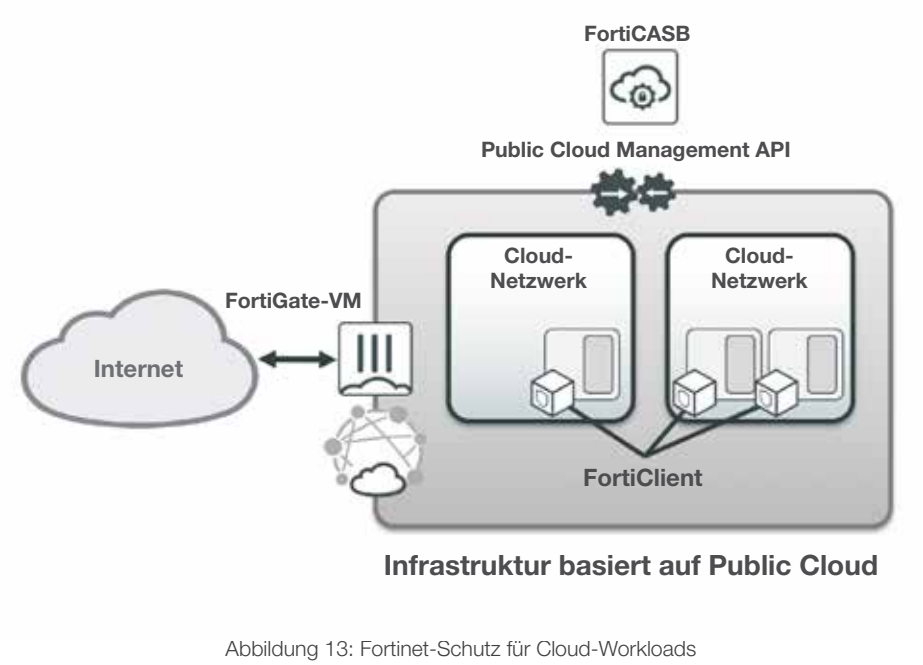

Abbildung 13: Fortinet-Schutz für Cloud-Workloads

FortiGate NGFWs und Cloud-Security-Lösungen bieten eine erstklassige sichere Konnektivität, Netzwerk-Segmentierung und Anwendungssicherheit für hybride cloudbasierte Implementierungen. Unternehmen erhalten damit eine zentralisierte, konsequente Durchsetzung von Sicherheitsrichtlinien und können Verbindungen über ultraschnelle VPN-Tunnel herstellen. Zudem können in der Public Cloud bereitgestellte FortiGate-VMs sicher mit FortiGate NGFWs kommunizieren und die gleichen Sicherheitsrichtlinien verwenden – unabhängig vom Formfaktor der NGFW im privaten Rechenzentrum.

Cloud Security Services Hub

Bei der Anwendungsentwicklung in separaten virtuellen Netzwerken und Clouds gibt es kein zentralisiertes Security-Management. Fertige Anwendungen und separate Umgebungen lassen sich daher nur schwer absichern.

Security-Teams, die unterschiedliche Umgebungen vereinheitlichen wollen, brauchen einen zentralen Hub für Sicherheitsdienste oder ein Transit-Netzwerk. Durch den Hub werden die Security und Anwendungsentwicklung voneinander getrennt. Das gewährleistet eine zentralisierte, gemeinsame und konsequente Durchsetzung der Sicherheitsmaßnahmen. Auch werden Netzwerke, Standorte, Clouds und Rechenzentren sicher miteinander verbunden. Zudem wird der ein- und ausgehende Traffic zwischen Clouds und dem Internet analysiert und unterliegt ebenfalls der Durchsetzung von Sicherheitsrichtlinien.

Sicherer Fernzugriff

Unternehmen benötigen einen globalen, bedarfsgerechten und sicheren Zugriff auf Cloud-Ressourcen, der eine intelligente Zugangskontrolle, das Nachverfolgen von Ereignissen sowie Analysen ermöglicht. Herkömmliche Remote Access VPNs können diese Anforderungen jedoch nicht erfüllen.

Security-Teams brauchen Konfigurationsvorlagen für eine sichere Remote-Access-Terminierung. Dann können sie dynamisch FortiGate-VM-Instanzen bereitstellen, die mit diesen Vorlagen einheitlich vorkonfiguriert wurden. Unternehmen können so sichere Verbindungen für mobile Mitarbeiter, Homeoffices, Kunden und Geschäftspartner zum virtuellen Unternehmensnetzwerk bereitstellen. Ein weiterer Vorteil ist, dass das Cloud-Netzwerk über VPN-Tunnel mit Geschäftsanwendungen verbunden wird – unabhängig davon, ob diese in der Cloud oder On-Premises implementiert sind.

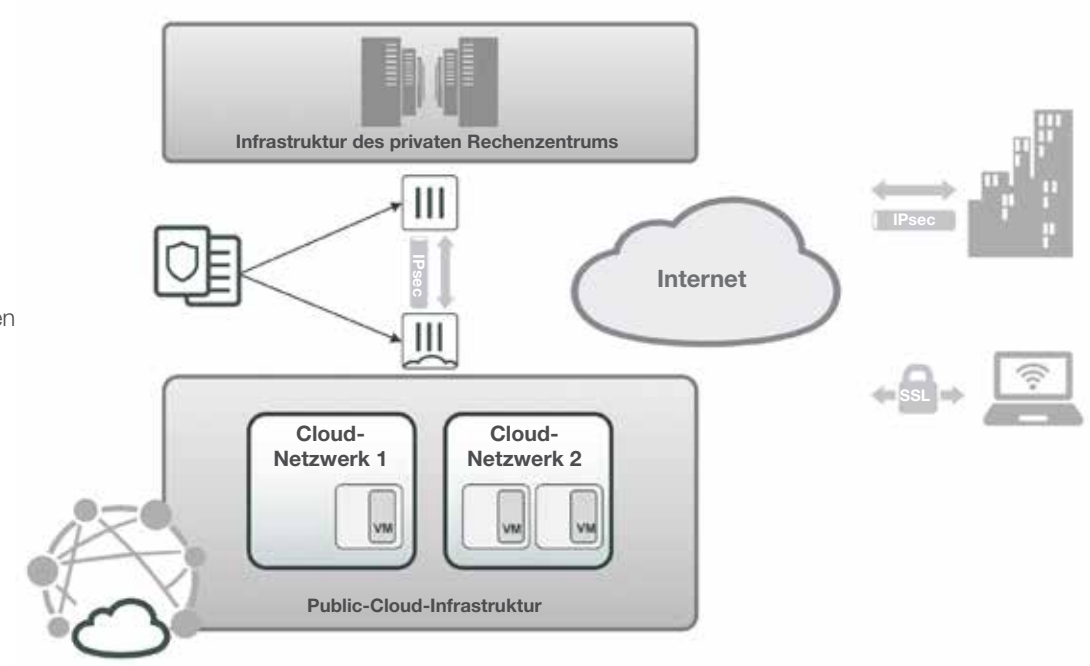

Abbildung 14: Schutz für Hybrid Clouds

Fazit

Die Cloud bietet Unternehmen immense Geschäftsmöglichkeiten. Ohne die richtige Security-Infrastruktur und ein geeignetes Framework für die betrieblichen Abläufe entstehen durch die Cloud-Einführung jedoch ernste Sicherheitsprobleme, die weitreichende Konsequenzen haben können. Durch den Einsatz von Cloud-Plattformen werden nicht nur geschäftskritische Anwendungen und Daten über mehrere Clouds hinweg verteilt, sondern oft auch dezentral schnell Cloud-Dienste eingeführt. Um diese Anwendungen, Daten und Dienste zu schützen, implementieren viele Unternehmen eine Fülle unterschiedlichster Security-Tools und -Richtlinien, die aber nur in isolierten Bereichen und unabhängig voneinander verwaltet werden können.

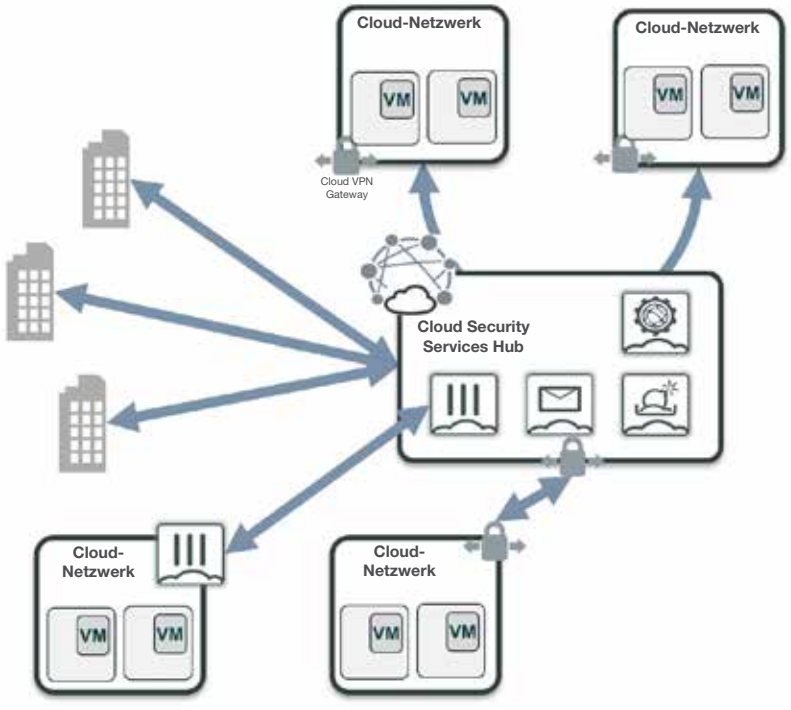

Abbildung 15: Fortinet fungiert als Steuerzentrale für Clouds und Rechenzentren.

Das Modell der gemeinsamen Verantwortung für die Cloud-Sicherheit gibt vor, dass Cloud-Anbieter nur die Infrastruktur schützen, nicht aber in der Cloud bereitgestellte, ausgeführten Anwendungen oder in der Cloud gespeicherte Daten. Vielmehr sind die Kunden für den Schutz der Anwendungsebene verantwortlich. Da jeder Cloud-Anbieter unterschiedliche Tools und Security-Ansätze verwendet, sind Unternehmen mit einer besonders komplexen Situation konfrontiert und müssen unterschiedliche Security-Komponenten verschiedener Anbieter miteinander verbinden, damit ihre Anwendungen sicher geschützt sind.

Zum Schutz von Multi-Cloud-Umgebungen sollten Unternehmen drei Prinzipien befolgen:

- native Integration mit allen wichtigen Cloud-Anbietern
- Einsatz einer breiten Palette von Security-Tools, die die gesamte Angriffsfläche abdeckt
- Verwendung eines zentralen Security-Managements, einschließlich Automatisierung von Workflows und Austausch von Bedrohungsdaten

Aufgrund der Heterogenität von Cloud-Implementierungen gibt es viele zu berücksichtigende Anwendungsfälle. Jeder dieser Anwendungsfälle stellt besondere Anforderungen an die Sicherheit, wie etwa die Integration aller Security-Elemente über die gesamte Angriffsfläche hinweg, eine sich über mehrere Clouds erstreckende Security-Automatisierung, cloudspezifische Security-Frameworks mit zentralisiertem Richtlinien-Management zur Erfüllung der Compliance-Anforderungen, eine Sicherheitslösung, die den vollständigen Anwendungslebenszyklus abdeckt, ein Cloud Service Hub für die Bereitstellung von Security-Diensten und viele weitere Funktionen.

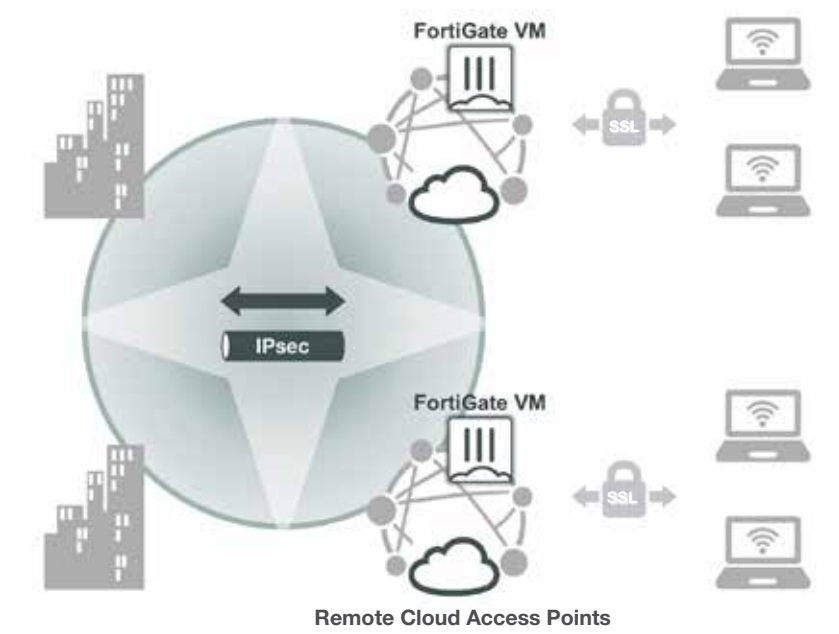

Abbildung 16: Fortinet fungiert als Steuerzentrale für Clouds und Rechenzentren.

[1] „Q3 2017 Threat Landscape Report“. Fortinet, 17. November 2017.

[2] „FortiGate: Secure SD-WAN“. Fortinet 2019.

[3] „Cloud Business Email Market, 2018-2022“. The Radicati Group, Inc., Juni 2018.

5. Mai 2020, 13:47 Uhr

471739-0-1-DE