FORTINET SECURITY FABRIC ERWEITERT SICHERHEITSFUNKTIONEN FÜR MICROSOFT AZURE

ZUSAMMENFASSUNG

Microsoft Azure ist eine Cloud-Plattform, die verbesserte Compliance und Sicherheit bietet und zudem eine einfache Migration in eine hybride Cloud sowie bessere Koexistenz ermöglicht. Microsoft Azure unterstützt eine Vielzahl von Sicherheitslösungen und -technologien, um die Informationen in Azure und vor Ort zu schützen. Darüber hinaus bietet Azure Organisationen, die sich an die Nutzung von Microsoft Enterprise Services gewöhnt haben und nun über Office 365 in die Cloud wechseln, besondere Vorteile. Azure und Office 365 stellen jedoch keine umfassenden Sicherheitsfunktionen zum Schutz der Daten in der Cloud bereit. Organisationen brauchen zusätzlich tiefgehende Transparenz und engmaschige Kontrolle über Anwendungen und Informationen über die Infrastruktur der Public Cloud und vor Ort. Die Fortinet Security Fabric für Azure erlaubt es Unternehmen, einheitliche Sicherheitsrichtlinien über ihre Multi-Cloud-Infrastruktur zu nutzen, um Transparenz und Kontrolle sowie den Schutz vor komplexen cloudbasierten Angriffen zu verbessern.

SCHUTZ FÜR EINE REIHE VON AZURE PUBLIC CLOUD-ANWENDUNGSFÄLLEN

Die Fortinet Security Fabric für Azure erweitert konsistenten, branchenführenden Schutz nun auch auf Microsoft Azure-basierte Cloud-Umgebungen. Die Security Fabric schützt die Rechenlasten über lokale Rechenzentren und Cloud-Umgebungen hinweg – dies umfasst auch mehrstufige Sicherheit für cloudbasierte Anwendungen. Die Security Fabric unterstützt eine Vielzahl gängiger Anwendungsfällen in Unternehmens-Clouds:

1. **Hybride Cloud.** Unternehmen benötigen eine nahtlose Security-Orchestrierung, die entsprechend den Cloud Workloads skaliert. Die Fortinet Security Fabric umfasst Next-Generation Firewalls (NGFWs), welche die integrierten Azure-Sicherheitsfunktionen ergänzen und gleichzeitig eine gesicherte und verschlüsselte Konnektivität zwischen allen denkbaren Varianten an Cloud-Infrastruktur unterstützen. Sie können entweder über eine Public Cloud oder On-Premise in einem eigenen Rechenzentrum verwaltet werden.
2. **Advanced Threat Prevention.** Ein zunehmender Anteil moderner Geschäftsanwendungen wird über Public Cloud-Infrastrukturen eingesetzt. Gleichzeitig sind Web- und E-Mail-Anwendungen für die meisten Datenschutzverletzungen pro Muster verantwortlich. Die Fortinet Security Fabric für Azure umfasst Lösungen, die diese geschäftskritischen Anwendungen vor bekannten und Zero-Day-Angriffen schützen, indem sie Lösungen wie FortiWeb, FortiMail und FortiSandbox nutzen. Dies verringert den Druck, ständige Patches auf Servern einzuspielen. Außerdem wird damit die Compliance mit gesetzlichen Anforderungen und Sicherheitsstandards, wie dem Payment Card Industry Data Security Standard (PCI DSS) und dem Health Insurance Portability and Accountability Act (HIPAA), unterstützt. FortiSandbox kann zudem Collaboration-Websites vor den Risiken durch Advance Persisten Threats schützen, die durch den Upload bösartiger Dateien entstehen.
3. **Secure Access VPN.** Die Fortinet Security Fabric bietet erstklassige Leistungen beim Schutz von VPN-Datenverkehr für ein Remote Access VPN in Azure. Durch die Nutzung der multiregionalen Infrastruktur von Azure können Unternehmen ihre Dienste sofort weltweit skalieren und eine Remote Access VPN-Terminierung in der Nähe des Endbenutzers anbieten. Ein Remote Access VPN kann genutzt werden, um den Zugriff auf cloudbasierte sowie lokale Anwendungen zu ermöglichen, die über andere Formen von Private Links oder VPN mit der Cloud verbunden sind.
4. **Cloud Services Hub (vNET).** Die Konnektivität von Cloud-Anbietern ist weitaus leistungsfähiger als die der typischen mittelständischen Unternehmen. Ein Azure-basiertes virtuelles Netzwerk (vNET) ermöglicht es Organisationen, Sicherheitsdienste für mehrere Netzwerke weltweit gemeinsam zu verwenden. Durch die umfassende Einbindung der Fortinet-Lösungen – einschließlich Netzwerktransparenz, VPN-Konnektivität, Next-Generation Firewall (NGFW), erweiterte Web Application Firewall, Sandboxing und Mail-Sicherheit – bietet die Security Fabric weitaus mehr Dienste und nutzt gleichzeitig die Elastizität und sofortige Skalierbarkeit der Cloud für ein optimales Preis-Leistungs-Verhältnis.
5. **Sicherheit für Office 365.** Da Office 365 oft mit Azure Cloud zusammen eingesetzt wird, und neben der Tatsache, dass die meisten Angriffe per E-Mail ins Unternehmen gelangen, ist der Schutzbedarft von Office 365-basierten E-Mail- und Geschäftsanwendungen weiterhin ausgesprochen wichtig. Die Kombination von FortiMail, FortiSandbox und FortiCASB bietet die entscheidenden Fähigkeiten zum Schutz von Office 365. Insbesondere ermöglicht die Security Fabric eine tiefgehende Transparenz von E-Mails zum Schutz vor Zero-Day-Attacken und die Überwachung der Office 365-API-Ebene.

WIE DIE SECURITY FABRIC DIE AZURE-SICHERHEIT ERGÄNZT

Die Security Fabric bietet tiefgehende, mehrschichtige Sicherheit und operative Vorteile für den Schutz von Anwendungen innerhalb von Azure und für die Verwaltung globaler Security-Infrastrukturen aus der Cloud. Zu den wichtigsten Funktionen der Security Fabric für Azure gehören:

Kontrolle und Verwaltung über eine zentrale Konsole: Mit der Security Fabric können sowohl Cloud- als auch On-Premise Sicherheitsfunktionen von Azure aus zentral verwaltet werden. So werden menschliche Fehler vermieden und der Zeitaufwand verringert.

Cloud-native Transparenz und Kontrolle: Unternehmen erhalten mit der Security Fabric umfassende Transparenz über ihre bereitgestellten Azure-Anwendungen. Sie müssen keine spezifischen Bereitstellungskonfigurationen mehr planen, sondern kommen näher zu absichtsbasierten Richtlinien. Durch die Verwendung dynamischer Adressgruppen und die logische Benennung von cloudbasiert Ressourcen können Sicherheitsrichtlinien erweitert werden, da Security Fabric-Ressourcen über die gesamte Cloud-Infrastruktur hinweg skaliert werden.

Schatten-IT: Da Organisationen ihren IT-Betrieb rationalisieren und die Security Controls konsolidieren nutzen viele Geschäftsbereiche nun ihre eigenen cloudbasierten Dienste. Die Security Fabric bietet IT-Abteilungen einen besseren Überblick über die Nutzung von Azure-Infrastrukturen und die Möglichkeit, eine strengere Kontrolle über die Nutzungsmuster zu implementieren, um das Unternehmen vor Risiken zu schützen.

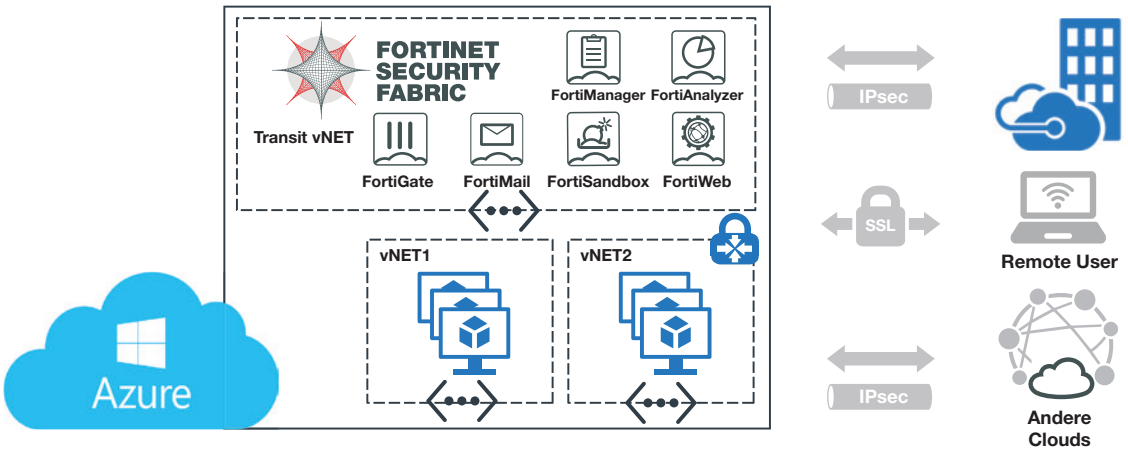

ABBILDUNG 1: DIE FORTINET SECURITY FABRIC FÜR MICROSOFT AZURE

Schutz vor Zero-Day-Angriffen: Die Lösungen der Fortinet Security Fabric bieten einen hochgradig skalierbaren Schutz von Zero-Day-Attacken, der vollständig in die Cloud-Infrastruktur integriert ist. Sie tragen dazu bei, das Risiko durch komplexe Bedrohungen zu verringern und das Vertrauen in die Bereitstellung von Anwendungen jeder Größenordnung in der Cloud zu erhöhen.

Compliance-tauglich: Die Security Fabric-Lösungen bieten Best-in-class-Schutz und unterstützen Unternehmen bei der Einhaltung aktueller Branchenstandards wie PCI DSS und der neuesten Datenschutzgesetze wie der Datenschutzgrundverordnung (DSGVO) der EU.

INTEGRIERTE VERTEIDIGUNGSMASSNAHMEN, DIE DAS GESAMTE ANGRIFFSSPEKTRUM ABDECKEN

Die verschiedenen Lösungen der Fortinet Security Fabric für Azure wurden entwickelt, um das Vertrauen der Endanwender in Azure Cloud-Umgebungen zu stärken. Alle diese Lösungen basieren auf den Formfaktoren der Fortinet Virtual Machine (VM). Lizenzen, die von einem Fortinet Channel-Partner für VMs erworben wurden, sind plattformübergreifend übertragbar, sodass beispielsweise dieselbe VM-Lizenz für FortiGate VM auf VMware auch für die FortiGate für Azure-Plattform funktioniert, wenn das Modell **Bring Your Own License (BYOL)** zur flexiblen Einbindung eigener Lizenzen verwendet wird. Außerdem können FortiGate, FortiMail und FortiWeb über das **Pay-As-You-Go-(PAYG-)Modell** direkt über den Azure Marketplace genutzt werden.

Die folgenden Lösungen sind Teil der Fortinet Security Fabric für Azure:

- **FortiGate VM NGFW** bietet den branchenweit besten Schutz vor den komplexesten bekannten und unbekannten Cyber-Angriffen. FortiGate VM skaliert nach oben und unten entsprechend den Kundenanforderungen und wird in verschiedenen Größen angeboten, sodass es in einer Vielzahl von unterstützten Anwendungsfällen einsetzbar ist.
- Die **FortiMail** E-Mail Security Gateways nutzen die neuesten Technologien und Dienste der FortiGuard Labs, um einen durchgängigen erstklassigen Schutz vor bekannten und komplexen Bedrohungen zu gewährleisten und gleichzeitig robuste Datenschutzfunktionen zu integrieren, um Datenverluste zu vermeiden.
- **Die FortiSandbox** bietet eine leistungsstarke Kombination aus innovativer Erkennung, automatisierter Abwehr, umsetzbaren Erkenntnissen und flexibler Implementierung, um gezielte Angriffe und nachfolgende Datenverluste zu stoppen.
- **Die FortiWeb** Web Application Firewalls (WAFs) schützen gehostete Web-Anwendungen vor Angriffen, die auf bekannte und unbekannte Exploits abzielen. FortiWeb verwendet mehrschichtige und korrelierte Erkennungsmethoden, um Anwendungen vor bekannten Schwachstellen und Zero-Day-Attacken zu schützen.
- **Der FortiManager** stellt zentrales Management und Richtlinienkontrollen über die Extended Enterprise hinweg bereit, die Einblicke in die netzwerkweiten, datenverkehrs-basierten Bedrohungen liefern. Der FortiManager umfasst Funktionen zum Eindämmen komplexer Bedrohungen und bietet Skalierbarkeit für die Verwaltung von bis zu 10 000 Fortinet-Geräten.
- **Der FortiAnalyzer** erfasst, analysiert und korreliert Daten von Fortinet-Produkten und liefert so erhöhte Transparenz und verlässliche Informationen bei Sicherheitswarnungen. Wird der FortiAnalyzer mit einem Subscription des FortiGuard Indicators of Compromise-(IOCs-) Diensts kombiniert, wird auch eine priorisierte Liste kompromittierter Hosts geliefert, sodass schnelle Maßnahmen möglich sind.
- **FortiCASB** bietet einen cloud-native Cloud Access Security Broker-(CASB-)Subscription Service, der Transparenz, Compliance und Datensicherheit unterstützt und über umfassende Reporting-Tools Einblicke in Benutzer, Verhalten und die in der Cloud gespeicherten Daten bietet.
- **Fabric Connectors** ermöglichen eine offene Integration der Fortinet Security Fabric zur Automatisierung der Integration von Firewall und Netzwerksicherheit in dynamische Netzwerkabläufe mit mehreren vorhandenen Komponenten innerhalb des Ökosystems eines Kunden.

MEHRSCHICHTIGER SCHUTZ REDUZIERT DAS RISIKO

Fortinet überwindet die Barrieren, die die Transparenz und -verwaltung auf Private, Public und Hybrid Cloud-Plattformen behindern. Mit Fortinet können Sicherheitsexperten sicherstellen, dass ihre Security-Netzwerke die gesamte Angriffsfläche abdecken.

Die Fortinet Security Fabric für Azure hilft Organisationen, mit einem Modell gemeinsamer Verantwortung durchgängigen Schutz bereitzustellen, On-Premise ebenso wie in der Cloud. Sie bietet umfassende mehrschichtige Security und Threat Prevention für Azure-Anwender. Gleichzeitig werden Betrieb, Policy Management und Transparenz für ein verbessertes Security Life-Cycle-Management optimiert.

März 15, 2019 11:15 vorm.

279230-0-1-DE

Solution-Brief-Azure_DE