FORTINET

# Schutz von Clouds mit Fortinet

## 5 Schlüsselbereiche, in denen Architekten cloudnative Security-Tools erweitern müssen

# Inhaltsverzeichnis



FORTINET

# Zusammenfassung

Die Umstellung auf die Cloud wird in vielen Unternehmen vom DevOps-Team vorangetrieben, ohne jedoch alle Konsequenzen zu bedenken, die diese Umstellung für die Sicherheit mit sich bringt. Übernimmt das Unternehmen einfach die Security-Funktionen der Cloud-Plattform, sind Sicherheitslücken vorprogrammiert, über die Angreifer Daten stehlen oder in andere Bereiche des Unternehmensnetzwerks vordringen können. Beim Einrichten und Verwalten der Cloud-Sicherheit müssen Security-Architekten dafür sorgen, dass mindestens fünf Sicherheitsbereiche abgedeckt sind.

Mit Fortinet erhalten Unternehmen eine kritische Sicherheitsebene, die in die weiter gefasste Security-Architektur integriert ist. Dazu gehören Lösungen für das Security-Management von Cloud-Plattformen, die native Integration spezieller Sicherheitsfunktionen in die Cloud-Plattform, der Schutz von Web-Anwendungen und APIs (Application Programming Interface) sowie Integrationen, um Sicherheitsaufgaben in Cloud-Umgebungen zu automatisieren. All dies verbessert das Sicherheitsprofil des Unternehmens, da die Security vereinheitlicht wird und sich konsequent durchsetzen lässt. Unternehmen können so ein effektives Betriebsmodell für das Security-Life-Cycle-Management realisieren – ohne neue Cyber-Security-Experten einstellen zu müssen oder Zeit in die Schulung von DevOps-Teams für neue Tools zu investieren.

# Einleitung: Security-Tools von Cloud-Anbietern genügen nicht

Die stärksten Befürworter von Cloud-Lösungen sind DevOps-Teams. Aus gutem Grund: Das Cloud-Modell ist ideal für die kontinuierliche Integration und Bereitstellung – Stichwort „Continuous Integration und Delivery (CI/CD)“. In vielen Unternehmen verfügen diese Entwicklungsteams über weitreichende Benutzerrechte für Implementierungen in der Cloud-Infrastruktur, um je nach geschäftlichen Anforderungen Rechenleistung, Speicher, Netzwerk-Verbindungen und andere Ressourcen bereitzustellen. Das Problem: Die Entwickler sind zwar „an der Macht“, müssen sich aber nicht um die Konsequenzen kümmern. Denn für die Risiken, die Cloud-Neuerungen für das Unternehmen bedeuten, ist das Security-Team zuständig. Tatsächlich stand schon 2019 die DevOps-Sicherheit bei vielen Security-Architekten an erster Stelle.[1]

Zu diesen Hauptrisiken zählen vor allem Fehlkonfigurationen und daraus resultierende Sicherheitslücken, die Cyber-Bedrohungen ausnutzen können. Ein erfolgreicher Angriff auf eine cloudbasierte Umgebung kann Folgen für das gesamte Unternehmen haben – von Image-Schäden, Störungen der Betriebsabläufe und Ausfallzeiten bis hin zum Verlust wichtiger Geschäftsdaten.

**Cyber-Kriminelle verwenden mittlerweile fortschrittliche Technologien wie künstliche Intelligenz (KI) und Schwarmtechnologien – und auch DevOps-Tools:[2] Sie entwickeln Malware, die nur einmal für ein bestimmtes Unternehmen verwendet wird und die Angriffsfläche an mehreren Stellen attackiert.**

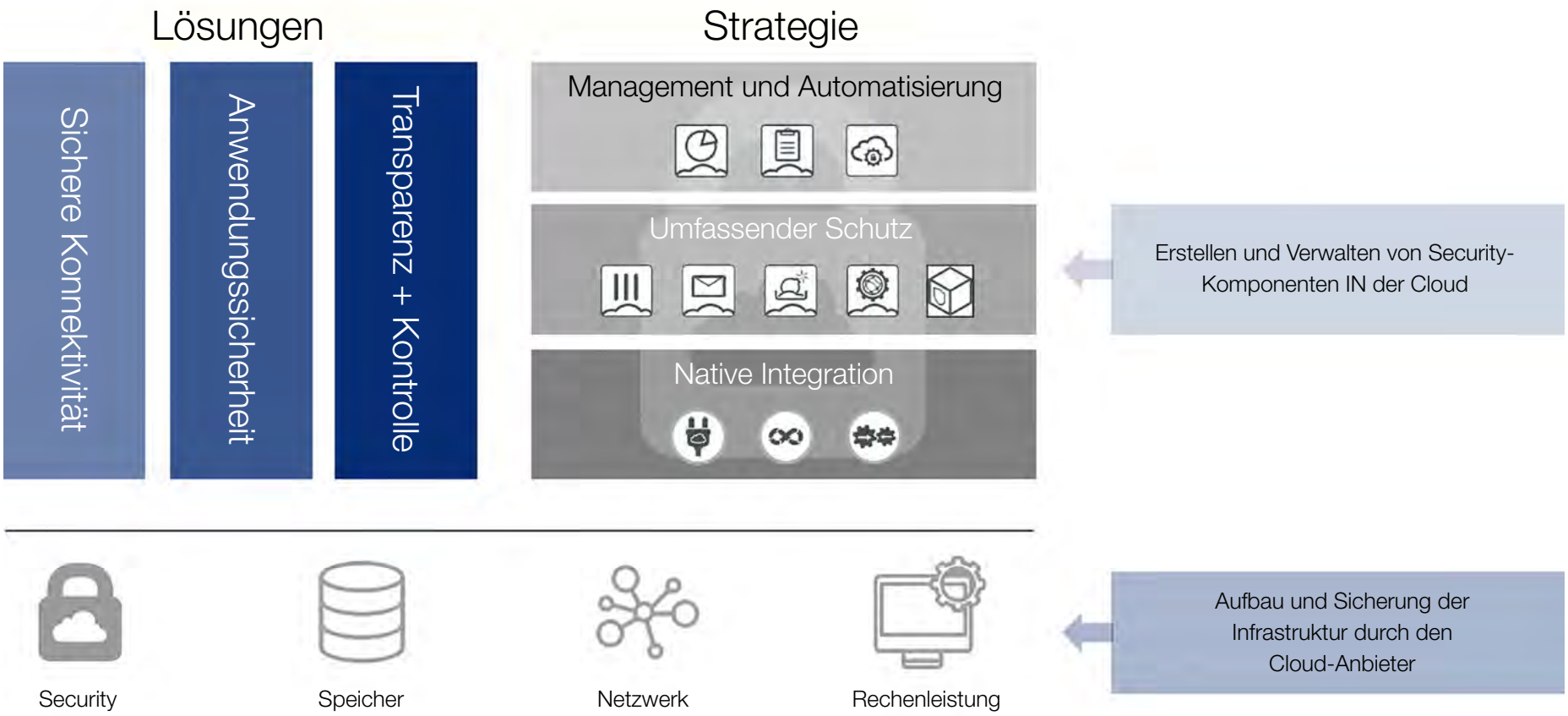


Abbildung 1: Cloud-Security-Lösungen müssen eine sichere Konnektivität, Anwendungssicherheit sowie hohe Transparenz und Kontrolle durch Management und Automatisierung, umfassenden Schutz und native Integrationsfunktionen bieten.

**Je komplexer die Konfiguration, desto höher das Sicherheitsrisiko**

DevOps-Verantwortliche können – fälschlicherweise – davon ausgehen, dass die Cloud-Security abgedeckt ist. Schließlich bieten die meisten Public-Cloud-Anbieter Security-Funktionen wie Sicherheitsgruppen oder Zugriffssteuerungslisten (Access Control Lists, ACLs), mit denen Cloud-Kunden die Zugriffsrechte für Dienste regeln können. Dazu kommen diverse cloudbasierte Tools von Drittanbietern wie verteilte Next-Generation-Firewalls (NGFWs), Web-Application-Firewalls (WAFs), Sandbox-Lösungen oder Management-Lösungen für das Cloud-Sicherheitsprofil und den Workload-Schutz. Die Fülle an Optionen kann überwältigend sein, weshalb vielbeschäftigte DevOps-Teams oft einfach die grundlegenden Security-Tools einer Cloud-Umgebung verwenden und weitere Schwachstellen mit isolierten Einzellösungen schließen.

Für Security-Architekten, die die DevOps-Sicherheitsrisiken minimieren sollen, ist dies aus mehrerlei Gründen problematisch. Selbst rudimentäre Cloud-Tools haben umfangreiche Konfigurationsoptionen und DevOps-Teams fehlt womöglich das Fachwissen, um jeden verfügbaren Sicherheitsdienst korrekt zu konfigurieren. Daher werden oft einfach die Standardkonfigurationen des integrierten Security-Tools übernommen – was das Unternehmen aber einem erhöhten Risiko aussetzt.

Um unerfahrenen Anwendern bei der Cloud-Security zu helfen und ein effektives Sicherheitsprofil zu gewährleisten, entwickeln DevOps-Teams häufig „goldene Regeln“ für die Konfiguration in Form von Vorlagen, die auch vorkonfigurierte Konfigurationsdienste umfassen. Leider sind Konfigurationsvorlagen anfällig für Programmierfehler und nicht immer auf dem neuesten Stand. Das Risiko, dass Fehler auftreten, steigt zudem, je häufiger eine Vorlage verwendet wird. Es überrascht daher kaum, dass Datenpannen aufgrund von Cloud-Fehlkonfigurationen innerhalb eines Jahres um 424 % zunehmen können und bereits im Jahr 2018 ganze 70 % aller Cloud-Datenschutzverletzungen ausmachten.[3]

**70 % der Cloud-Datenpannen gehen auf Fehlkonfigurationen zurück – eine Zahl, die im Jahresvergleich um 424 % gestiegen ist.[4]**

# Die Lösung: Eine zusätzliche, einheitliche Sicherheitsebene

Um das Risiko von Sicherheitslücken in der Cloud zu minimieren – und ohne Security-Teams zusätzlich zu belasten –, können Security-Architekten den robusteren Schutz der Fortinet-Cloud-Security-Lösungen in die weiter gefasste, zentral verwaltete Sicherheitsarchitektur des Unternehmens integrieren. Die dynamischen Cloud-Security-Lösungen von Fortinet decken vier Kernbereiche der Bedrohungsabwehr ab. Diese sind für alle Unternehmen unerlässlich, die vom Wettbewerbsvorteil einer DevOps-Agilität und Kundenorientierung profitieren möchten, ohne das geistige Eigentum oder die Compliance zu gefährden.

### 1. Sicherheit der Cloud-Plattform

DevOps-Umgebungen in der Cloud ändern sich schnell. Nimmt ein Cloud-Anbieter grundlegende Änderungen vor, muss das Unternehmen sich anpassen. Dies geschieht oft unkoordiniert und nur vereinzelt. Security-Architekten müssen daher DevOps-Teams und dem CISO eine zentralisierte Transparenz sowie ein Kontrollsystem bereitstellen, das den Konfigurationsstatus und das Sicherheitsprofil der gesamten Cloud-Infrastruktur überwacht.

Eigens für den Schutz von Cloud-Workloads bietet Fortinet **FortiCWP** an (Cloud Workload Protection). Security- und DevOps-Teams können hiermit das Sicherheitsprofil ihrer Cloud-Umgebungen kontinuierlich überwachen. Mit FortiCWP lassen sich potenzielle Bedrohungen erkennen, die sich aus einer Fehlkonfiguration der Sicherheitseinstellungen ergeben, verdächtige Aktivitäten in der Cloud-Infrastruktur identifizieren, Datenverkehr in und aus Cloud-Ressourcen analysieren und in der Cloud gespeicherte Daten auf schädliche oder sensible Inhalte untersuchen.

**DevOps-Manager benötigen zentrale Transparenz und eine automatisierte Überwachung des Konfigurationsstatus und des Sicherheitsprofils der Cloud-Infrastruktur.**

**FortiCWP** führt kontinuierliche Konfigurationsbewertungen durch, erstellt einen Risiko-Score und bietet Best-Practice-Empfehlungen zu dessen Verbesserung an. Anschließend werden die Konfigurationen weiterhin konsequent überwacht, um sicherzustellen, dass Probleme rechtzeitig erkannt und gelöst werden. Auch gibt es Analyse-Tools, mit denen Security-Architekten leichter DevOps-Managern erklären können, wie sich der Lebenszyklus von Konfigurationsänderungen auf Multi-Cloud-Umgebungen auswirkt.

### 2. Native Integration von FortiGate-Firewalls in die Cloud-Plattform

Für den Schutz von Betriebsabläufen in der Cloud muss die Security-Architektur so gestaltet werden, dass sie einen transparenten Überblick über das gesamte Unternehmen bietet. Security-Architekten können dies mit einer Kombination aus virtuellen und physischen Sicherheitslösungen realisieren: mit der Implementierung von FortiGate VMs in virtualisierten Umgebungen (Public und Private Cloud) und FortiGate-Appliances in Unternehmensstandorten.

Wie alle Komponenten der Fortinet Security Fabric verwenden auch virtuelle und physische FortiGate-Firewalls eine logische Informationsklassifizierung anhand von Tags und Metadaten-Annotationen. So können Security-Teams ein einheitliches Betriebsmodell und Sicherheitsprofil für die dynamische Multi-Cloud-Infrastruktur gewährleisten. Die Bedrohungsabwehr erfolgt dadurch innerhalb der gesamten Infrastruktur schnell und oftmals automatisch – unabhängig von der Verfügbarkeit von Mitarbeitern.

Um mit den dynamischen Zeitplänen einer wettbewerbsfähigen Geschäftsumgebung Schritt zu halten, lassen sich Fortinets Cloud-Security-Lösungen in eine Vielzahl von Cloud-Diensten nativ integrieren, z. B. für automatische Skalierungen, eine leistungsstarke, schnelle Vernetzung, Cloud-Hochverfügbarkeits-Schemata (HA), Cloud-Konfigurationsvorlagen und vieles mehr. Diese nativen Integrationen machen die Cloud-Security anpassungsfähiger an die Dynamik der Cloud-Infrastruktur.

**Security-Architekten müssen einen erweiterten Bedrohungsschutz aufrechterhalten – trotz begrenzter Sicherheitskompetenz bei Mitarbeitern. Die native Integration zwischen der FortiGate und der Cloud-Infrastruktur verringert diese Belastung.**

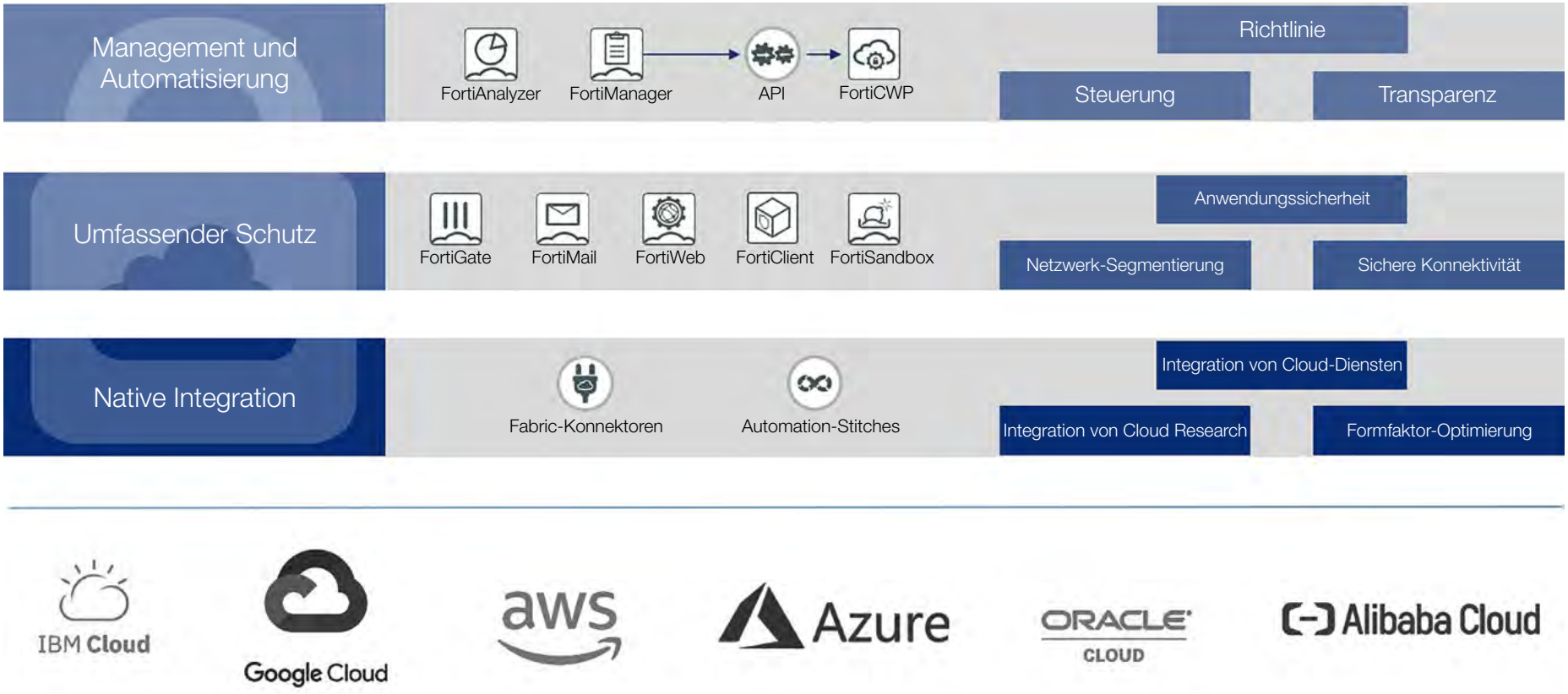


Abbildung 2: Fortinet bietet eine umfassende Cloud-Security-Strategie und maßgeschneiderte, integrierte Lösungen für Management, Automatisierung, umfassenden Schutz und native Integration.

### 3. Schutz von Web-Anwendungen und APIs

Viele Unternehmen können ihre Cloud-Umgebungen nicht angemessen sichern, weil sie das Modell der gemeinsamen Verantwortung nicht verstehen. Cloud-Anbieter sind für den Schutz ihrer Infrastruktur verantwortlich – einschließlich der Hardware- und Software-Komponenten, die ihren Client-Diensten zugrunde liegen – und leisten im Allgemeinen gute Arbeit bei der Sicherheit dieser Systeme. Der Schutz der in der Cloud gehosteten oder bereitgestellten Daten und Anwendungen liegt jedoch in der Verantwortung des Kunden. In den kommenden Jahren dürften sich die Folgen dieses Missverständnisses noch verschlimmern: Bis 2023 werden 99 % der Cloud-Probleme darauf zurückgehen, dass Kunden ihren Teil des gemeinsamen Sicherheitsmodells nicht erfüllen.[5]

Im Gegensatz zu On-Premises-Anwendungen, die sich durch Zugriffsbeschränkungen für bestimmte IP-Adressen schützen lassen, kann Anwendungsverkehr über das Internet (und der gesamte cloudbasierte Traffic läuft darüber) nicht mit einem solchen „Türsteher“ kontrolliert werden. In der Cloud muss die Bedrohungserkennung nicht am Port während der Datenübertragung erfolgen, sondern an den Inhalt von Anwendungen und den Kontext des Datenverkehrs geknüpft sein.

Um diesen tieferen Einblick zu ermöglichen, müssen die Sicherheitsrichtlinien für Web-Anwendungen ständig exakt angepasst werden. Manuell lässt sich das kaum effizient bewerkstelligen – erst recht nicht in großem Maßstab. Security-Architekten müssen daher auf einen Ansatz zurückgreifen, der mit künstlicher Intelligenz (KI) arbeitet, wie z. B. **FortiWeb**. Zusätzlich zu typischen WAF-Techniken wie dem Abgleich von Signaturmustern verwendet FortiWeb zwei Engines für maschinelles Lernen (ML), um Web-Anwendungen vor Zero-Day-Bedrohungen zu schützen. Dank dieser ML-gestützten Funktionen kann die Lösung Anomalien im Benutzer- oder Anwendungsverhalten erkennen und bietet einen wesentlich skalierbareren, präziseren Schutz vor neuen Botnetzen.

FortiWeb schützt Web-Anwendungen auch effektiv vor allen OWASP Top 10 Threats sowie vor bekannten und unbekannten Angriffen, die Schwachstellen für Exploits, Bots und Malware ausnutzen.

Da alles mit dem Internet verbunden wird – von Anwendungen über Middleware bis hin zu Backends für mobile Apps –, legen Unternehmen zunehmend Wert auf einen Bedrohungsschutz auf Web-Ebene. Welche Art von Security implementiert wird, variiert jedoch: Einige benötigen eine VM, um die Sicherheit für mehrere Anwendungen zu gewährleisten, während andere sich für ein Container-Konzept entscheiden, bei dem an jede Anwendung ein Web AppSec Container für die Application-Security als Microservice angehängt wird. Andere Unternehmen bevorzugen eine SaaS-Lösung (Software-as-a-Service), um sämtliche Sicherheitsanforderungen für Web-Anwendungen abzudecken, ohne die zugrunde liegende Infrastruktur verwalten zu müssen. In diesem Fall genießen Security-Architekten Flexibilität bei der Implementierung, da FortiWeb in verschiedenen Formfaktoren erhältlich ist und alle genannten betrieblichen Anforderungen ausnahmslos erfüllen kann.

### 4. Automatisierung von Security-Funktionen

Obwohl DevOps eine IT-Funktion ist, zeigen Studien, dass es bei der Sicherheit erhebliche Qualifikationsdefizite gibt. Beispielsweise sind nur 42 % der Entwickler mit sicheren Programmiertechniken vertraut und 57 % der Operations-Teammitglieder ignorieren Security-Best-Practices.[6] Um den Mangel an Sicherheitskenntnissen in DevOps-Teams auszugleichen – und ohne extra Security-Administratoren für den DevOps-Bereich einzustellen –, sollten Security-Architekten nach Möglichkeiten suchen, um DevOps-Teams bei einer umfassenden Automatisierung von Sicherheitsfunktionen zu unterstützen.

**In der Cloud muss sich der Schwerpunkt der Bedrohungserkennung vom Netzwerk-Kontext auf den Anwendungs-Kontext verlagern.**

Die Fortinet Security Fabric erleichtert diese Automatisierung mit Plugins (den sogenannten **Fabric-Konnektoren**), die Transparenz über Cloud-Objekte bieten. DevOps- und Security-Teams können so leichter mit Anwendungsänderungen Schritt halten, ohne dass bei jeder Änderung der Anwendungsattribute die Sicherheitsrichtlinien aktualisiert werden müssen.

Zusätzlich zu Fabric-Konnektoren können Security-Teams Sicherheitsabläufe über APIs für das FortiOS-Betriebssystem automatisieren oder auch FortiOS-Konfigurationsskripte über Automation-Frameworks wie Terraform und Ansible herunterladen.

Terraform gehört zu den beliebtesten Plattformen für die Automatisierung des IT-Lebenszyklus. Mit neuen FortiOS-Provider-Modulen für Terraform umfasst die Terraform-Automatisierung jetzt alle FortiOS-bezogenen Abläufe auf physischen und virtuellen FortiGate-Geräten. Entwickler können dadurch FortiGate-Terraform-Konfigurationen gemeinsam mit anderen Anwendungselementen integrieren, um schnell portierbare, sichere Application Stacks bereitzustellen.

Red Hat Ansible automatisiert die Konfiguration der FortiGate VM. Da Ansible-Module für FortiOS auf GitHub verfügbar sind, profitieren Entwickler von ihren Ansible-Kenntnissen und können FortiGate-Konfigurationsaufgaben komplett in der Ansible-Tower-Umgebung erledigen – und Unternehmen bei Entwicklerschulungen viel Geld sparen.

Eine weitere Automatisierungsressource für Entwickler ist das Fortinet Developer Network (FNDN) mit Dokumentationen und Tutorials, die genau erklären, wie sich mit FortiOS RESTful-APIs Fortinet-Funktionen direkt automatisieren lassen.

# 70 %

**der Unternehmen programmieren und verwalten Code mit einem automatisierten Ansatz.[7] FortiOS wurde von Grund auf für die Automatisierung entwickelt.**

# Fazit: Die Erweiterung cloudnativer Tools mit Fortinet-Lösungen ist notwendig und realisierbar

Security-Standard-Tools von Public-Cloud-Diensten genügen nicht, um eine dynamische Multi-Cloud-Umgebung zu schützen. Fehlkonfigurationen sind unvermeidlich und die daraus resultierenden Sicherheitslücken können das gesamte Unternehmen schädigen. Auch wenn diese Risiken in der Anfangsphase der Software-Entwicklung noch nicht offensichtlich und folgenschwer sein mögen, sollten Security-Architekten diesen Punkt frühzeitig angehen, um spätere Sicherheitsprobleme zu vermeiden.

Durch die Erweiterung der cloudnativen Sicherheit mit Fortinet-Lösungen können Security-Architekten Sicherheitslücken in der Cloud schließen und gleichzeitig die Belastungen durch das Security-Management verringern. Das breite Spektrum intelligenter Sicherheitstechnologien, nahtlos integrierter Funktionen und KI-gesteuerter Funktionen der Fortinet Security Fabric ergänzt und stärkt die Sicherheitsstrategie jedes Unternehmens.

[1] „The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 29. Juni 2019.

[2] „2019 State of DevOps Security Report“. Fortinet, 10. Mai 2019.

[3] Phil Muncaster: „Breached Records Fall 25% as Cloud Misconfigurations Soar“. Infosecurity, 6. April 2018.

[4] Ebd.

[5] „Key Principles and Strategies for Securing the Enterprise Cloud“. Fortinet, 3. Dezember 2018.

[6] Daniel Newman: „5 Reasons DevOps And Security Need To Work Together“. Forbes, 30. September 2018.

[7] Ian Barker: „Most organizations are not fully embracing DevOps“. BetaNews, 14. Juni 2018.

www.fortinet.com/de



430753-0-0-DE

26. Juni 2020, 15:48 Uhr