Forcepoint Next Generation Firewall mit Amazon Web Services

Die sicherste und effizienteste Enterprise-Firewall – zentral verwaltet, immer aktiv und kompromisslos

Herausforderung

- Unternehmen und Organisationen müssen dasselbe Sicherheitsniveau in Cloud- und Hybrid-Umgebungen einhalten wie in den traditionellen lokalen Infrastrukturen.
- Es kann teuer und technisch herausfordernd sein, eine sichere Cloud- oder Hybrid-Infrastruktur zu erstellen und zu warten.
- Die Einhaltung gesetzlicher Vorschriften kann schwierig und zeitaufwendig sein.

Lösung

- Die softwarebasierten Lösungen von Forcepoint Next Generation Firewall (NGFW) wurden dafür konzipiert, maximale Sicherheit mit minimalen Kosten und minimaler Komplexität bereitzustellen.
- Forcepoint NGFW Security Management Center (SMC) ist eine einheitliche Plattform, die Prozesse optimiert und Transparenz und Kontrolle bietet.
- Mit Forcepoint NGFW SMC können IT-Administratoren ihre Initiativen zur Vorschrifteneinhaltung in virtuellen und physischen Netzwerken optimieren und erhalten einfachen Zugriff auf Prüfberichte.

Ergebnis

- Maximale Cloud- und Hybrid-Sicherheit mit minimaler Komplexität
- Schnellere Reaktion auf Vorfälle
- Vereinfachte Einhaltung gesetzlicher Vorschriften, Umsetzung und Verwaltung
- Geringere Kosten für Netzwerk-infrastruktur und -sicherheit

Forcepoint Next Generation Firewall (NGFW) verbindet und schützt Mitarbeiter und die verwendeten Daten im gesamten Cloud- oder Hybrid-Netzwerk des Unternehmens mit der größten Effizienz, Verfügbarkeit und Sicherheit. Die Netzwerksicherheitslösungen von Forcepoint werden von Tausenden von Kunden weltweit geschätzt und stehen über den AWS Marketplace zur Verfügung. Sie ermöglichen es Unternehmen und Organisationen, kritische Probleme effizient und ökonomisch anzugehen.

Forcepoint-Sicherheit für öffentliche Cloud-Umgebungen

Durch Cloud-basierte Dienste und virtuelle Bereitstellungen werden Unternehmen aller Arten und Größen umgeformt. Traditionelle lokal installierte Hardware verschwindet rapide, weil Unternehmen mehr Effizienz, Agilität und Kostenkontrolle ohne die Belastung durch Wartung und Mehraufwand benötigen, um wettbewerbsfähig zu bleiben. Diese weit verbreitete Einführung von Cloud-Architekturen stellt Sicherheitsexperten und IT-Verantwortliche vor die zusätzliche Aufgabe, diese neuen Umgebungen genauso zu schützen wie ihre physischen Vorgänger.

Die softwarebasierten Lösungen von Forcepoint Next Generation Firewall (NGFW) wurden dafür konzipiert, maximale Sicherheit mit minimalen Kosten und minimaler Komplexität bereitzustellen. Forcepoint NGFW Security Management Center (SMC) ist eine einheitliche Plattform, die Ihnen unübertroffene Transparenz, Kontrolle und konsistente Durchsetzung von Richtlinien bietet und Sie dabei unterstützt, die Einhaltung von Vorschriften in physischen Infrastrukturen und in virtuellen und Cloud-basierten Umgebungen sicherzustellen.

AWS-Cloud-Sicherheit

Zur Sicherung von Cloud-Umgebungen bietet Forcepoint die führende Firewall-Technologie der nächsten Generation für AWS – mit erprobter Skalierbarkeit, operationaler Effizienz und starker Sicherheit. Erweitern Sie einfach und sicher das Netzwerk Ihrer Organisation – von Rechenzentren und dem Netzwerkrand bis zu Ihren Zweigstellen und Remote-Standorten – über ein sicheres VPN-Gateway (Virtual Private Network) auf Ihre AWS-Cloud-Umgebung. Unsere zentralisierte Verwaltung ermöglicht es Ihnen, Richtlinien zügig und konsistent für alle Systeme zu erstellen und anzuwenden. Sie können schnell feststellen, was sowohl in Ihrer AWS-Umgebung als auch in Ihrem physischen Netzwerk geschieht.

Kunden, die zu Forcepoint NGFW wechseln, berichten von einem Rückgang der Cyber-Angriffe um 86 %, einer um 53 % geringeren zeitlichen Belastung der IT-Abteilung und einem Rückgang der geplanten Wartungsarbeiten um 70 %.

Maximale Sicherheit, minimale Komplexität

Die softwarebasierte Architektur der Sicherheitslösungen von Forcepoint, wie erweiterter Schutz vor Bedrohungen, detaillierte Paketüberprüfung und Kontrolle auf Anwendungsebene, sind für eine einfache Bereitstellung konzipiert, um ein Maximum an Sicherheit zu gewährleisten – ohne die ganze Komplexität und zusätzliche Kosten. Die softwarebasierte Sicherheitsplattform von Forcepoint bietet eine umfassende und integrierte mehrschichtige Verteidigung, die auf die spezifischen Anforderungen jeder Person, jedes Ortes oder jeder Anlage zugeschnitten werden kann, einschließlich Firewall, VPN, IPS und URL-Filterungsschutz. Diese Software-Plattform bietet alle vorhandenen Funktionen hardwarebasierter Appliances, wie zustandsabhängige Inspektion, granulare Richtlinien- und Zugriffskontrolle sowie redundante ISP-Verbindungen – allerdings ohne Box.

Transparenz und Kontrolle in Echtzeit

Forcepoint NGFW bietet vollständige Transparenz und Kontrolle über den Datenverkehr in virtuellen und Cloud-Umgebungen, die herkömmliche Managementkonsolen nicht bieten können. Das SMC liefert schnelle Berichte über den Umfang des Datenverkehrs zwischen virtuellen Systemen und warnt Administratoren, wenn ein System auszufallen droht. Verwalten Sie eine beliebige Anzahl oder Kombination von physischen oder virtuellen Forcepoint-Geräten oder -Clustern sowie softwarebasierten Versionen, die auf Standard-x86-Hardware ausgeführt werden. Das SMC erhöht auch die virtuelle Systemsicherheit über ein ganzheitliches Überwachungs-Dashboard mit umfassender Anwendungstransparenz und granularer Kontrolle.

Vereinfachte Einhaltung von Vorschriften

Die Einhaltung der neuesten gesetzlichen Anforderungen wie PCI DSS, HIPAA, Sarbanes-Oxley und FISMA in der physischen Welt ist schwierig, aber die Einhaltung dieser Vorschriften in der virtuellen Welt ist eine noch größere Herausforderung. Die traditionellen Kontrollen der jeweiligen Anwendungen sind in einer virtuellen Umgebung nicht gegeben. Dies macht es fast unmöglich, festzustellen, welche Informationen von wem und wann abgerufen wurden, und wird bei einer Prüfung wahrscheinlich zu Sicherheitswarnungen führen. Das SMC bietet Ihnen die Funktionen für Überwachung, Analyse und Berichterstellung, die erforderlich sind, um die Einhaltung von Vorschriften in virtuellen und physischen Netzwerken sicherzustellen. Es sammelt umfassende Daten für alle Netzwerkereignisse und stellt sie in klaren und verständlichen Prüfprotokollen zusammen. Das SMC listet ferner Sicherheitseinstellungen auf, protokolliert Systemänderungen und bietet die von Ihnen benötigten genauen Prüfberichte – alles mit nur einem Klick auf eine Schaltfläche.

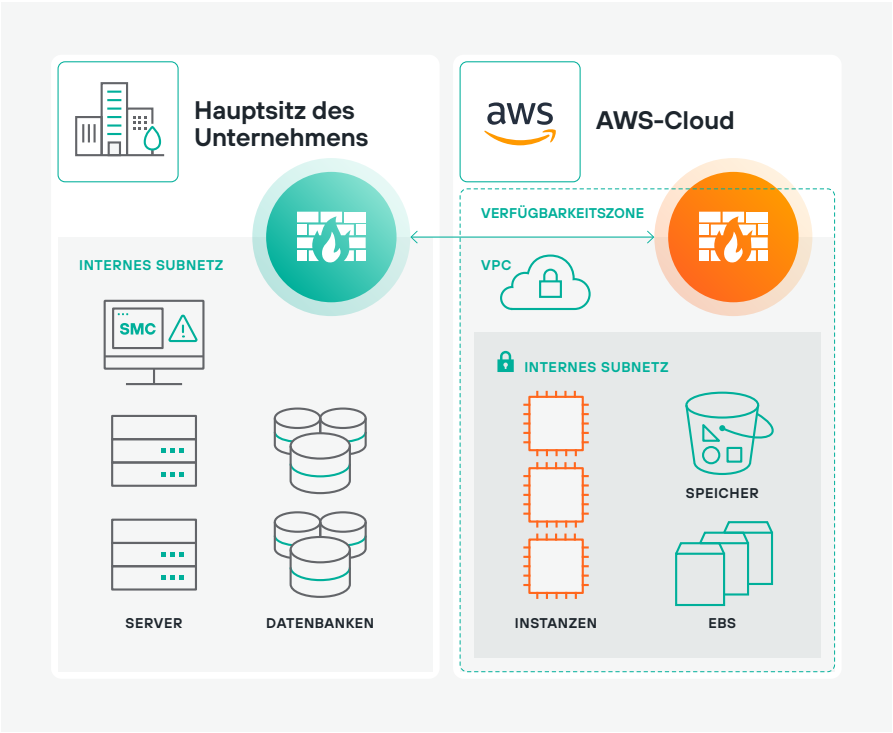
Schnelle und flexible Bereitstellung

Um die softwarebasierte Forcepoint-Sicherheitsarchitektur schnell in Ihrer AWS-Umgebung bereitzustellen, wählen Sie einfach eine der verfügbaren Optionen im AWS Marketplace.

→ Marketplace besuchen

Forcepoint NGFW und AWS-Lösungen

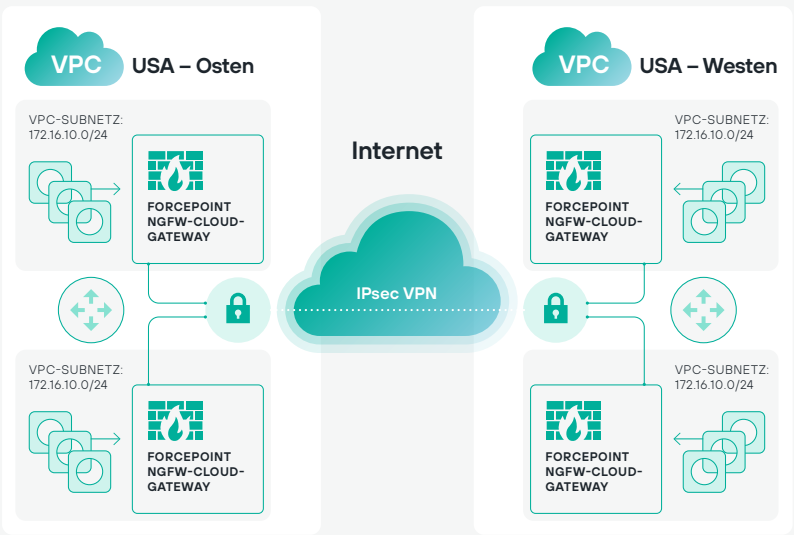
Erweitern Sie auf sichere Weise die Unternehmensnetzwerke und nutzen Sie die Möglichkeiten von AWS mit Forcepoint NGFW.



Erweitern von Unternehmensnetzwerken in AWS-Umgebungen

Forcepoint NGFW verwendet anwendungsspezifische Richtlinien zur Gefahrenabwehr: zum Schutz vor Exploits, Malware und Zero-Day-Schwachstellen in Anwendungen. Damit wird das Herausschleusen von Daten aus AWS-Umgebungen eines Unternehmens verhindert. Der AWS Security Hub bietet einen zentralen Einblick in alle Aktionen und Bedingungen, die Warnungen zur Durchsetzung von Richtlinien ausgelöst haben.

- → Erweitern des Unternehmens-netzwerks auf AWS
- → Ermöglichen von hybrider IT auf effiziente Weise und Vereinfachen der Datenübertragung in und aus AWS
- → Einfaches Verwalten beider Enden mehrerer VPN-Verbindungen an einem Ort



VPC-zu-VPC-Routing zwischen Regionen

Verbinden Sie sicher VPCs zwischen mehreren AWS-Regionen. Mit der branchenführenden Netzwerksicherheitstechnologie von Forcepoint können Sie Sicherheitsrichtlinien verwalten, kontrollieren und durchsetzen.

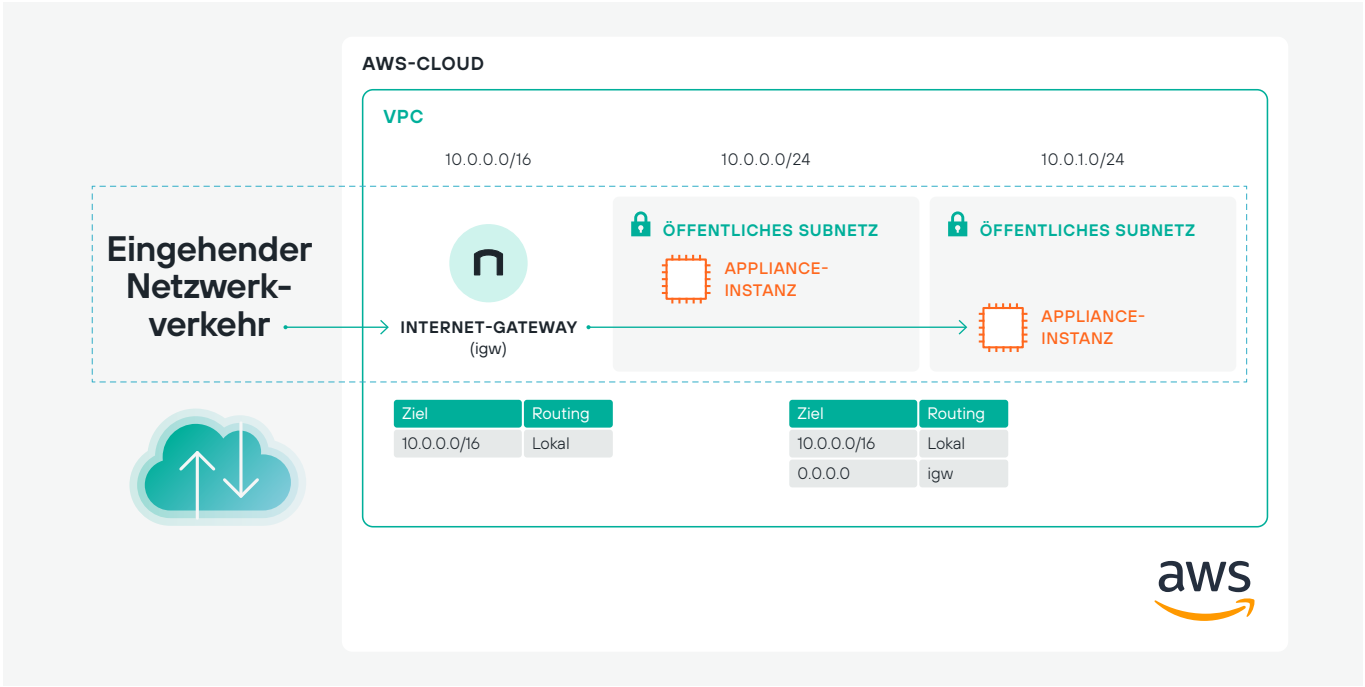
- → Sicherer Informationsfluss zwischen Regionen
- → Anwenden von konsistenten Sicherheitsrichtlinien in mehreren Regionen

Ein Energieversorger konnte 90 % seiner WAN-Kosten durch den Einsatz von NGFW mit SD-WAN von Forcepoint und den Wechsel in die Cloud sparen – und das alles mit einer Zero-Touch-Installation.

Amazon VPC Ingress Routing

Amazon VPC Ingress Routing vereinfacht die Integration der Netzwerksicherheit in Ihre Amazon Virtual Private Cloud-(VPC-) Infrastruktur und macht es für Sie einfacher, Sicherheitsrichtlinien einheitlich auf das gesamte Unternehmensnetzwerk anzuwenden – sowohl in der Cloud als auch lokal, um Ihre AWS-Workloads effektiv zu schützen.

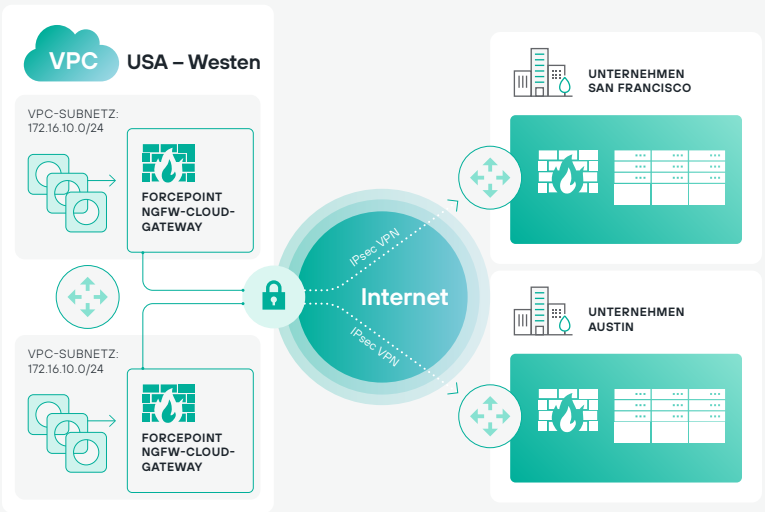
- → Gewinnen Sie die Flexibilität, den Datenverkehr, der für Amazon VPC bestimmt ist, mit dem gleichen Maß an Kontrolle zu behandeln, das für den Zugriff auf das Unternehmensnetzwerk verwendet wird.
- → Setzen Sie die Richtlinien für die Netzwerksicherheit einheitlich im gesamten Unternehmensnetzwerk um, ohne zusätzliche Latenz.
- → Erzielen Sie maximale Sicherheit mit minimalen Kosten und minimaler Komplexität



AWS VPN CloudHub

Verbinden Sie sicher VPCs zwischen mehreren AWS-Regionen. Mit der branchenführenden Netzwerksicherheitstechnologie von Forcepoint können Sie Sicherheitsrichtlinien verwalten, kontrollieren und durchsetzen.

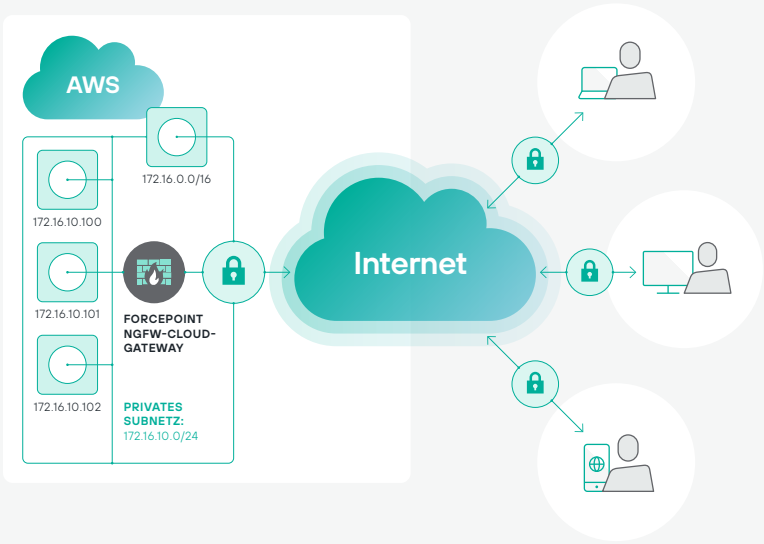
- → Sicherer Informationsfluss zwischen Regionen
- → Anwenden von konsistenten Sicherheitsrichtlinien in mehreren Regionen



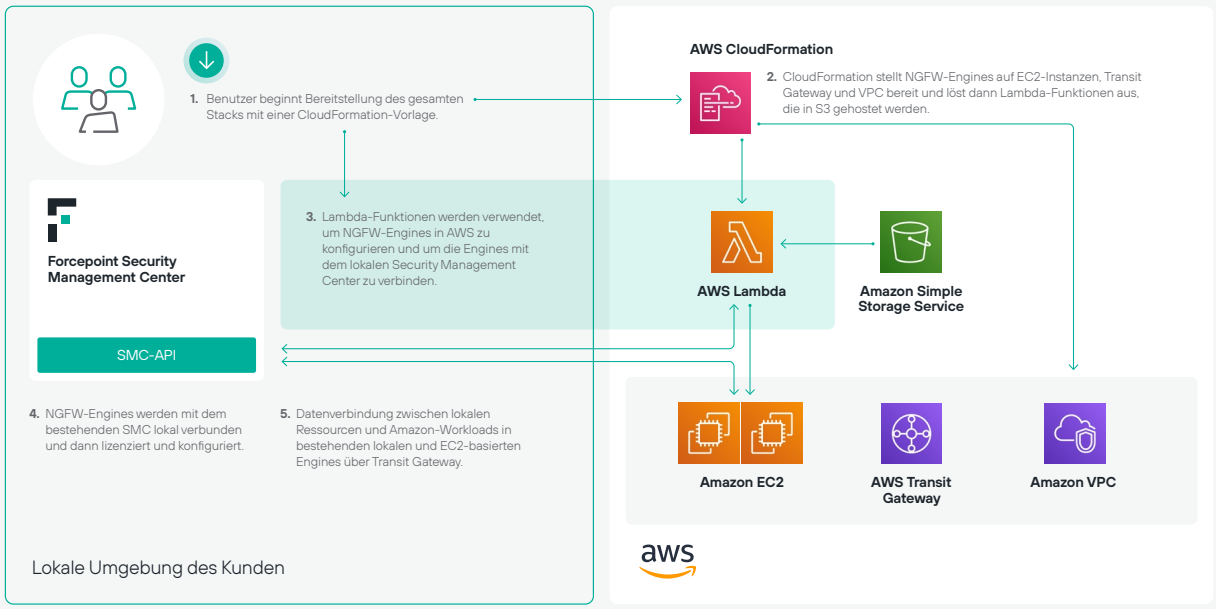
Konnektivität für den Remote-Zugriff

Forcepoint NGFW kann als Cloud-Edge-Gateway verwendet werden, um Ihre Remote-Benutzer mit Amazon Virtual Private Cloud (VPC) zu verbinden. Das Cloud-Gateway von Forcepoint NGFW kann in einer Amazon Elastic Compute Cloud-(EC2-) Instanz eingesetzt werden und bietet erweiterte Firewall-Funktionen zum Schutz Ihrer EC2-Instanzen für alle ein- und ausgehenden Zugriffe, wie z. B.:

- → Anwendungsbewusstsein
- → Funktionen zur Benutzeridentifizierung



Forcepoint NGFW und AWS-Serviceintegrationen

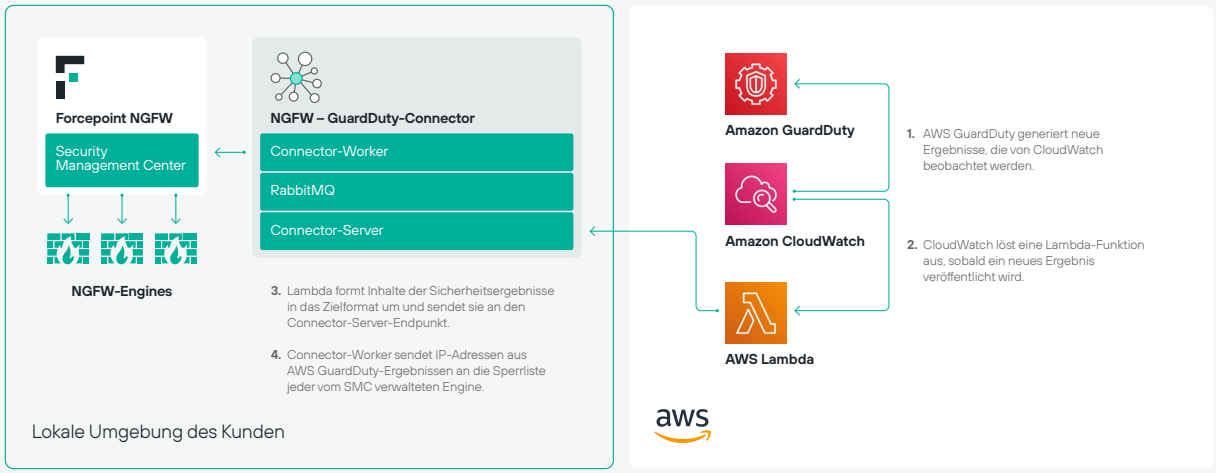


Transit Gateway-Integration

Stellt einen redundanten Satz von Forcepoint Next Generation Firewalls als EC2-Instanzen und ein AWS Transit Gateway bereit und verbindet die NGFW-Engines mit einem vorhandenen Forcepoint Security Management Center über AWS Lambda-Funktionen. Redundante IPSEC-Tunnel werden zwischen den Cloud-internen NGFW-Engines und dem Transit Gateway eingerichtet. Sicherheitsrichtlinien, die vom Forcepoint Security Management Center verwaltet werden, können auf die NGFW-Engines in AWS angewendet werden, um den zum und vom Transit Gateway fließenden Datenverkehr zu sichern.

- → Ermöglicht die konsistente Anwendung von Sicherheitsrichtlinien in lokalen und AWS-Systemen.
- → Automatisiert die Bereitstellung der gesamten Technologie unter Verwendung einer einzigen AWS CloudFormation-Vorlage mit anpassbaren Parametern, um maßgeschneiderte Bereitstellungen zu ermöglichen.

Leitfaden herunterladen

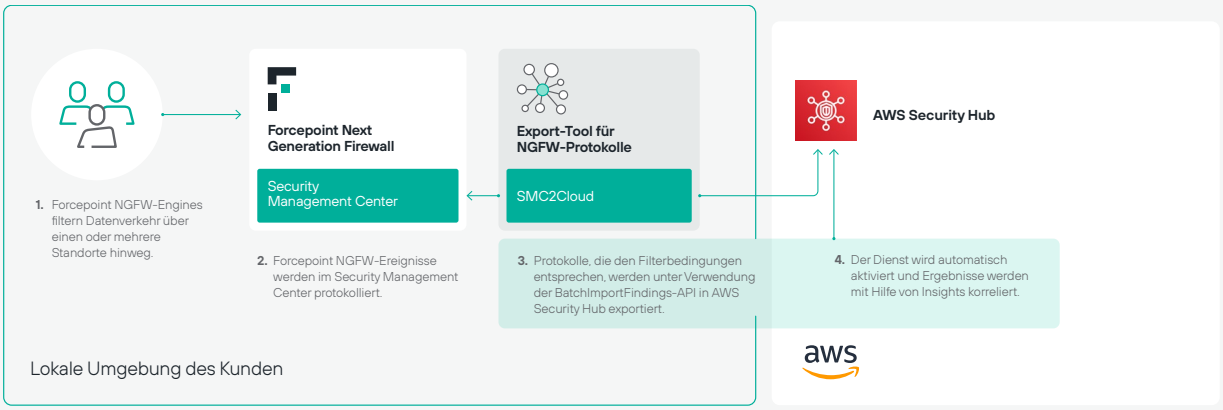


Amazon GuardDuty-Integration

GuardDuty bietet AWS-Kunden eine intelligente und kostengünstige Option für die kontinuierliche Bedrohungserkennung in der AWS-Cloud. Der Dienst verwendet maschinelles Lernen, Anomalieerkennung und integrierte Threat Intelligence, um mögliche Bedrohungen zu erkennen und zu priorisieren. Die Forcepoint NGFW-Integration automatisiert den Import in Echtzeit von Sicherheitsergebnissen von Amazon GuardDuty.

- → Benutzer, Anwendungen und Dienste, die lokal gehostet und von NGFW geschützt werden, profitieren von der besseren Sichtbarkeit von Bedrohungsakteuren, die auf den AWS-Footprint eines Unternehmens abzielen.
- → Bösartige Quell-IP-Adressen, die von Amazon GuardDuty identifiziert wurden, werden anschließend in einer ganzen Reihe von NGFW-Engines, die an den Standorten des Unternehmens eingesetzt werden, auf eine Sperrliste gesetzt.
- → Effektiver Schutz als Ergebnis der geteilten Erkenntnisse.

Leitfaden herunterladen



Interoperabilität mit AWS Security Hub

AWS Security Hub bietet eine konsolidierte Ansicht Ihres Sicherheitsstatus in den AWS-Konten. Die Forcepoint-Integration mit AWS Security Hub bietet Einblicke darüber, wie Benutzer mit Ihren sensibelsten Daten interagieren – unabhängig davon, wo sie sich befinden.

- → Automatischer Export von Protokollereignissen von NGFW in AWS Security Hub in Echtzeit, um die Antwortzeiten zu beschleunigen.
- → Korrelation von Sicherheitsergebnissen mit anderen Quellen, um die Transparenz in allen Standorten zu verbessern, die von NGFW geschützt werden.
- → Einfache Datenpflege über die Gruppierung mit einer Vielzahl von Feldern, wie Schweregrad und Typ, um die für Ihr Unternehmen wichtigsten Maßnahmen zu priorisieren.

Leitfaden herunterladen Demo-Termin vereinbaren

[Forcepoint Next Generation Firewall with Amazon Web Services Solution-Brief-DE] 24May2021