Cloud NGFW: Erstklassige Sicherheit und einfaches Management auf AWS

Mit der ML-gestützten NGFW, die von Palo Alto Networks verwaltet und als cloudnativer Service auf AWS bereitgestellt wird, sind Sie in Sachen Cybersicherheit immer auf dem neuesten Stand.

paloalto® NETWORKS | aws

Inhalt

Die zunehmende Cloud-Nutzung erfordert moderne Cybersicherheitslösungen

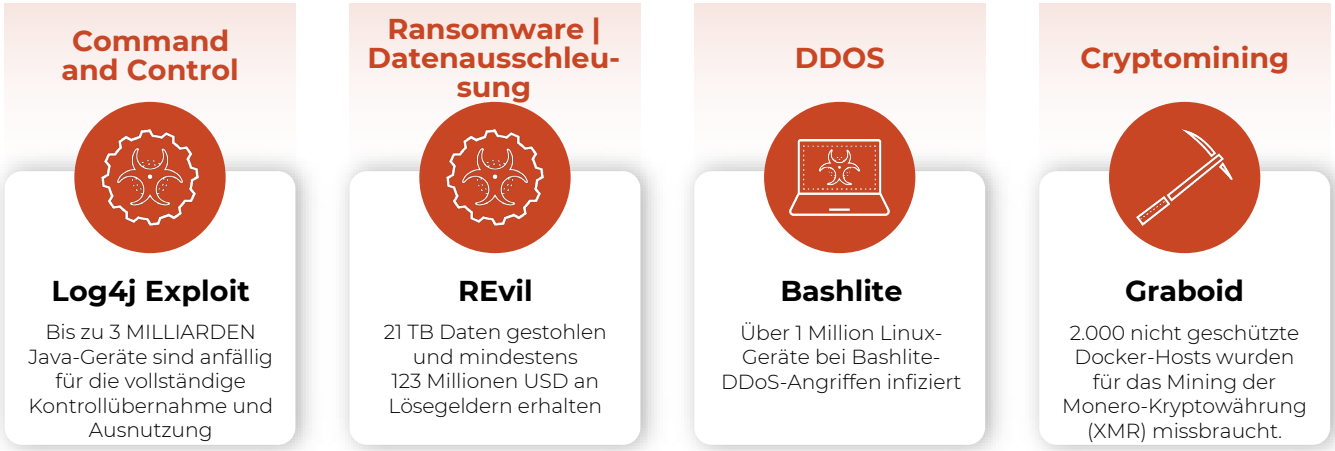
In den letzten Jahren hat die Public-Cloud-Nutzung stark zugenommen und während der Pandemie haben Unternehmen ihre Cloud-Umgebungen zusätzlich erweitert. Inzwischen hosten 69 Prozent der Unternehmen mehr als die Hälfte ihrer Workloads in der Cloud – das ist eine Steigerung um 123 Prozent im Vergleich zu 2020.

Doch damit wächst auch die Verantwortung für die Sicherheit der Cloud-Daten. Public Clouds wie Amazon Web Services (AWS) verschaffen Organisationen eine größere Agilität und die Möglichkeit, die Kosten zu reduzieren und das Infrastrukturmanagement zu minimieren. Für Sicherheit sorgt das Modell der gemeinsamen Verantwortung, das heißt, AWS schützt die Cloud-Infrastruktur und die Kunden schützen ihre Daten. Durch die Zusammenarbeit mit einem Sicherheitspartner wie Palo Alto Networks können sich Organisationen weiterhin auf ihren Geschäftsbetrieb konzentrieren und sind dennoch umfassend geschützt. Das Modell der gemeinsamen Verantwortung ist ein wichtiger Faktor, wenn Organisationen den Cyberkriminellen stets einen Schritt voraus und für neue Bedrohungen gewappnet sein möchten.

Die gute Nachricht: Es gibt eine effektive Sicherheitslösung. Next-Generation Firewalls (NGFWs) sind die Grundpfeiler moderner Netzwerksicherheit. Sie schützen vor Bedrohungen, die versuchen, den ein- und ausgehenden sowie den lateralen Datenverkehr zu infiltrieren, und decken physische, virtuelle und Container-Umgebungen ab.

Sicherheitsteams benötigen zuverlässigen Netzwerkschutz und einfaches Cloud-Management

Die Bereitstellung in der Cloud ist allerdings nicht ganz risikofrei, da sich die Bedrohungslandschaft ebenfalls rasant weiterentwickelt. Das zeigt sich an der kürzlich ausgenutzten Log4j-Sicherheitslücke, aber auch an der Zunahme von Angriffen mit Ransomware, DDoS (Distributed Denial of Service) und Cryptojacking-Würmern.

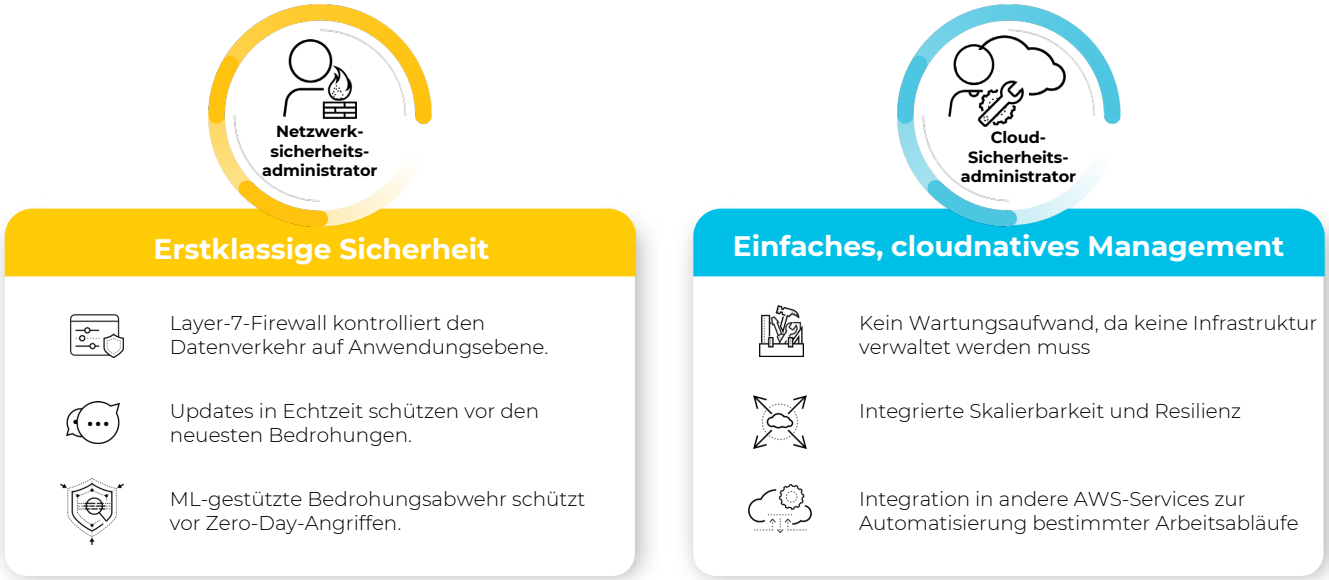


Diese netzwerkbasierten Bedrohungen können nicht nur den Geschäftsbetrieb stören, sondern auch den Ruf des betroffenen Unternehmens schädigen. Daher müssen AWS-Kunden erstklassige Sicherheit zum Schutz ihrer zunehmenden Public-Cloud-Workloads implementieren können. Sie benötigen in ihren Umgebungen Transparenz und Sicherheit auf Layer 7, um moderne Cyberangriffe abzuwehren, und gleichzeitig einen geringeren Aufwand für Netzwerksicherheits- und DevOps-Teams. Denn Sicherheitsteams fragen sich zu Recht: Ist es nicht möglich, das Beste aus beiden Welten zu erhalten? NGFW-Schutz und das einfache Management in der Cloud?

Cloud NGFW von Palo Alto Networks

Cloud NGFW ist die erste NGFW, die in AWS Firewall Manager integriert werden kann. Cloud NGFW wird von Palo Alto Networks verwaltet und bietet branchenführende Schutzfunktionen mit einem beispiellos einfachen Management, um auch die komplexesten Angriffe in Echtzeit abzuwehren. Sie funktioniert wie alle anderen nativen AWS-Services, ist aber dennoch einzigartig, da AWS-Kunden ihre Workloads mit den erstklassigen Sicherheitsfunktionen schützen können, für die Palo Alto Networks bekannt ist.

Profitieren Sie mit nativ integrierter Netzwerksicherheit als Service auf AWS vom Besten aus beiden Welten.



Moderne Unternehmen benötigen beides: erstklassige Sicherheit + einfaches, cloudnatives Management.

Cloudnative Netzwerksicherheit zum Schutz von AWS

Cloud NGFW bietet ML-gestützte Netzwerksicherheit für Ihre Amazon Virtual Private Clouds (VPCs). Sicherheitsfunktionen wie Palo Alto Networks App-ID, Threat Prevention und Advanced URL Filtering wurden speziell entwickelt, um bekannte Bedrohungen und Zero-Day-Angriffe abzuwehren.

App-ID: Durch die Kontrolle des Netzwerktraffics mithilfe der patentierten Technologie von Palo Alto Networks zur Klassifizierung des Layer-7-Datenverkehrs werden die Risiken minimiert. App-ID identifiziert anhand unterschiedlicher Klassifizierungen die Anwendungen, die Daten über das Netzwerk senden. So wird die Identität einer Anwendung ermittelt – unabhängig von Port, Protokoll, SSH/SSL-Verschlüsselung oder sonstigen Umgehungstaktiken. Anschließend führt App-ID eine Richtlinienüberprüfung durch, um festzustellen, ob die Anwendung blockiert, durchsucht, untersucht oder umgeleitet werden soll.

Threat Prevention: Mit der branchenführenden Threat Prevention lassen sich bekannte Malwarevarianten, Exploits von Sicherheitslücken und C2-Infrastrukturen (Command and Control) automatisch verhindern. Threat Intelligence wird jeden Tag automatisch zusammengestellt und direkt an die Cloud NGFW weitergeleitet und implementiert, um alle Bedrohungen abzuwehren. Die effektiven IPS-Funktionen (Intrusion Prevention System), zum Beispiel die Single-Pass-Architektur und Richtlinienverwaltung, ermöglichen eine umfassende Erkennung und Abwehr von Bedrohungen – ganz ohne Leistungseinbußen.

Advanced URL Filtering: Unbekannte webbasierte Angriffe werden in Echtzeit abgewehrt, damit Sie nicht zum ersten Opfer werden. Advanced URL Filtering analysiert den Netzwerkverkehr, kategorisiert die URLs und blockiert Bedrohungen in Sekundenschnelle. Da sowohl mehrere als auch benutzerdefinierte Kategorien unterstützt werden, können zusätzliche Sicherheitsebenen eingerichtet werden, zum Beispiel die gezielte SSL-Entschlüsselung und erweiterte Protokollierung. Zusätzlich zu den eigenen Analyseergebnissen verwendet Advanced URL Filtering auch freigegebene Threat Intelligence von dem Malwareschutz WildFire® und anderen Quellen, um die Sicherheitsfunktionen zum Schutz vor schädlichen Websites automatisch zu aktualisieren.

Einfaches Management und problemlose Skalierung auf AWS

Mit Cloud NGFW lassen sich die Sicherheitsfunktionen ganz einfach in die AWS-Umgebung integrieren. Das vereinfacht die Prozesse, sodass Ihr Team Daten, Anwendungen und Workloads problemlos mit der für die Cloud typischen Agilität schützen kann.

Vereinfachte Management- und Automatisierungsfunktionen: AWS Firewall Manager erleichtert große Implementierungen und ermöglicht das konsistente Management von Firewallrichtlinien für mehrere AWS-Konten und Amazon VPCs. Cloud NGFW kann nativ in AWS Firewall Manager integriert werden und vereinfacht daher die Cloud-Netzwerksicherheit. So können Sie ohne großen Aufwand Ihre automatisierten Arbeitsabläufe schützen und dank der Load-Balancing- und Auto-Loading-Funktionen von AWS dynamisch an den Bedarf anpassen.

Außerdem kann Cloud NGFW auch mit unerwarteten Leistungsspitzen umgehen, da es den AWS Gateway Load Balancer (GWLB) für die bedarfsgesteuerte Hochverfügbarkeit und eine flexible Skalierung nutzt.

Kein Wartungsaufwand: Der resiliente Cloud-Service wird dynamisch und in Abstimmung mit dem Netzwerktraffic skaliert, sodass kein Infrastrukturmanagement erforderlich ist. Mit Cloud NGFW muss keine aufwendige hochverfügbare Firewallarchitektur entwickelt, manuell bereitgestellt und konfiguriert werden. Da die Firewall speziell für AWS entwickelt wurde, sorgt sie zudem für zuverlässige Sicherheit und Resilienz.

Umfassender Überblick: Sie erhalten einen umfassenden Überblick über Anwendungen, Inhalte und den Datenverkehr, unabhängig von den Ports, Protokollen und Umgehungstaktiken.

Cloudnatives Design zur Vereinfachung des Geschäftsbetriebs

Dank IaC (Infrastructure as Code) und der Integration in die CI/CD-Pipelines (Continuous Integration/Continuous Delivery) reduziert Cloud NGFW den Arbeitsaufwand der Cloud-Sicherheitsteams.

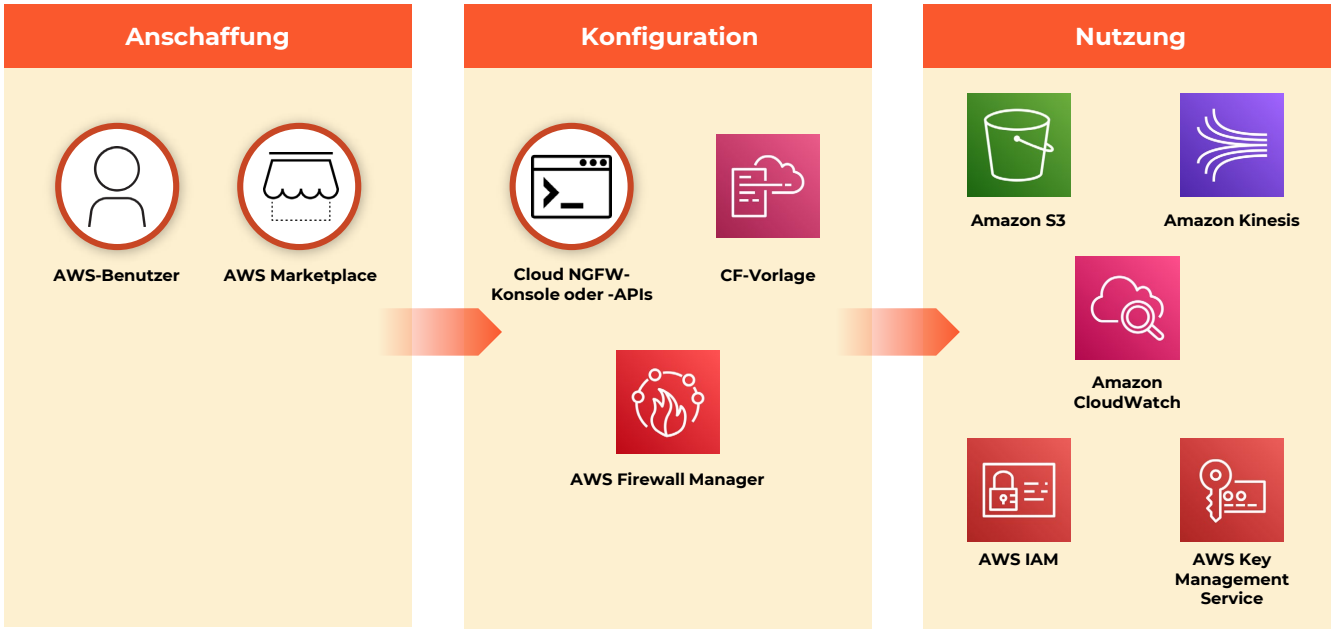
IaC zur Automatisierung der Best Practices im Sicherheitsbereich: DevSecOps-Teams können die IaC-Tools nutzen, die sie bereits kennen, und die Sicherheitsfunktionen der Next-Generation Firewall schnell und einfach bereitstellen.

Deklarative Richtlinien in CI-/CD-Prozessen: Cloud NGFW-Funktionen können über deklarative Richtlinien in Terraform- und CloudFormation-Vorlagen bereitgestellt werden. Wenn Sie die Richtlinienerstellung in die CI/CD-Pipeline integrieren, sorgen Sie für konsistente Arbeitsabläufe und können Richtlinien-Tags einfacher hinzufügen oder entfernen.

Automatisierungsfunktionen: Unabhängig davon, ob Sie Ihre Bereitstellungen mit Cloud NGFW oder AWS Firewall Manager verwalten, sollten Sie unbedingt die Automatisierungsfunktionen nutzen, um Arbeitsabläufe zu optimieren, repetitive Aufgaben zu vermeiden und Ihr Team zu entlasten. Cloud NGFW unterstützt AWS CloudFormation-Vorlagen, Terraform Provider und APIs. AWS Firewall Manager unterstützt dieselben Automatisierungsfunktionen und zudem auch die Befehlszeilenschnittstelle (CLI) und SDK (Software Development Kits).

Einrichtung mit nur einem Klick: Die Einrichtung dauert nur etwa fünf Minuten. Sie können Cloud NGFW über den AWS Marketplace erwerben und mit nur einem Klick einrichten.

Native Protokollierung: Cloud NGFW kann problemlos in native AWS-Services, wie Amazon Simple Storage Service (Amazon S3), Amazon CloudWatch und Amazon Kinesis integriert werden, und erfüllt damit die Complianceanforderungen zur zentralen Protokollierung.



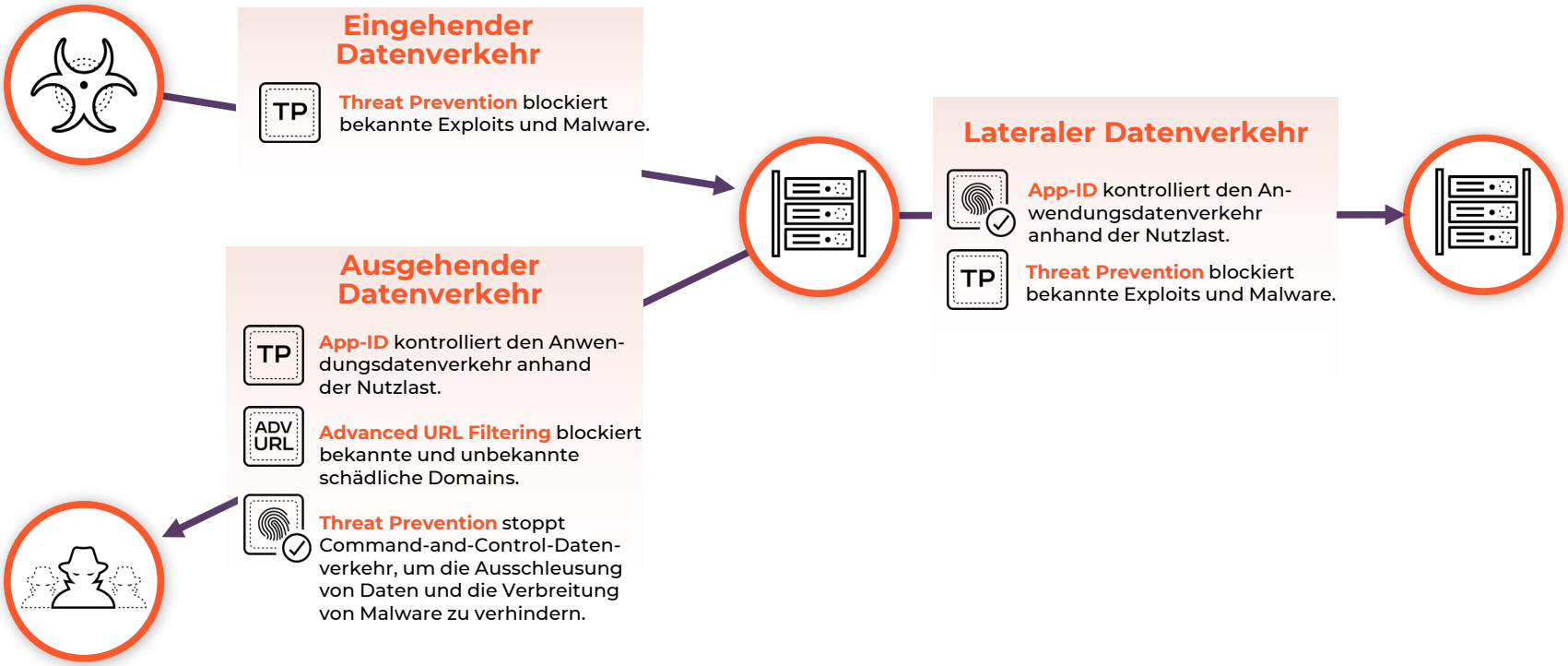
Cloud NGFW kann in Ihre AWS-Umgebung integriert werden.

Schnelle und einfache Bereitstellung von Sicherheitsfunktionen der nächsten Generation

Palo Alto Networks und AWS haben die Schritte für die Cloud NGFW-Implementierung so einfach wie möglich gestaltet, damit Sie die ML-gestützten Netzwerksicherheitsfunktionen schnell einrichten können.

1. Suchen Sie Cloud NGFW im AWS Marketplace und abonnieren Sie es mit ein paar Klicks. Anschließend können Sie Ihre AWS-Konten einbinden und Zahlungsoptionen auswählen, zum Beispiel ein nutzungsbasiertes Modell.
2. Erstellen Sie Cloud NGFW-Ressourcen, die keine manuellen Administrationsaufgaben erfordern, beispielsweise eine Architektur für die Hochverfügbarkeit und bestimmte Konfigurationen für die Skalierung.
3. Sicherheitsrichtlinien können Sie ganz einfach im AWS Firewall Manager oder in der Cloud NGFW-Konsole festlegen, die über eine API verbunden wird. Hier können Sie auch Sicherheitsrichtlinien für App-ID, Threat Prevention und Advanced URL Filtering angeben, damit Cloud NGFW Ihre AWS-Umgebung automatisch schützt.
4. Verknüpfen Sie Cloud NGFW mit GWLB als Endpunkt, um den Netzwerktraffic zu schützen und den ein- und ausgehenden Datenverkehr sowie Datenverkehr zwischen Amazon VPCs und zwischen Amazon VPCs und internen Subnetzen zu überprüfen. Dadurch erhalten Sie ein Cluster mit hoher Verfügbarkeit, das je nach Datenverkehr dynamisch skaliert wird, und ermöglichen nahtlose Softwareupdates. GWLB bietet eine einfache, transparente Einbindung in vorhandene AWS-Umgebungen.

Cloud NGFW in der Praxis



Cloud NGFW schützt den ein- und ausgehenden Datenverkehr und verhindert die Ausbreitung im Netzwerk.

Cloud NGFW in der Praxis

Ausgehender Datenverkehr: Cloud-Workloads, die auf externe Quellen zugreifen, bergen das Risiko, dass sie über das Web angegriffen und Daten ausgeschleust werden. Regulierte Apps, die mit dem PCI- (Payment Card Industry) oder HIPAA-Standard konform sind, erfordern zudem IPS-Funktionen für den ausgehenden Datenverkehr.

Cloud NGFW stoppt neue webbasierte Angriffe, reduziert die Komplexität für das Sicherheitsteam und minimiert das Gesamtrisiko für Ihr Unternehmen. Threat-Prevention-Funktionen erfüllen die IPS-Anforderungen bezüglich der Compliance.

Eingehender Datenverkehr: Öffentlich zugängliche und regulierte Apps müssen vor schädlichen Aktivitäten geschützt werden.

Cloud NGFW reduziert die Risiken und manuellen Aufgaben durch die automatische Abwehr von Bedrohungen. Sie können problemlos die IPS-Anforderungen zur Einhaltung von Vorgaben wie PCI und HIPAA erzielen.

Datenverkehr zwischen Amazon VPCs: Zur Erfüllung der Zero-Trust-Prinzipien und Complianceanforderungen sowie zur Verhinderung der Ausbreitung im Netzwerk ist für Cloud-Workloads eine erweiterte Segmentierung und Bedrohungsabwehr notwendig.

Cloud NGFW implementiert Threat Prevention und App-ID zwischen Netzwerksegmenten, um die Ausbreitung von Bedrohungen zu vermeiden und Compliancevorgaben zu erfüllen. Gleichzeitig vereinfacht es die Bereitstellung, da keine älteren IPS-Appliances eingebunden werden müssen.

Datenverkehr zwischen Amazon VPC und On-Premises-Umgebungen: Der Datenverkehr zwischen VPCs und On-Premises-Umgebungen erfordert erweiterte Segmentierung und Bedrohungsabwehr, um die Zero-Trust-Prinzipien und Complianceanforderungen zu erfüllen sowie die Ausbreitung im Netzwerk zu verhindern.

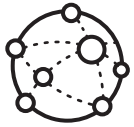
Cloud NGFW implementiert Threat Prevention und App-ID zwischen Netzwerksegmenten, um die Ausbreitung von Bedrohungen zu vermeiden die Compliancevorgaben zu erfüllen. Gleichzeitig vereinfacht es die Bereitstellung, da keine älteren IPS-Appliances eingebunden werden müssen.

Die Vorteile eines weltweit führenden Cybersicherheitsanbieters

Cloud NGFW wird von der größten Netzwerksicherheitsplattform der Branche und einem führenden Cybersicherheitsanbieter unterstützt. Palo Alto Networks ist stets über die Entwicklungen der Cyberkriminellen informiert und schützt Sie vor potenziellen neuen Bedrohungen.

4,3 MIO.
Sicherheitsupdates pro Tag

224 MRD.
blockierte Bedrohungen pro Tag



15 MIO.
geschützte Transaktionen pro Tag

95 %
der Fortune 100-Unternehmen vertrauen auf Palo Alto Networks

FÜHREND
in der Unternehmenssicherheit

10 MAL
Leader im Gartner® Magic Quadrant™ for Network Firewalls

Palo Alto Networks bietet Funktionen für einen fortlaufenden Überblick, die Durchsetzung von Compliancevorgaben, die Berichterstellung und die Bedrohungsabwehr für alle AWS-Ressourcen. Von Amazon Elastic Cloud Compute (Amazon EC2) über Amazon Elastic Container Service (Amazon ECS) bis AWS Lambda und zahlreiche andere Produkte: Palo Alto Networks bietet native AWS-Services für erstklassige Sicherheit. Gemeinsam stellen AWS und Palo Alto Networks ein umfassendes Angebot an integrierten Sicherheitsfunktionen bereit und unterstützen damit sowohl Unternehmen, die gerade erst mit der Cloud-Migration beginnen, als auch Organisationen, die ihren Geschäftsbetrieb bereits in die Cloud ausgelagert haben.

Der nächste Schritt?

Abonnieren Sie Cloud NGFW gleich über den AWS Marketplace, damit Ihre Anwendungen und Workloads sofort durch erstklassige Sicherheit geschützt sind und Ihr Team von dem einfachen, cloudnativen Management profitiert.

Zum AWS Marketplace >>

cloud-ngfw-ebook-033022