How Palo Alto Networks and AWS Deliver Unparalleled Cloud Security

Cloud adoption is growing by leaps and bounds – and so are its security challenges. With cyberthreats becoming ever more sophisticated, large-scale cloud estates are increasingly difficult for security teams to protect. Plus, these environments are changing constantly, with developers and DevOps teams building and deploying at a frenetic pace. Too often, they're doing so without security guidance or controls.

AWS' published shared responsibility model, an integral aspect of cloud services, aims to heighten awareness of security considerations amidst the ongoing adoption of cloud technologies. In this model, security and compliance are jointly managed between AWS and the customer. AWS shoulders the responsibility for ensuring the security of the cloud infrastructure, encompassing everything from the host operating system to physical facility security.

Conversely, customers are accountable for securing their data, applications, and configurations in the cloud environment. Nonetheless, many organizations face constraints in addressing threats across cloud applications, networks, and computing resources due to limited resources or expertise. Palo Alto Networks can play a crucial role in helping customers secure their applications and data.

Palo Alto Networks and AWS Elevate Your Cloud Security

AWS manages and controls cloud infrastructure components from the host operating system and virtualization layer down to the physical security of the facilities where the services operate. Palo Alto Networks helps customers do their part by protecting compute, network, and storage services along with the apps they run.

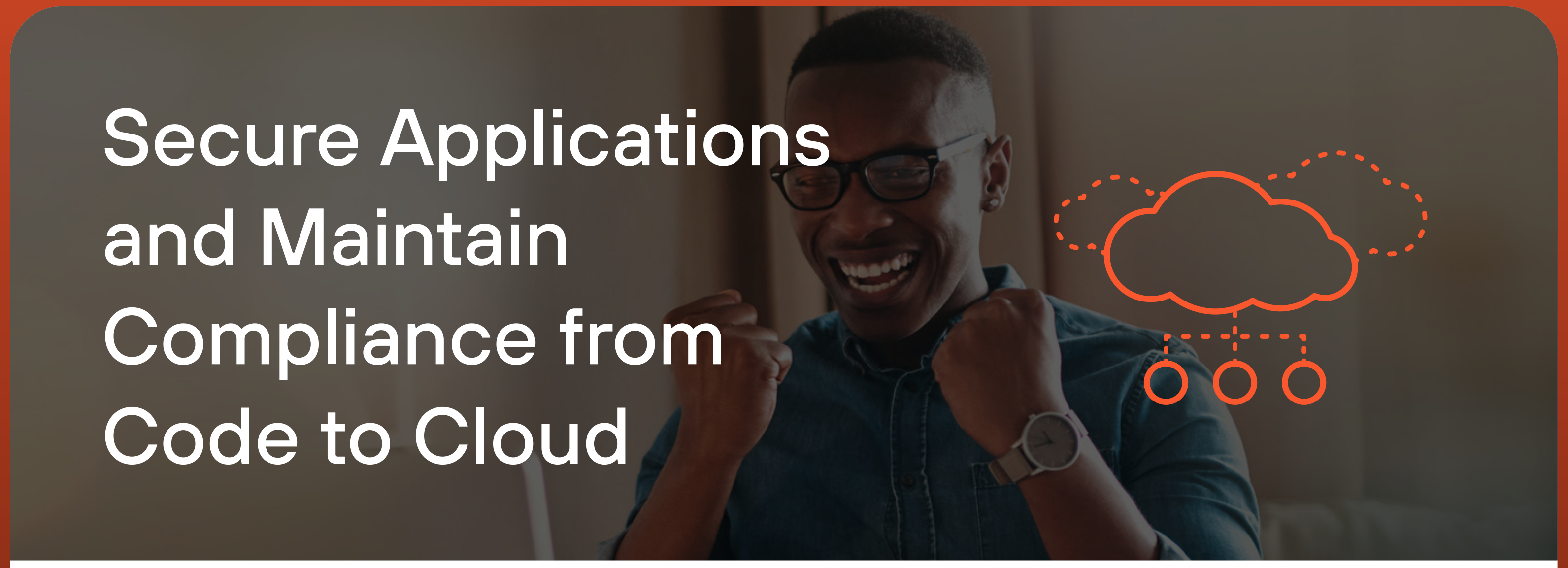
Together, we provide the broadest set of integrated cloud-native security solutions on the market. We also ensure that security and compliance are properly implemented and easily maintained across apps, data, workloads, infrastructure, networks, and code.

Integrated Cloud Security Solutions at a Glance - Click to Explore:

Palo Alto Networks security solutions are purpose-built for AWS. They integrate with AWS' native security services to help our mutual customers achieve their desired security outcomes and meet compliance regulations. These integrated offerings provide unparalleled visibility, protect against dynamic threats, and automate and streamline SOC processes.

Gain Advanced Network Protection and Threat Prevention

Blocks detected malicious activities in real time by automatically updating security policies on Palo Alto Networks Next-Generation Firewalls – including CN-Series Containerized, VM-Series Virtual, and Cloud NGFWs – based on threat feeds from AWS Security Hub and Amazon GuardDuty.



Secure Applications and Maintain Compliance from Code to Cloud

Prisma Cloud by Palo Alto Networks ingests AWS findings from security services like AWS Security Hub, Amazon GuardDuty, Amazon Inspector, and more to help you consolidate findings, accurately assess constantly changing cloud resources, and better secure your cloud.

Automate and Accelerate Response for Security Incidents and Forensic Use Cases

Ingest alerts across AWS and other sources, execute automatable playbooks – and up to 95% of response actions that typically require human review – with Palo Alto Networks Cortex XSOAR and AWS Security Hub.

Palo Alto Networks Products for AWS

Prisma Cloud

Prisma Cloud is a Code to Cloud™ Platform that makes it easy to securely scale, automate, and stay agile. We deliver cloud-native security and application protection for multi- and hybrid-cloud environments. The platform supports wide-ranging cloud security needs, including shift-left code security, full-lifecycle cloud security posture management, cloud workload protection, cloud infrastructure entitlement management, and also data and AI security.

VM-Series Virtual Next-Generation Firewall

This all-in-one, class-leading firewall helps you secure AWS deployments from migration to reinvention. Powered by inline deep learning, security services such as Advanced Threat Prevention and Advanced URL Filtering find and stop zero-day threats to applications and networks in real time. You can even integrate with your application developer's workflows without tradeoffs between deployment speed and security. Plus, its centralized management lets you deploy VM-Series virtual firewalls anywhere while maintaining consistent visibility, security, and logging across everything. Managed by Palo Alto Networks and easily procured in AWS Marketplace, the service has been designed to easily deliver best-in-class security protections with AWS simplicity and scale.

Cloud Next-Generation Firewall

The industry's first machine learning-powered NGFW provides unparalleled protection from known, unknown, and zero-day cyber threats within Amazon's Virtual Private Clouds (VPC). It combines threat intelligence from over 15 trillion daily transactions and in-depth application intelligence to deliver real-time threat detection, proactive defense measures, granular traffic control, and reduced attack risk. You'll be able to meet critical compliance standards while adhering to zero-trust security models.

Palo Alto Networks Products for AWS

Prisma Access

Prisma Access protects all cloud application traffic with best-in-class Zero Trust Network Access (ZTNA) 2.0 capabilities, while securing both access and data. With globally distributed networking and security for all users and applications, it safeguards the hybrid workforce while providing exceptional user experiences. Users can connect to Prisma Access to safely access cloud and data center applications as well as the Internet. With its common policy framework and single-pane-of-glass management, you can easily secure AWS VPCs without compromising performance.

CN-Series Containerized Next-Generation Firewall

This NGFW is purpose-built to secure Kubernetes (K8) from cyberthreats and attacks. Network Security teams gain Layer 7 visibility into Kubernetes environments, provide inline threat prevention for containerized applications deployed anywhere, and dynamically scale security without compromising DevOps agility. You'll realize frictionless CI/CD pipeline deployment while delivering extraordinary runtime network protection by enabling unified management across all firewalls.

Cortex XSOAR

Streamline security operations for speed and consistency by integrating automation, case management, real time collaboration, and threat intelligence management. Cortex XSOAR helps stop breaches with AI-driven threat prevention, detection, and response across cloud, endpoint, network, and third-party assets. You'll improve your SOC team's productivity and free them to focus on critical needs by eliminating manual repetitive data enrichment and remediation tasks associated with cloud security alerts.

Customer Testimonial

Registers of Scotland

Challenge

The Registers of Scotland planned to digitally transform over 400 years of land registry history. To ensure security and avoid compliance violations while deploying their new cloud apps, they needed a fail-safe way to detect and prevent development misconfigurations.

Solution

They standardized on Palo Alto Networks Prisma Cloud, gaining all essential security capabilities, including VCG (visibility, compliance, governance), IAM (identity access management), and Data, Container, Serverless, and CCS (cloud code security) for workloads running in AWS. This enabled complete visibility, threat detection, and automated response.

Results

Registers of Scotland launched new services faster while eliminating security constraints around cloud-native architecture. Not only did they simplify AWS management and security, they also accelerated time to value and boosted efficiency by saving the equivalent of 4 staff people's time.

Get started with Palo Alto Networks solutions on AWS. Visit the AWS Marketplace or APN Partner website to start a free trial of our products today.

> "Prisma Cloud security posture management gives us complete control across the development pipeline, preventing insecure AWS configurations from entering production."
>
> \- **Bob Bowden,**
> *Security Architect,*
> Registers of Scotland

Advanced Network Protection and Threat Prevention

The number of workloads migrating to the cloud has skyrocketed. Gartner says that by 2028, 70% of tech workloads will run in the cloud.

They also predict that 90% of organizations will run containerized applications in production by 2026. A recent Palo Alto Networks Threat Report showcases the need for concern: 24% of today's deployed containers have security faults.

Clearly, the surface area for cyberattacks will continue expanding as will sophisticated ransomware and zero-day threats on networks and applications. Palo Alto Networks and AWS mitigate these risks for you.

Securely Migrate and Scale with Strata Next-Generation Firewalls,Gateway Load Balancer, Security Hub, and GuardDuty

Palo Alto Networks and AWS take a proactive, prevention-based security approach, immediately blocking detected malicious activities and protecting your applications and networks.

Strata VM-Series, CN-Series, and Cloud NGFWs are powered by inline learning and informed by insights from over 15 trillion daily transactions processed by Palo Alto Networks. Together with AWS, they provide always-on security and automated threat response for your business needs.

- **Protect** against advanced and evolving threats on VMs, containers, and baremetal in real time with full traffic visibility and granular control.
- **Enforce trust zones** and securely allow traffic between microsegments.
- **Implement consistent network security** between on-premises, private, and public cloud deployments.
- **Dynamically scale** security to accommodate fluctuating traffic without compromising DevOps agility.
- **Automate and centralize** management of all Palo Alto Networks NGFWs.
- **Integrate** with your application developers' workflows without compromising DevOps deployment and security.

RETURN TO MENU

Advanced Network Protection and Threat Prevention

How It Works

Automatically updates dynamic address groups and security policies on Palo Alto Networks' Strata Next-Generation Firewalls – including CN-Series Containerized, VM-Series Virtual, and Cloud NGFWs – based on threat feeds from AWS Security Hub and AWS GuardDuty.

Solution Component Highlights

VM-Series Virtual Next-Generation Firewall: All-in-one virtual security appliance

- **Stop zero-day** attacks and lateral movement of threats with in-depth security for inbound and outbound traffic.
- **Deploy VM-Series virtual firewalls anywhere** while maintaining consistent visibility and logging across everything.
- **Protect applications in all use cases** – whether lifting and shifting existing apps to the cloud or developing new, cloud-native applications.

Cloud Next-Generation Firewall: Industry's first machine learning- powered NGFW

- **Provide protection within Amazon Virtual Private Clouds** (VPC) from known, unknown, and zero-day cyberthreats.
- **Meet critical compliance standards** while adhering to zero-trust security models.

CN-Series Containerized Next-Generation Firewall: Runtime security for Kubernetes (K8)

- **Empower DevOps teams** to secure containers effectively.
- **Gain Layer 7 visibility and context** inside Kubernetes clusters at the application and namespaces level.
- **Ensure frictionless CI/CD pipeline deployment** while delivering extraordinary runtime network protection.

Security Hub: Cloud security posture management (CSPM) service

- **Automates security best practice checks** and detects deviations with a single click.
- **Aggregates security alerts** from AWS and partner services into a single place and a standardized format.
- **Accelerates mean time to resolution** with automated response and remediation actions.

GuardDuty: Intelligent threat detection service

- **Continuously monitors** AWS accounts and workloads for malicious activity.
- **Identifies and prioritizes** potential threats.
- **Delivers detailed security findings** for visibility and remediation.

Case Study

Verge Health

Challenge

Verge Health™ provides healthcare organizations with a systematic approach to managing governance, risk, and compliance through a SaaS-based offering hosted by AWS. Because the company handles sensitive protected health information (PHI), it requires the highest level of network security to prevent cyberattacks.

Solution

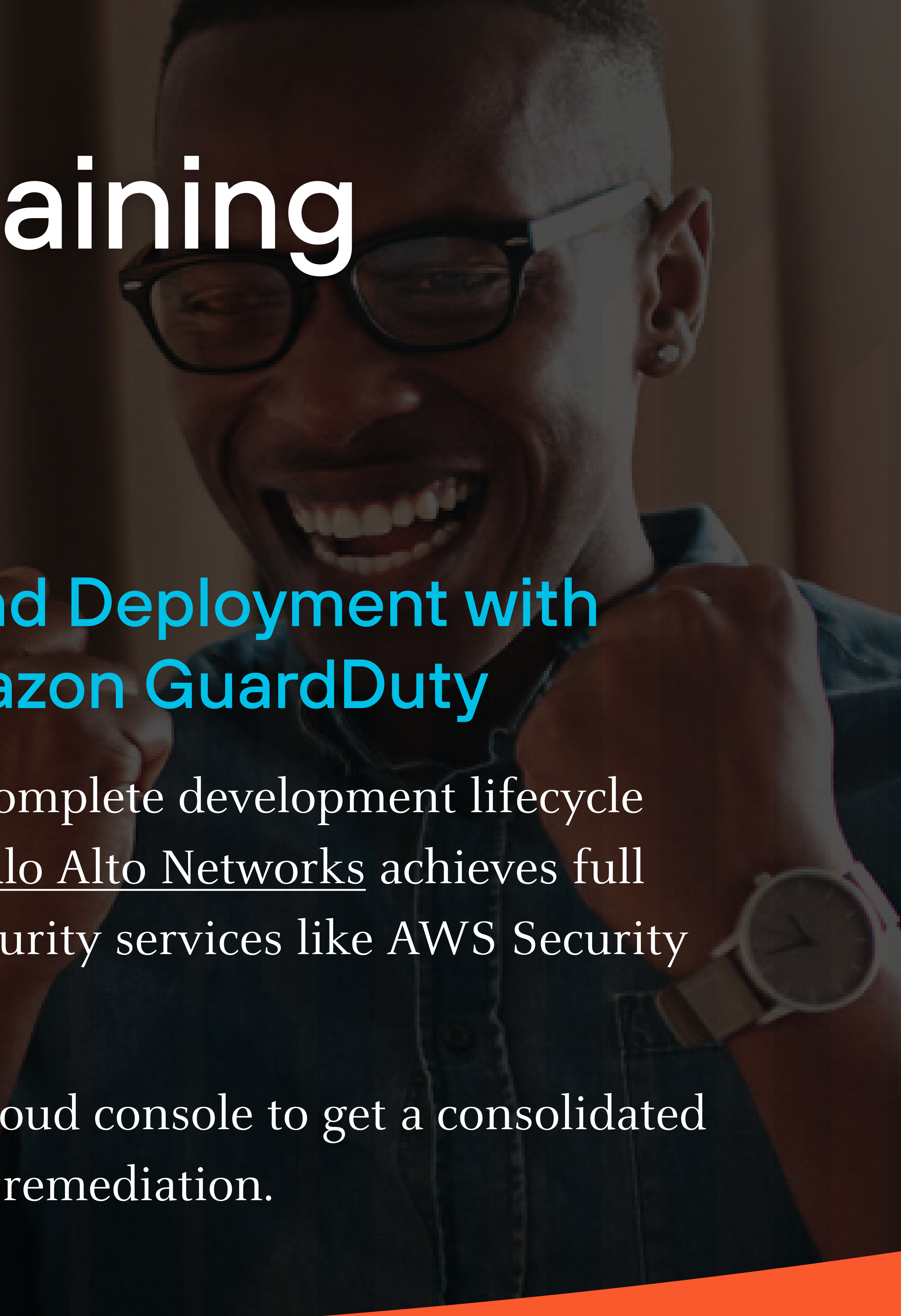
By deploying VM-Series virtual firewalls with Threat Prevention, URL Filtering, and WildFire® services on AWS, Verge Health is able to intelligently prevent breaches globally and assure sensitive data and vital risk management services are safe, compliant, and available 24/7.

Results

Verge Health revealed previously unrecognized threats and reduced unnecessary communications by 30%. The healthcare risk management provider reduced platform failover time from up to 60 seconds to less than one second.

Get started with Palo Alto Networks solutions on AWS. Visit the AWS Marketplace or APN Partner website to start a free trial of our products today.

Securing Applications and Maintaining Compliance from Code to Cloud



Developers and DevOps teams are rapidly deploying applications to AWS. However, the dynamic nature of cloud environments can obscure security visibility, making it a challenge to ensure that new deployments are compliant and protected.

Together, Palo Alto Networks and AWS can improve visibility and eliminate security challenges by helping security and DevOps teams monitor to prevent risks earlier in the lifecycle and ensure runtime compliance.

Secure Cloud-Native App Development and Deployment with Prisma Cloud, AWS Security Hub, and Amazon GuardDuty

Palo Alto Networks and AWS are fully integrated to provide complete development lifecycle security and full-stack runtime protection. Prisma Cloud by Palo Alto Networks achieves full environment coverage by ingesting security findings from security services like AWS Security Hub and Amazon GuardDuty to add to our own findings.

SOC teams can use either AWS Security Hub or the Prisma Cloud console to get a consolidated view of all environment telemetry and indicators and enforce remediation.

- **Gain near real-time visibility** and immediate risk clarity with continuous monitoring of all AWS environments and a comprehensive view of security and compliance.
- **Streamline compliance and establish API-driven guardrails** with **over** 900 pre-built policy checks specifically for AWS.
- **Stop breaches** by detecting misconfigurations, compliance violations, and network security risks early and fixing vulnerabilities at the source.
- **Secure the DevSecOps lifecycle** from Build to Deploy to Run across public and private clouds.

Securing Applications and Maintaining Compliance from Code to Cloud

How It Works

Prisma Cloud ingests data from a variety of AWS services, including information on configurations, user activity, network traffic, host vulnerabilities, and threats. Palo Alto Networks machine learning (ML) and AI algorithms enrich captured telemetry with context, based on behavior monitored in the cloud. The Prisma Cloud console provides security alerts and highly contextual threat information back to AWS Security Hub.

Solution Component Highlights

Prisma Cloud

- **Comprehensive cloud-native application protection platform** (CNAPP) for multi- and hybrid-cloud environments.
- **Protects code, infrastructure, applications, workloads and APIs, networks, and data** with a consolidated platform approach that scales and automates.
- **Supports wide-ranging cloud security needs**, including code security, security posture management, workload protection, infrastructure entitlement management, and data and AI security.

Security Hub: Cloud security posture management (CSPM) service

- **Automates security best practice checks** and detects deviations with a single click.
- **Aggregates security alerts** from AWS and partner services into a single place and a standardized format.
- **Accelerates mean time to resolution** with automated response and remediation actions.

GuardDuty: Intelligent threat detection service

- **Continuously monitors** AWS accounts and workloads for malicious activity.
- **Identifies and prioritizes** potential threats.
- **Delivers detailed security findings** for visibility and remediation.

Prisma Cloud Creates Beneficial Outcomes Across the Enterprise

Security (CISO, AppSec, IT Security)

27% reduced likelihood of significant breach

- Cloud Security Posture Management
- Cloud Workload Protection
- Code Security
- Cloud Identity Security
- Cloud Network Security

Governance (CIO, PM, Business Analyst)

80% reduced time configuring policies

- Cloud-native compatibility
- Single SKU procurement
- Flexible cloud credits
- Accelerated cloud productivity

People (HR, People Manager)

90% reduced time for compliance reporting

- Pre-built policies and capabilities
- Every industry use case
- Persona-based operation guides
- Single-click reporting and auditing

Platform (CTO, IT, Solution Architect)

60% reduced DevOps time addressing vulnerabilities

- Integrated Cloud Native Security Platform (CNSP)
- Cloud Native Application Protection Platform (CNAPP)
- Full lifecycle, full stack, across multiple AWS accounts
- Enterprise-grade cloud security at scale
- DevOps-native "Shift Left" security
- Purpose-built platform for AWS

Operations (IT Operations, IT Support)

44% reduced time to investigate incidents

- Single pane of glass console
- Asset discovery
- CI/CD integrated workflows
- Infrastructure-as-code (IaC) guardrails
- Automated security with machine-learning
- AWS Control Tower integration

Business (Business, Finance, Budget, Strategy)

Proven 276% ROI (3 years)*

*Total Economic Impact^{TM} of Prisma Cloud

Prisma Cloud is a Leader in Cloud Security

Cloud Workload Protection
LEADER
Cloud Workload Security Wave
FORRESTER

Cloud-Native App Protection
LEADER
Global CNAPP Radar
FROST & SULLIVAN

DevSecOps
LEADER & FAST MOVER
Developer Security Tools Radar
GIGAOM

Cloud Security
LEADER & FAST MOVER
Policy as Code Radar
GIGAOM

Vulnerability Management
LEADER & OUTPERFORMER
Vulnerability Management Radar
GIGAOM

Cloud Security Posture Mgmt
LEADER & OUTPERFORMER
CSPM Radar
GIGAOM

What Prisma Cloud Customers Say:

"Best tool in the market."

★★★★★ **5 stars out of 5** Full review

"Seamless integration with AWS, super easy to setup, ability to enforce policies both on block and detection, easy to integrate with ticketing systems (SNOW, JIRA, etc.)."

- Director,
  Cyber Security And Compliance

"Mind blowing capabilities."

★★★★★ **5 stars out of 5** Full review

"From deployment to customer support and service, we have been delighted. **Feature set is endless.** By far one of the best tools."

- Analyst,
  IT Security and Risk Management

paloalto NETWORKS | aws

Case Study

Ame Digital

Challenge

- Needed to scale quickly due to rapid growth
- At the same time, need to release customer products more quickly
- All within the highly regulated financial market

Solution

Centralized policy management and security visibility through:

- Prisma Cloud running on Amazon Elastic Computer Cloud (Amazon EC2)
- Palo Alto Networks Strata firewalls for secure access service edge

Results

- Ame now manages security in a continuous delivery environment
- Faster time to market for new products due to reduced app development time
- Teams have full visibility into software and workloads, resulting in quicker detection and response to security issues

Ame, a fintech and mobile business platform, has been revolutionizing the way people handle money. App downloads have surpassed 17 million, allowing customers to pay for their purchases with the app on all websites, in 3 million establishments and in 1,707 Americanas retail stores across the country.

See why Prisma Cloud is a Leader in the Forrester Wave: Cloud Workload Security Q1 2024

Automating and Accelerating Response for Security Incidents and Forensic Use Cases

Security teams are drowning in alerts and endless manual security tasks. They also waste precious time pivoting across consoles to collect data, determine false positives, and take remedial actions.

Palo Alto Networks and AWS empower you to replace manual, piecemeal responses with intelligent, automated operations.

Orchestrate, Simplify, and Enhance Security Operations with Cortex XSOAR and Security Hub

Palo Alto Networks Cortex XSOAR and AWS Security Hub help SOC teams keep pace with overwhelming volumes of alerts while accelerating incident response.

- **Centralize cloud security**, ensure consistent operations, and eliminate the need to pivot among consoles.
- **Speed incident investigation and remediation** with hundreds of out-of-the-box playbooks that automate 95% of response actions that typically require human review.
- **Free SOC teams to focus on high-fidelity** malicious incidents and breaches that require manual intervention.
- **Reduce mean time to respond (MTTR)** from hours to minutes.

Automating and Accelerating Response for Security Incidents and Forensic Use Cases

How It Works

Cortex XSOAR ingests alerts across multiple sources – such as GuardDuty, Amazon Inspector, and third-party providers, as well as Prisma Cloud – and executes standardized playbooks.

SOC teams have full visibility into what playbooks were executed and what incident triggered the execution, and can measure progress against the occurrence of incidents.

Solution Component Highlights

Cortex XSOAR

- **A comprehensive security orchestration, automation, and response** (SOAR) platform provides centralized visibility and makes it easy to parse, manage, and act on threat intelligence.
- **Stops breaches** with AI-driven threat prevention, detection, and response across cloud, endpoint, network, and third-party assets.
- **Leverage AWS Identity and Access Management roles** from within Cortex XSOAR, attach privileges and users, and execute automated actions without the need for credential storage and transfer.

Security Hub: Cloud security posture management (CSPM) service

- **Automates security best practice checks** and detects deviations with a single click.
- **Aggregates security alerts** from AWS and partner services into a single place and a standardized format.
- **Accelerates mean time to resolution** with automated response and remediation actions.

Contact us

Unify your cloud security across the entire application lifecycle. Request your Prisma Cloud demo to see how!

Extend your threat prevention to AWS with our best-in-class NGFW. Start your free trial today!