Cloud security that strikes the perfect chord

How Palo Alto Networks and AWS work in concert to harmonize your cloud security

Table of Contents

Out-of-tune services are open to vulnerabilities

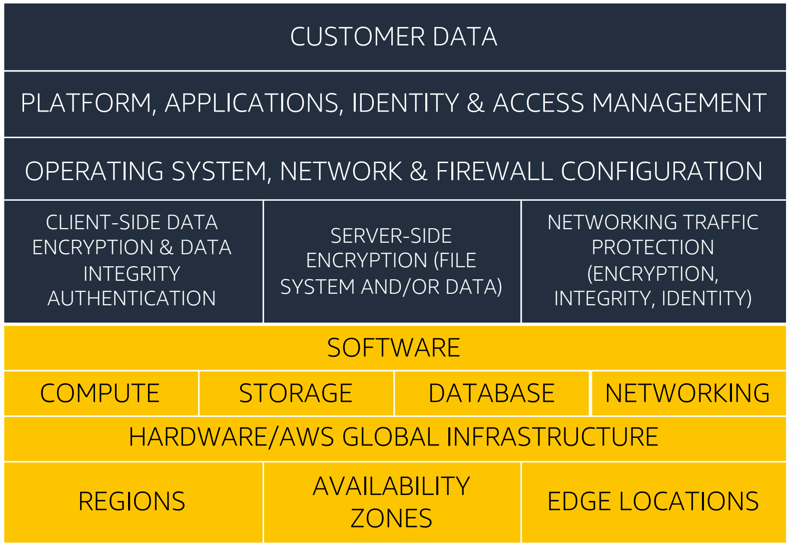
It can be hard to synchronize your security instruments to detect threats and automatically respond to attacks

For your security to sing, all the cloud services in your orchestra have to harmonize. But with ever-changing cloud environments, playing conductor isn't that simple. It can be tough to see all your dynamic entities clearly, let alone protect them from attacks.

Security services from Amazon Web Services (AWS) paired with products from Palo Alto Networks help you harmonize your cloud environments, accounts, and pipelines to keep them working together for comprehensive security. Through AWS Security Hub you can view, organize, and prioritize security findings from monitoring services like Amazon GuardDuty, while Palo Alto Networks provides complete security orchestration to unify your complex AWS environments and automate responses.

Customers have their choice of security configurations **IN** the Cloud

AWS is responsible for the security **OF** the Cloud



CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Palo Alto Networks helps customers enhance security in the cloud

aws partner network

Advanced
Technology Partner

Security Competency
Networking Competency
Containers Competency
Marketplace Seller
Public Sector Partner

AWS Security Hub delivers a comprehensive view of your AWS accounts

- Aggregate alert data from your AWS workloads and monitoring services like Amazon GuardDuty
- Evaluate against compliance and AWS security standards and best practices
- Investigate findings and take remediation action

Palo Alto Networks unifies your complex environments for automated, scalable cloud security

- Monitor constantly changing cloud resources for holistic protection
- Embed in-line network security and threat prevention into your AWS application workflow
- Orchestrate cloud security monitoring and automate response actions through playbooks

Palo Alto Networks plus AWS provide complete orchestration for in-tune security

Automatically detect then respond to security incidents, and remove vulnerability gaps

Prisma Cloud, VM-Series virtual next-generation firewalls, and Cortex XSOAR from Palo Alto Networks tightly integrate with AWS Security Hub and Amazon GuardDuty for a single orchestration platform where you can manage AWS workloads and automate responses to security incidents.

Prisma Cloud

Prisma Cloud—monitoring service with visualizations to track AWS resources

Monitor constantly changing cloud resources and integrate with Security Hub and GuardDuty for a holistic approach to protection.

VM-Series

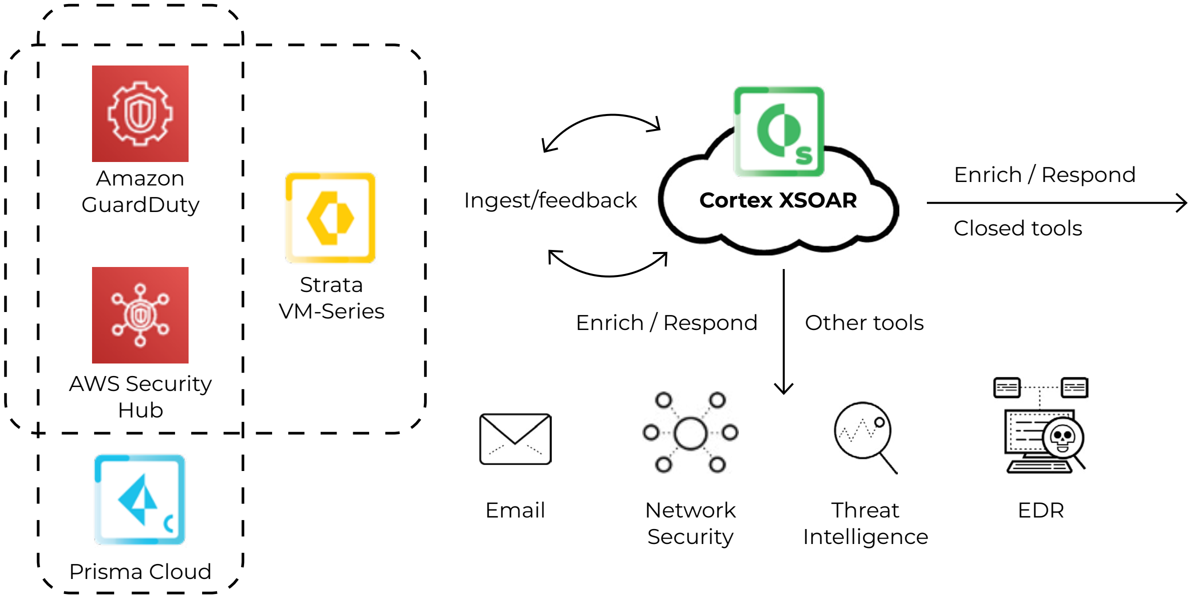
VM-Series—virtual next-generation firewalls to protect your AWS workloads

Block detected malicious activity by automatically updating security policies on VM-Series virtual firewalls based on threat feeds from Security Hub and GuardDuty.

Cortex XSOAR

Cortex XSOAR—orchestration platform for standardized, scalable security

Ingest alerts from Security Hub, GuardDuty, and Prisma Cloud, then execute automatable playbooks that coordinate across your entire system for repeatable and scalable incident responses.



Full lifecycle, full stack security and compliance with Prisma Cloud

Prisma Cloud is a comprehensive cloud native security platform with the industry's broadest security and compliance coverage—for applications, data, and the entire cloud native technology stack—throughout the development lifecycle and across multi- and hybrid cloud environments. Prisma Cloud integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively and accelerate cloud native application development and deployment securely.

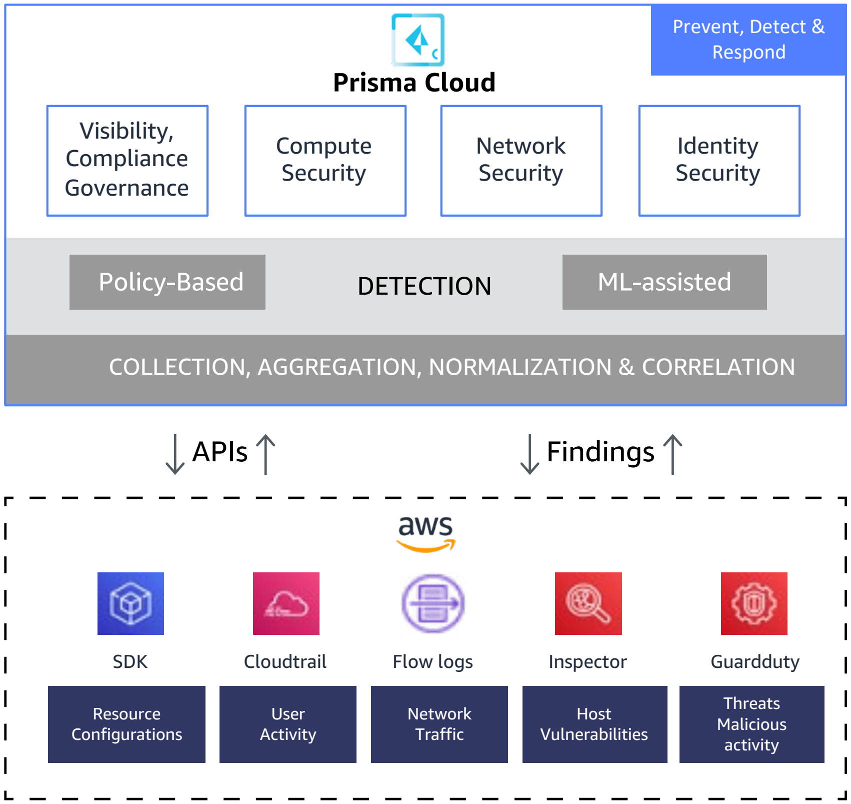
Expand compliance checks and fill in additional context to alerts

Prisma Cloud runs more than 500 compliance checks as part of its continuous monitoring of AWS resources. It imports resource configurations, AWS CloudTrail, VPC flow logs data, and findings from GuardDuty and host vulnerabilities from Amazon Inspector to detect misconfigurations, compliance violations, network security risks, and anomalous user activity, then feeds those findings into Security Hub to see it all in one place. By correlating log data with findings from GuardDuty, Prisma Cloud provides the additional context around alerts.

Prisma Cloud automatically detects anomalies in user behavior across your entire AWS environment, establishing behavior baselines and flagging any deviations. You can also filter common vulnerabilities and exposures (CVE) from Amazon Inspector and GuardDuty, then prioritize remediation findings. For example, you can show all Amazon Elastic Compute Cloud (Amazon EC2) instances with open security groups that have unpatched CVEs and are receiving malicious internet traffic.

Benefits of Prisma Cloud on AWS

- Add additional context to findings from Inspector and GuardDuty, then correlate findings with AWS resource configs, AWS CloudTrail, and network traffic
- Achieve a 360-degree view of AWS resources (such as EC2 instances), config info, network settings, network traffic, vulnerabilities from Inspector, GuardDuty findings, user activity, and audit history, all through a single pane of glass
- Filter CVEs from Inspector and GuardDuty findings, and prioritize remediation findings



Virtual firewalls with VM-Series

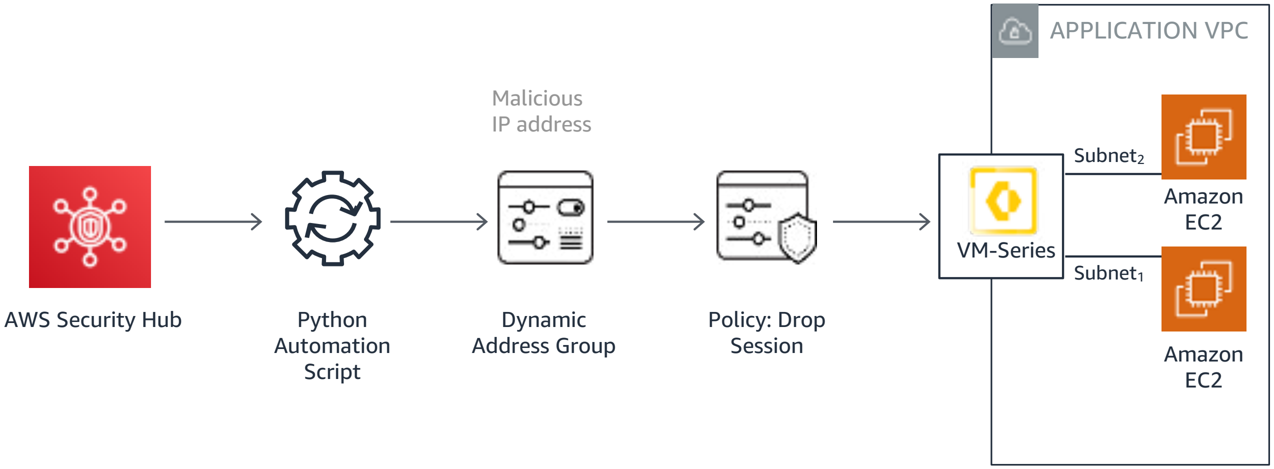
VM-Series virtual firewalls augment native AWS security controls, such as security groups, with capabilities like layer 7 traffic inspection, IPS, URL filtering, and cloud sandboxing that allow you to embrace a prevention-based approach to protecting your AWS-hosted applications and data. Automation and centralized management features enable you to embed next-generation security in your AWS application workflow, allowing security to keep pace with development.

VM-Series' flexible policy model enables automatic threat response

The VM-Series integrations with GuardDuty® and Security Hub use an AWS Lambda function to collect threat findings such as malicious IP addresses. The Lambda function feeds the malicious IP address findings to the VM-Series, using the XML API to create a Dynamic Address Group that can be used to define within a security policy to block any activity emanating from the IP address in the group. When Amazon GuardDuty updates the list of malicious IP addresses, the Dynamic Address Group and security policy are automatically updated without administrative intervention.

Benefits of VM-Series on AWS

- Create dynamic address groups within security policies for automated responses
- Prevent known and unknown threats with virtual firewalls
- Segment and whitelist applications for security and compliance
- Prevent data exfiltration with traffic content inspection and URL filtering



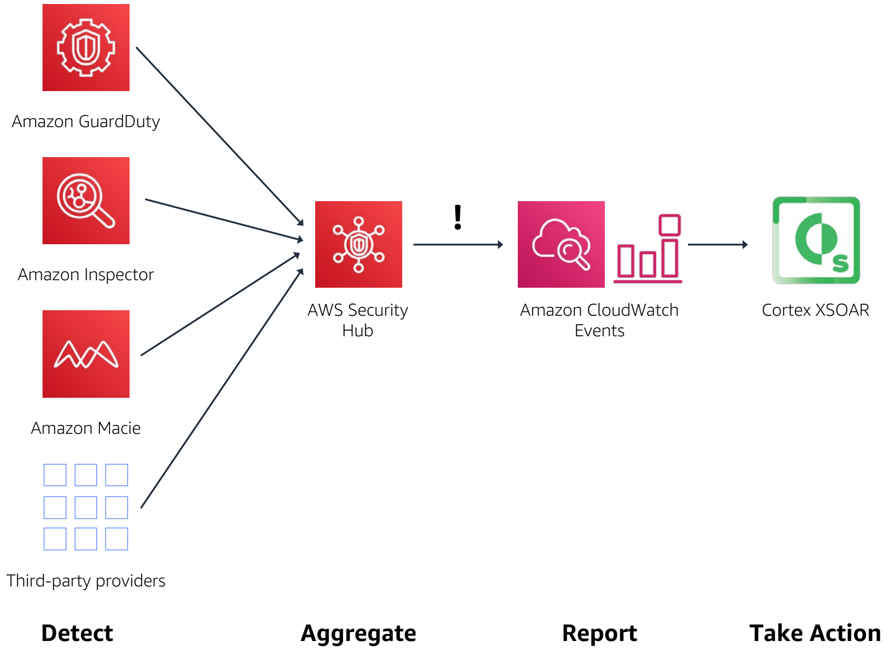
Unified security orchestration with Cortex XSOAR

Rather than disparate, siloed environments, Cortex XSOAR (security, orchestration, automation, and response) integrates with Security Hub to provide unified, automated security intelligence and incident response across your infrastructure. One connected platform enables orchestration across multiple cloud security products and environments for faster incident response and improved team productivity.

Orchestrate and automate security incident response

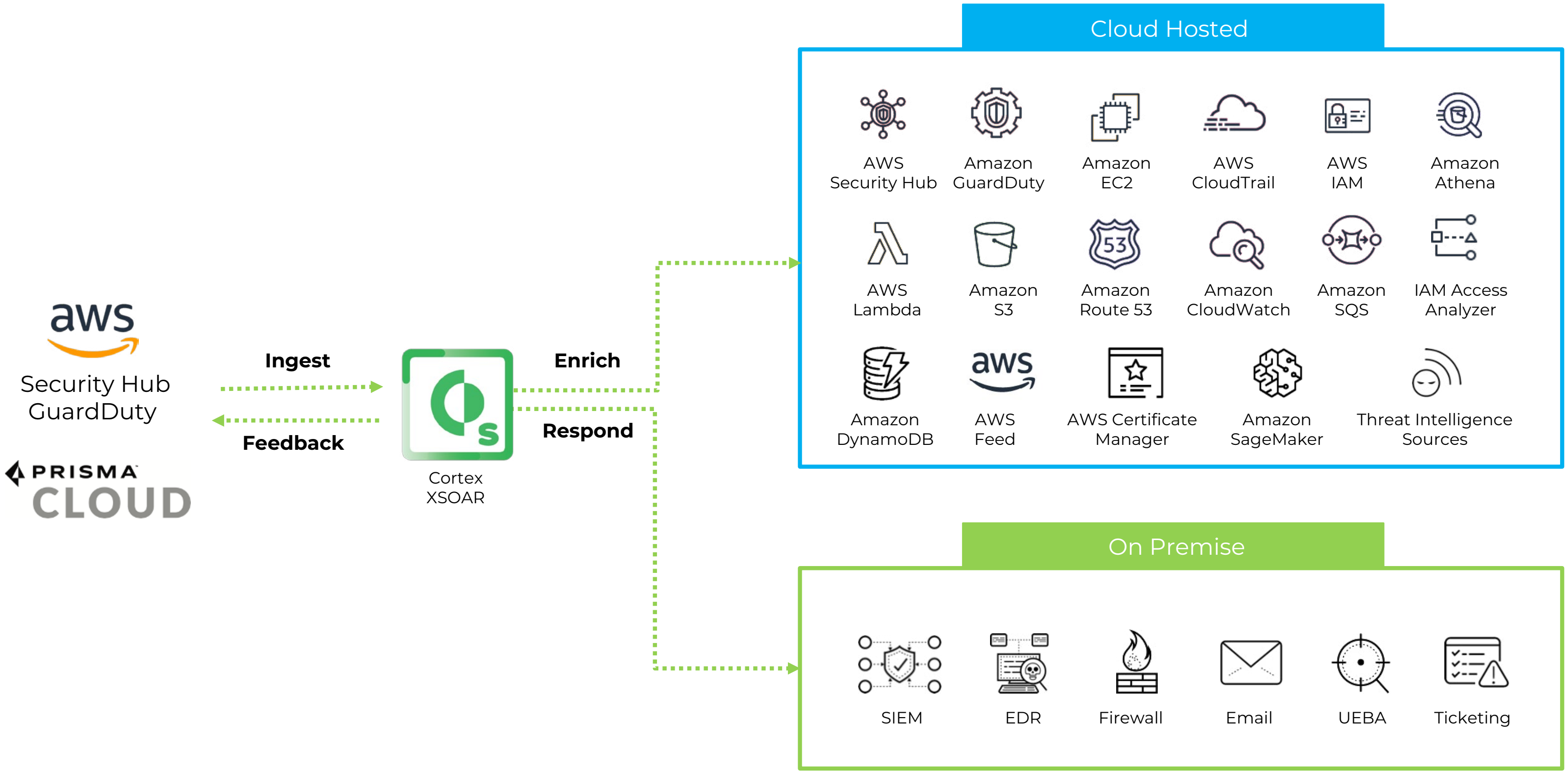
Cortex XSOAR ingests alerts from Security Hub, GuardDuty, and Prisma Cloud, then triggers automated playbooks in response. Playbooks are task-based workflows that can be fully or partially automated to speed and scale incident response. They automate repetitive data enrichment and remediation of cloud security alerts, eliminating the need for an analyst to manually perform such tasks across multiple consoles. For example, a playbook can enrich alerts with data from threat intelligence sources, query GuardDuty for IP sets, use Amazon Route 53 for domain information, and retrieve message queues from Amazon Simple Queue Service before updating bucket policies on Amazon Simple Storage Service (Amazon S3) and terminating instances from Amazon EC2 as response actions.

In addition to automating response actions, Cortex XSOAR also enables analysts to perform unstructured investigations by reviewing rich incident data, running AWS commands in real time, and collaborating with team members to resolve more complex cases. And with Cortex XSOAR's extensive product integrations, the same playbooks can be used to coordinate response across SecOps, DevOps and IT functions, standardizing incident response across cloud and on-premises networks for end-to-end incident lifecycle management.



Benefits of Cortex XSOAR on AWS

- Orchestrate security incident responses and case management through one system
- Trigger automated playbooks for coordinated responses across products and teams
- Leverage hundreds of Cortex XSOAR product integrations to add further context to Security Hub findings and standardize incident response across hybrid environments



Gotta catch 'em all (security threats, that is)

The Pokémon Company International found a comprehensive orchestration platform in Cortex XSOAR, using additional compliance checks from Prisma Cloud, plus integrations with AWS Security Hub and Amazon GuardDuty.

Disparate security tools slow down team and make it difficult to catch malicious activity

As a multi-national company that does a lot of business with third-party vendors, Pokémon's infrastructure is a complex ecosystem of products and services. It was hard for the security team to understand specific vulnerabilities across the entire system and keep pace with as the company's cloud environments kept changing. Bringing in more security tools helped, but it added to the complexity of their stack and made it difficult to harmonize the various players. Often times it felt like the security team was just putting out fires and wasting time jumping between different systems.

New level of visibility plus automated responses speed time to action

With the Prisma Cloud integration, Pokémon was able to go from 15,000 different alerts and misconfigurations across all their accounts down to 2,000 alerts within 6 months, and going down every day.

Using Cortex XSOAR, Pokémon was able to navigate its complex ecosystem and remain agile by seamlessly pivoting between platforms. The modularity of the orchestration platform helped the team quickly onboard new technology.

“Cortex XSOAR's process modularity has helped us stay agile as we onboard new technologies in a fast-moving environment. Cortex XSOAR is really the constant sheet music that keeps our security orchestra going.”

— Sean Hastings,
Senior Information Security Analyst,
The Pokémon Company International

“Working with AWS and Prisma together has made my job incredibly easy...they integrate together so seamlessly.”

— Jacob Bornemann,
Senior Security Engineer,
The Pokémon Company International

Harmonize your cloud security

Visit the AWS Marketplace and the Palo Alto Networks website to learn how you can deploy innovative cybersecurity across your AWS workloads.