Advanced Security & Analytics Environment

Automate the deployment of an enterprise-class security and analytics environment on AWS

Technology challenges

As the rapid adoption of Amazon Web Services (AWS) for enterprise workloads increases, organizations are realizing the critical importance of their role in the shared responsibility model for security. The shared responsibility model requires the customer to be responsible for protecting their applications and data on AWS. Attackers can target applications and data regardless of where they are located, so robust protection policies are warranted across the entire enterprise. These very practices can inadvertently stifle business agility and innovation, so security must be a complementary strategy implemented from the beginning of cloud adoption.

In the sprint to realize the many benefits of AWS, your organization must address a set of common technology challenges to:

- Position security as an enabler to business goals and technology innovations rather than a bottleneck
- Quickly gain visibility into all devices and applications running in your data center or cloud environment
- Identify anomalous network traffic to inform and prioritize security investigations
- Automate policy changes and updates based on malicious activity
- Aggregate threat intelligence feeds into one place and make them actionable.

Industry trends

Cloud adoption

Accelerated cloud adoption, with AWS becoming an extension of on-premises data centers or the main destination for production workloads.

Physical and virtual network attacks

Attackers will target applications and data, regardless of whether they are on-premises or AWS.

Simplifying security deployment

Organizations are seeking automated solutions that simplify the secure deployment of their cloud environments.

Solution overview

To protect against malware and other attacks, your organization can take a hybrid approach to deploying an environment on AWS that leverages and expands the best security practices of your data center. An enterprise-class security and analytics environment can deliver complete visibility into application traffic, which can help security teams by:

Enforcing policy-based control and prevention of known and unknown threats

Identifying the root cause and making informed decisions on how to remediate an issue

Deploying a security and analytics environment that is consistent from the data center to the cloud is an ideal approach to prevent cyber threats that may target your organization's applications and data on the cloud. AWS enables users to operate at a rapid and dynamic pace, leveraging its agility and flexibility to create, iterate, and deploy. The brisk introduction of new features, capabilities, and support on AWS can tax the security team's ability to keep pace with policy updates. An ideal solution is one where security can keep pace with the advance of cloud benefits through visibility and automation.

Get end-to-end security visibility quickly with AWS, Palo Alto Networks, and Splunk

AWS, Palo Alto Networks, and Splunk have collaborated to deliver a solution that automates the deployment of enterprise-class security and analytics environments on AWS that can be integrated into the users' workflow, ensuring that security keeps pace with the speed of the cloud. This package helps Palo Alto Networks and Splunk users securely migrate to the cloud, leveraging their existing investments, skills, and domain knowledge, while accelerating their cloud adoption and extending consistent policies, practices, and processes on AWS.

Utilizing the breadth and depth of AWS resources, this solution implements:

- Palo Alto Networks VM-Series next generation firewall: Supporting on-premises, cloud, and hybrid deployments, the VM-Series analyzes all traffic to provide full visibility into applications across all ports, protecting your workloads with threat prevention policies.
- Splunk Enterprise: Monitors and analyzes machine data from any source to deliver Operational Intelligence to enhance your IT, security, and business performance.
- Splunk enables security analysts to take a proactive stance to investigation and response – from monitoring and triage, verifying and escalating, to responding to a breach or infection.

Once deployed, the VM-Series will protect your workloads from cyberattacks emanating from either the network or the web, while Splunk Enterprise provides visibility, analytics, and reporting across cloud, on-premises, and hybrid environments.

Visibility enables faster remediation

This collaborative solution is run from a "single pane of glass" and presents contextual views across all of your environments – from the on-premises data center to the cloud. With enhanced visibility, you can accelerate your security posture assessments, automate your responses to prevent threats, and expedite your investigations. And, when you need to remediate issues, you can streamline the process with orchestration enabled by the bi-directional integration.

Implementing this joint solution helps you migrate workloads to the cloud securely, confidently, and quickly, as well as:

- Gain end-to-end security visibility across cloud, on-premises, and hybrid environments
- Improve your security posture by proactively identifying, scoping, and analyzing security threats
- Enable faster investigation, breach analysis, incident response, and threat hunting
- Automate actions to mitigate risk to business continuity and reputation with faster security insight and decisions
- Deliver customized reporting, and long-term and historical trending

Benefits of Palo Alto Networks and Splunk integration on AWS

Threat Prevention

Monitor traffic, analyze content, determine app and prevent threats

Automated Deployment

AWS Quick Start enables automation, reducing manual overhead and errors

Leverage Existing Knowledge

Consistent user experience from the network to the cloud enables rapid migration to AWS

Operational Analytics and Reporting

Easy collection, analysis, and reporting on security data to make informed decisions

Security Posture Visibility

Complete, consistent view of apps, activity and data across on-premises and cloud

Partner Ecosystem

APN Partners with Security Competency designation ready to support you

Security Quick Start featuring Palo Alto Networks and Splunk

In concert with this solution, a Quick Start Guide is available to accelerate cloud adoption, customer education, and secure system implementation. The Quick Start demonstrates a cloud system with optional AWS architecture elements such as virtual private cloud (VPC), multiple Availability Zones, internet gateways, network address translation (NAT) gateways, webservers, numerous load balancers, and more.

Utilizing the AWS Quick Start guide for Palo Alto Networks and Splunk, users can rapidly perform the following steps:

- Deploy Palo Alto Networks VM-Series firewalls on AWS with an option for auto-scaling capabilities
- Automatically forward VM-Series firewall logs to Splunk Enterprise for analysis and reporting
- Deploy Splunk Enterprise and the Palo Alto Networks App for Splunk on AWS

Once the initial Palo Alto Networks VM-Series next generation firewall and Splunk Enterprise environment is deployed on AWS, you can re-use the Quick Start guide to expand deployments as use of AWS grows.

Both Quick Start components are available now in AWS Marketplace. The Palo Alto Networks VM-Series is available as a bundle, purchased directly from AWS Marketplace or via a bring your own license model (BYOL). Learn more here: VM-Series in AWS Marketplace and Splunk Enterprise platform in AWS Marketplace.