aws marketplace

SANS

Enabling a Security Investigation in AWS

Learn how to conduct an effective investigation in your Amazon Web Services (AWS) environment.

AWS Marketplace Introduction

With the ability to stand up a global cloud infrastructure with a few clicks, security organizations should review how they can adapt their processes and proactively decrease risk to their environment. This includes enabling investigations in the cloud. In this whitepaper, SANS analyst and senior instructor, Kyle Dickinson covers incident response plans in cloud environments, different services for conducting an investigation, how to perform a forensic image analysis, and how to review the communications related to an Amazon EC2 Instance.

Following on Kyle's perspective, AWS Marketplace will share how you can apply this process to your AWS environment with an introduction to relevant AWS services that can enhance your organization's security posture. Finally, Palo Alto Networks will be presented as a solution to help strengthen investigations in AWS.

You can access the featured Palo Alto Networks solutions in AWS Marketplace, including:

Palo Alto Networks Prisma Cloud

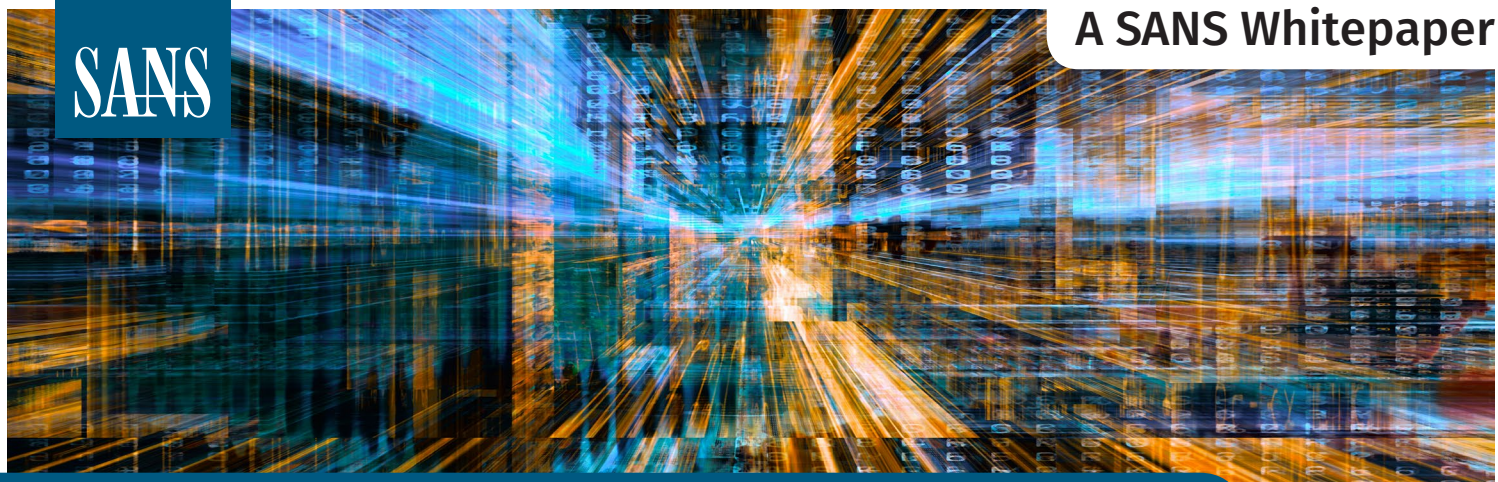
Demisto Enterprise AMI

Palo Alto Networks VM-Series Next-Generation Firewall

Palo Alto Networks Panorama

SANS

A SANS Whitepaper



How to Perform a Security Investigation in AWS

Written by **Kyle Dickinson**

October 2019

Sponsored by:

AWS Marketplace

Introduction

With the rapid growth of cloud service providers and the appeal, for organizations, of no longer having to manage their own data centers, more organizations are migrating to infrastructure-as-a-service (IaaS) providers. And the ability to stand up global infrastructure in a few clicks, or through a Continuous Integration and Continuous Deployment (CI/CD) pipeline, is drawing developers to cloud services as well.

What does this mean for incident response and forensics teams? We advocate for putting cloud-specific plans into place, because the technologies that enable investigations in the cloud differ from the ones for on premises, as do the levels of responsibility.

In this paper, we cover incident response plans in IaaS implementations, various services available that aid in conducting an investigation and the different components of an audit log. We also explore how to perform a forensic image analysis and how to review the communications that are coming to and from an EC2 instance.

Investigations vs. Incident Response

Investigations (or forensics), by definition is "... the process of using scientific knowledge for collecting, analyzing, and presenting evidence. ..."[1] Although investigations do not have to be aimed at providing evidence for a court case, understanding the process is important.

Investigations

The process of using scientific knowledge to collect, analyze and present evidence

Incident response

The process of using knowledge gained from an investigation to address a security incident

[1] US-Cert, "Computer Forensics," www.us-cert.gov/sites/default/files/publications/forensics.pdf

How Investigations Differ in Cloud-Based Environments

When performing an investigation in Amazon Web Services (AWS),[2] it's essential to understand that the investigation "playbook," or process, that an organization has for on-premises investigations is not exactly the same as for cloud-based investigations. Table 1 shows the differences between on-premises and cloud-based investigations.

The majority of the data sources and preparatory steps should be included in an incident response plan, which changes based on the type of cloud service model that is being consumed, such as software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS).

Table 1. On-Premises vs. Cloud-Based Investigations

Process	On-Premises	In the Cloud
Disk imaging	Physical drive connected to forensic workstation	Snapshot taken from Amazon EC2 instance, converted to volume and attached to forensic instance
Memory acquisition	Physical access to workstation as it's running	Private key or local user/trusted host access required
Network logging	PCAP in-line with netflow	Amazon VPC Traffic Mirroring

The Incident Response Process

Let's start by outlining the incident response process. An incident response is typically triggered by reports of "something happening" or notification that "something happened." Figure 1 shows the steps for responding using the SANS six-step incident response methodology.[3]

Figure 1. SANS Incident Response Steps

This methodology can easily be adapted to cloud-based environments. Here's a simple example:

- **Preparation**
  - What cloud service provider is being used?
  - What is the deployment model? (Public, hybrid, private?)
  - What is the cloud model? (SaaS, PaaS, IaaS?)
- **Identification**
  - Is there unusual activity in the audit logs?
  - Did something get misconfigured?
- **Containment**
  - Can we disable a user's access?
  - Can we isolate the VM or subnet?
  - How do we acquire an image?

[2] Because this paper is an exploration of performing investigations in AWS, it is important to talk about the tools available. The use of these examples is not an endorsement of any product or service.

[3] "Incident Handler's Handbook," December 2011, www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

- **Eradication**
  - Can we remove affected systems?
  - Can we remove/replace compromised credentials?
- **Recovery**
  - Can we restore normal business operations?
  - Is a business continuity plan available?
  - Did that plan need to be implemented?
- **Lessons Learned**
  - What gaps in coverage did we discover?
  - How do we close those gaps?

For cloud-based environments, the preceding methodology does not provide a complete incident response plan; however, we can see there may be some crossover from an on-premises plan, but it is not a one-for-one replacement when moving to the cloud.

Shared Responsibility Model

The shared responsibility model is a common method of determining where the responsibility shifts and which party is responsible for specific parts of the infrastructure. Depending on the type of service you're consuming, the provider can be responsible for some aspects or most aspects of the cloud.

Typically, with IaaS, the provider is responsible for security *of* the cloud, while our security teams are responsible for security *in* the cloud. When moving to IaaS providers, such as AWS, security teams must consider capabilities and services like the ones shown in Table 2.

Table 2. Key Capabilities and Services

Capability	AWS Service	Description
Compute	Amazon Elastic Cloud Compute (EC2)	Uses Amazon Machine Images (AMIs) to get started Multiple OS support Pay for what you use Next-gen Nitro infrastructure, created by AWS
Storage	Amazon Elastic Block Store (EBS), Amazon Simple Storage Service (S3), Amazon Elastic File System (EFS)	Amazon S3 offers multiple storage classes for multiple use cases. Amazon EBS is used for the "block device" or hard drive for Amazon EC2 instances. Amazon EFS is used for file sharing storage with two storage classes to choose from.
NetFlow	Amazon VPC Flow Logs, Amazon VPC Traffic Mirroring	Capture information of network traffic going in and out of a VPC
Auditing	AWS CloudTrail	User attribution data Log integrity can be enabled Can send data to an Amazon S3 bucket for storage/archival

Modern Security Controls

A typical on-premises environment may include the following tools that could be used in conducting incident response or investigations:

- Network intrusion detection systems (NIDS)
- Packet capture devices or network taps
- Vulnerability management scanners
- Endpoint detection
- Proxies and firewalls

When we move our investigations to a cloud-based environment, there are no decisions like "Where to ship my NIDS, network taps, vulnerability management, etc. ..." details. This is because we lose physical access to our infrastructure. That is okay. Instead of worrying about physical infrastructure, we can now focus on how to modernize our security controls.

AWS Marketplace allows security teams to stand up modern tooling that can come in the form of SaaS or AMIs and allow organizations to use the capabilities provided by AWS Partners to supplement the services that are available directly from AWS.

To better understand how to conduct an investigation within AWS, it is best that we understand the native services available to security practitioners so that we can understand what is and is not possible out of the box. This also strengthens the understanding of how to integrate the different capabilities that third-party tools offer.

Using AWS Services in Investigations

As part of the evidence gathering and analysis process, user attribution information tells us about the activity that a particular resource or user has performed. In the following sections, we discuss these activities as well as describe how to gain insight into network traffic.

Understanding User Activity

AWS CloudTrail gives security teams the who/what/when/where/how of the activity being investigated. This is the information that the auditing data teams need to better understand a user's actions. By default, AWS CloudTrail is enabled within the AWS Management Console. However, to ship these logs out of the account to a SIEM or log analysis tool, we need to set up a trail first. If we look at an example of an AWS CloudTrail log in the AWS Management Console, security teams have multiple ways to search for data:

- **Username—**Search by the user's name
- **Event name—**Search by a specific API call (e.g., `DeleteTrail`)
- **Resource type—**Search by an AWS service type (e.g., Amazon EC2 instance)
- **Resource name—**Search by a resource name (e.g., instance ID, ENI)
- **Event source—**Search results from specific AWS services
- **Event ID—**Search based on a unique ID for an AWS CloudTrail event
- **AWS access key—**Search by access key to show what was done in a single session

Figure 2 shows an example of an AWS CloudTrail event.

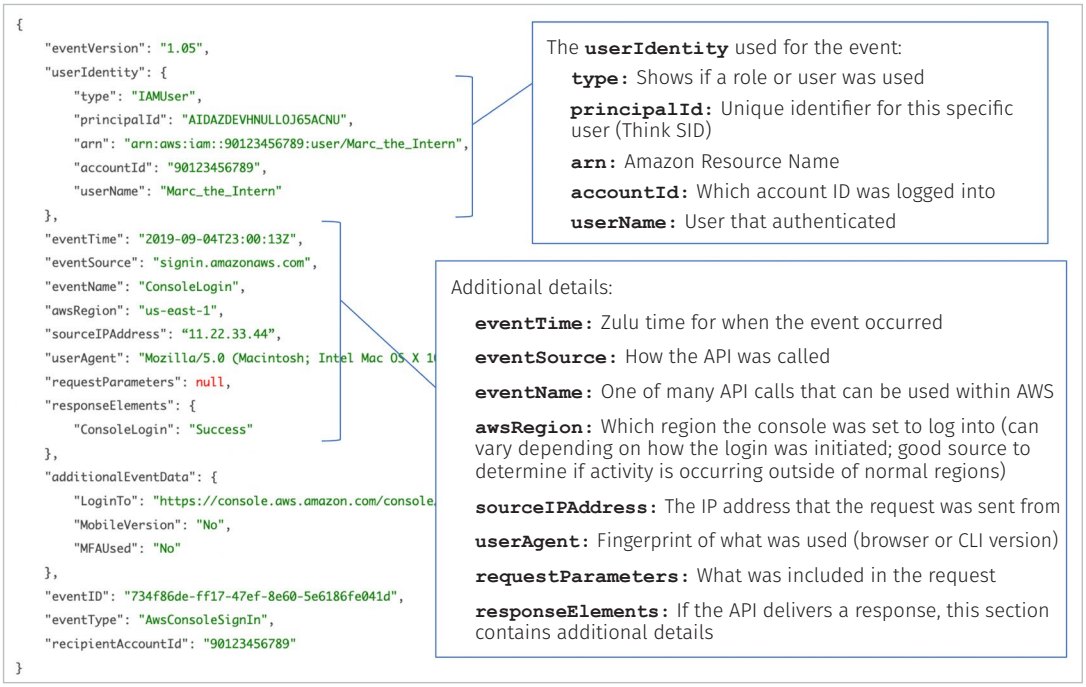


Figure 2. An AWS CloudTrail Event

By looking at the single AWS CloudTrail event shown in Figure 2, we can piece together that the user (Marc the intern) successfully logged into the AWS Management Console using Google Chrome, from IP address **`11.22.33.44`**, using a password with no multifactor authentication.

Keeping this information in mind, the majority of these fields remain persistent in each AWS CloudTrail event as we look to conduct an investigation. Having this data visualized and stored in a central location aids us significantly. Not only do we benefit from having the logfiles stored in a single location under the security team's control, but we have heightened security controls around this storage. Visualization allows investigators to demonstrate the activity and the location from which the activity was performed.

We *highly recommend* that you enable Amazon VPC Flow Logs for your VPCs; they are not enabled by default.

Gaining Visibility into Network Traffic

Amazon VPC Flow Logs provide visibility of network traffic going in and out of a VPC, also known as north-south traffic.

Looking at the structure of a VPC Flow Log, we see the details listed in Figure 3.

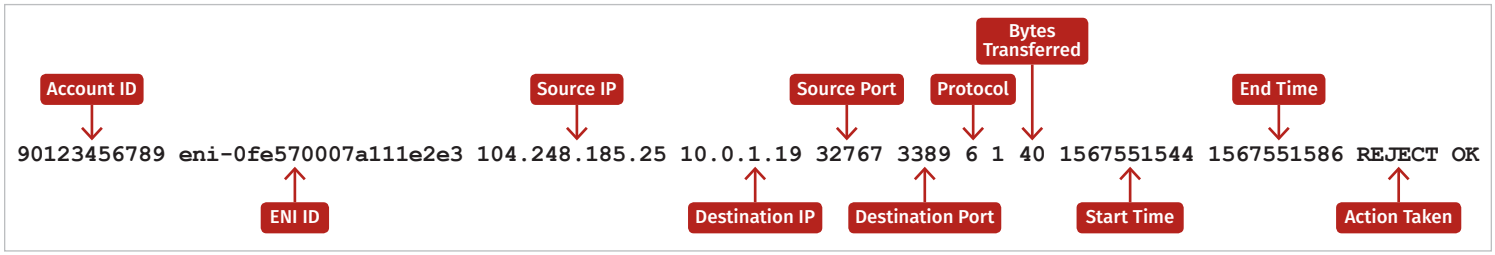


Figure 3. Structure of a VPC Flow Log

Amazon VPC Flow Logs give us a high-level view of network traffic. Exporting this data to a SIEM can add more context to Flow Logs by correlating threat intelligence data to the source or destination IP addresses to determine whether Amazon EC2 instances are communicating to potentially hostile hosts, such as those known from cryptomining or botnets.

Amazon VPC Traffic Mirroring is another method of obtaining insight into your network traffic that is available on AWS Nitro instances. What's handy about Amazon VPC Traffic Mirroring is that it's a "spanport-as-a-service" that enables security to send all north-south traffic to another instance for further analysis, if required, or integrate to another traffic-analysis toolset.

Forensic Acquisition

Should the incident require the security team to perform forensics on an Amazon EC2 instance, we need to take a snapshot of that instance and create a volume from that snapshot to share to a SIFT Forensic Workstation.

The following steps are an example of that process for a compromised implementation:

1. Create a security group that does not allow outbound traffic
2. Attach to compromised Amazon EC2 instance
3. Take snapshot of Amazon EC2 instance
4. Perform memory acquisition, if possible
5. Share snapshot with Security Account (if using one)

6. Create volume from snapshot
7. Attach volume to SIFT EC2 instance
8. Conduct forensics

It is possible to automate this process, which would provide faster data acquisition and response.

Use Case: An Investigation

Consider a case where the internal audit organization has approached the security organization. The audit organization requires an investigation of the user, Marc the Intern. It also requests that the security team acquire a forensic image, summarize that image and include a summary of the communications the instances had if Marc created any Amazon EC2 instances.

With running the Amazon EC2 instance, the security team wants to understand what this instance is doing so it can perform further analysis. After acquiring a snapshot, the team converts the snapshot to a volume so that it may attach the new volume that contains evidence to its analysis instance.

The team finds that Marc had access keys on this instance, which is not common in the organization's environment. What did Marc do with these keys? Looking back at the AWS CloudTrail logs, the team sees that this access key spun up another instance, in a region the organization doesn't currently leverage. Was Marc trying to fly under the radar? Or did he accidentally script this instance creation and forget to set a region?

The final requirement from the internal audit organization is to explore what this instance had been communicating to. When the security team looks at the instance configuration further, it sees that the Amazon VPC Flow Logs show that this instance was communicating to a remote host over ICMP—an abnormal behavior. Fortunately, the team requires Amazon VPC Traffic Mirroring to be enabled on new Amazon EC2 instances that are created. This instance's traffic has been captured, so the team is able to analyze what was going over ICMP.

After further exploration, the team can piece together a timeline of events for its report to the requesting audit organization.

Summary

When moving to the cloud, it's best to outline a new incident response plan and plan out how you are able to perform investigations within AWS so that you can validate that any obligation you may have as a security organization can be met as well as it once was in-house.

With the fast and dynamic pace of the cloud, and with adoption of these new services increasing every day, security organizations need to review how they can adapt their processes and stay ahead to proactively enable developers and decrease risk in the environment.

About the Author

Kyle Dickinson teaches SANS SEC545: Cloud Security Architecture and Operations and has contributed to the creation of other SANS courses. He is a cloud security architect for one of the largest privately held companies in the United States. As a strategic consultant in his organization, Kyle partners with businesses in various industries to better understand security and risks associated with cloud services. He has held many roles in IT, ranging from systems administration to network engineering and from endpoint architecture to incident response and forensic analysis. Kyle enjoys sharing information from his experiences of successes and failures.

Sponsor

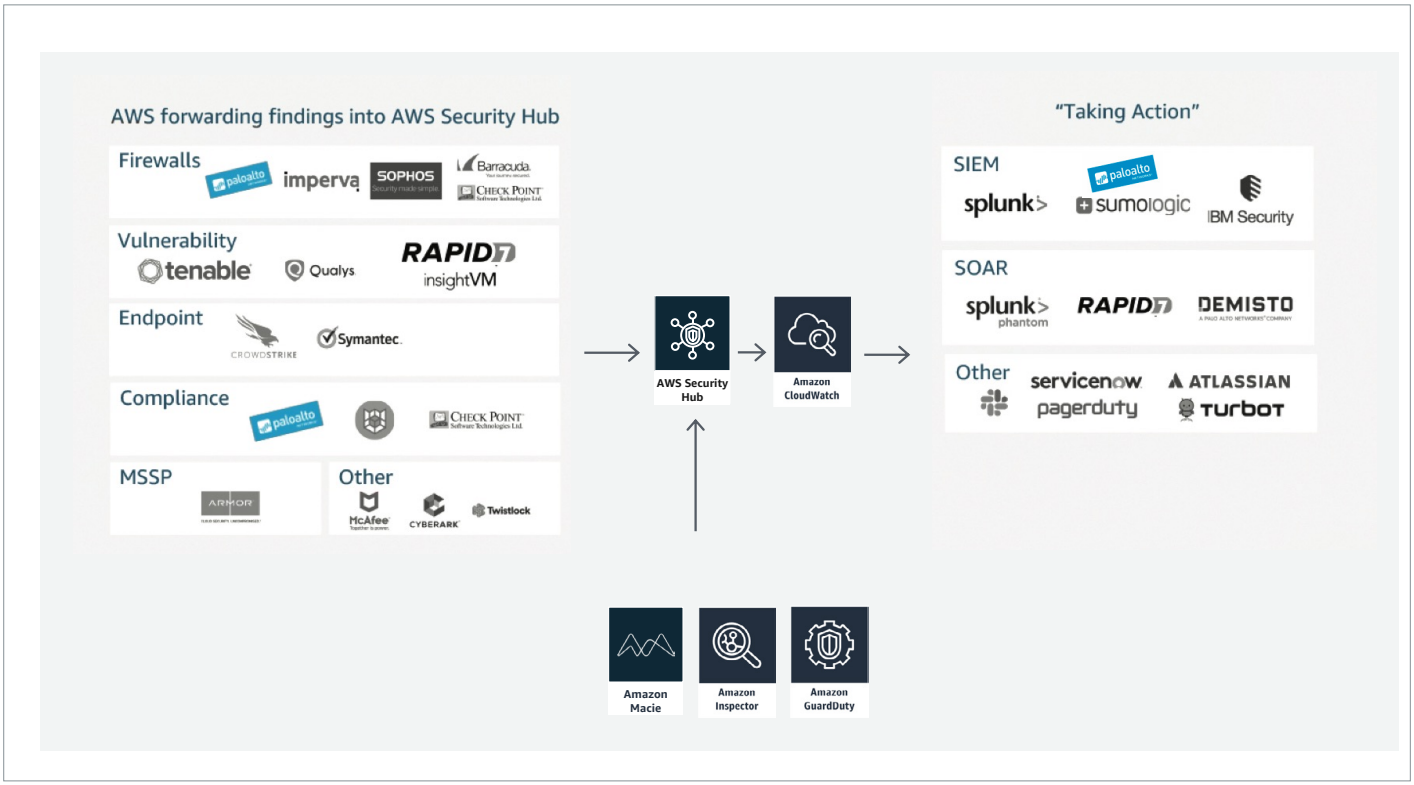
SANS would like to thank this paper's sponsor:

aws marketplace

aws marketplace

Strengthen your security investigations in AWS with third-party solutions.

As an organization moves to the cloud and adopts cloud-based solutions, it's important to outline a plan on how to conduct an investigation. A sound plan should include collaborative discussions about how to conduct cloud investigations in AWS, the incident response process, the shared responsibility model, and how investigations differ in cloud-based environments. Building on foundational services in AWS, such as AWS CloudTrail, Amazon CloudWatch, and AWS Security Hub, AWS Marketplace offers a breadth of solutions that enhance your security investigations. For instance, Palo Alto Networks' Prisma Cloud solution can be integrated with AWS Security Hub to provide enhanced intel for investigations. This additional information can enable customers to gain actionable insights, identify cloud threats, reduce risk, and remediate incidents.



How AWS customers are using Palo Alto Networks to secure their cloud environment

Palo Alto Networks offers multiple solutions that can both enable and enrich a security investigation. Specifically, customers are using these solutions to:

- **Expedite security investigations:** The ability to prioritize your investigations and incident responses is critical for developing a robust security posture. With Prisma Cloud, you can eliminate blind spots across your AWS environment, such as seeing publicly exposed EC2 instances that receive traffic from suspicious IP addresses. Incident response is also expedited by providing a visual threat map that provides context on risks.

- **Automate responses to security threats:** With Demisto's Security Orchestration, Automation, and Response (SOAR) platform, security teams can leverage integrations with external tools to automate repeatable steps at machine speed and improve investigation quality through collaboration, real-time command execution, and machine learning. This allows you to remove manual, repetitive tasks, potential human mistakes, and reduce mean time to detect and respond.

- **Remediate findings:** There are also other ways to remediate findings, such as using findings to further strengthen your firewalls, leveraging Palo Alto Network's VM-Series next-generation firewalls. This can be done directly or managed in one central location through Palo Alto Networks Panorama.

Why use AWS Marketplace?

AWS Marketplace simplifies software licensing and procurement by offering thousands of software listings from popular categories like Security, Networking, Storage, Business Intelligence, Machine Learning, Database, and DevOps. Organizations can leverage offerings from independent security software vendors in AWS Marketplace to secure applications, data, storage, networking, and more on AWS, and enable operational intelligence across their entire environment.

Customers can use 1-Click deployment to quickly launch pre-configured software and choose software solutions in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with software entitlement options such as hourly, monthly, annual, and multi-year.

AWS Marketplace is supported by a global team of security practitioners, solutions architects, product specialists, and other experts to help security teams connect with the software and resources needed to prioritize security operations in AWS.

aws marketplace

How to get started with security solutions in AWS Marketplace

Security teams are using AWS native services and seller solutions in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security posture. The following solutions can help you get started:

Browse Palo Alto Networks solutions on AWS Marketplace

Prisma Cloud Threat Defense and Compliance
Security and compliance in under 5 minutes without proxies or agents

Enterprise AMI
Security automation and response platform

VM-Series Next-Generation Firewall
Embed inline thread and data theft prevention into your application

Panorama
Central management for Firewalls, Wildfire Appliances, and Log Collectors