aws marketplace

SANS

Building an Endpoint Security Strategy in AWS

Gain visibility into your endpoints, current threat intelligence, compliance status, and more by leveraging AWS services and solutions in AWS Marketplace.

AWS Marketplace Introduction

Cloud endpoint security is increasingly relevant in today's business world, whether you are moving workloads to the cloud, integrating IoT, or adopting container technology. In this whitepaper, SANS analyst, Thomas Banasik, will discuss how endpoint security solutions in the cloud differ from on-premises practices and identify top considerations when migrating to Amazon Web Services (AWS). You will also learn the process of creating an endpoint security strategy that uses a defense-in-depth architecture to protect vital assets.

Following Thomas' perspective, AWS Marketplace will share how this process can be applied to your AWS Cloud environment with an introduction to relevant AWS services that can enhance your endpoint security. CrowdStrike, and their security solutions available in AWS Marketplace, will also be featured as an available option that can facilitate your endpoint security strategies and tactics.

Explore CrowdStrike's Falcon Endpoint Protection Premium in AWS Marketplace:

Falcon Endpoint Protection Premium

Bundled platform with managed services for full protection

SANS

A SANS Whitepaper

How to Build an Endpoint Security Strategy in AWS

Written by **Thomas J. Banasik**

June 2019

Sponsored by:

AWS Marketplace

Introduction

The nature of today's business is driving organizations away from traditional on-premises data centers and into distributed cloud computing environments, and with this move comes the challenge of securing endpoints in a cloud-dominated world.

Not long ago, endpoint security involved little more than signature-based antivirus, but endpoint security capabilities have evolved. Now we have endpoint detection and response (EDR), machine learning (ML), user and entity behavior analytics (UEBA) and data loss prevention (DLP) integrated suites. These cloud-based endpoint security technologies are adapting to industry trends, providing cost-effective, readily deployable and fully integrated solutions to protect assets in the cloud—all managed from a single comprehensive view.

In this paper, we evaluate endpoint security requirements in Amazon Web Services (AWS). We delve into identifying threats, protecting assets, responding to events and recovering from incidents in a distributed cloud environment. This strategy develops a defense-in-depth architecture aligned with organizational business drivers in the cloud. Endpoint security solutions in the cloud provide greater flexibility to manage physical, hybrid and cloud security models while providing enhanced visibility in centralized monitoring services.

Moving Endpoint Security Solutions to the Cloud

The business case for moving to the cloud arises from the economies of scale for computing resources and storage, as physical layers of computing are abstracted to a managed partner. As endpoints are transferred, provisioned or migrated from a physical asset into a cloud model, ensuring their security is critical. A successful endpoint security strategy that addresses the various challenges of cloud migration, such as scale, speed and complexity, can yield better cost savings, visibility, agility and scalability.

Endpoint security solutions in AWS are the hallmark of successful cloud migrations. Amazon Elastic Compute Cloud (EC2) instances provide nearly limitless efficiency gains while encompassing data protection and unparalleled visibility through cloud-native security services including Amazon GuardDuty and AWS Security Hub.[1] AWS also leverages industry-leading partners to streamline tools, ensuring that an organization's defense doesn't blink. These groundbreaking integrations allow security operations teams to identify the indicators of attack (IoAs) and indicators of compromise (IoCs) to act proactively—instead of reactively, after a breach.

A successful endpoint security strategy that addresses the various challenges of cloud migration, such as scale, speed and complexity, can yield better cost savings, visibility, agility and scalability.

Importance to the InfoSec Community

Why is an endpoint security solution so critical? With GDPR and its significant penalties for non-compliance, the expectations for data protection have changed. For example, the European Union (EU) holds data controllers and processors responsible not only for personally identifiable information (PII), but also for timely notifications when a breach occurs:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. … Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[2]

Of course, data is stored, processed and accessed via the endpoints that are commonly the user's interface to sensitive data, including PII. Information security starts at the endpoint to build a defense-in-depth architecture capable of securing people, processes and technology. Elevated compliance directives make the endpoint attack vector even more critical in global business operations.

With GDPR and its significant penalties for non-compliance, the expectations for data protection have changed.

[1] This paper mentions product names to provide real-life examples of how visibility tools can be used. The use of these examples is not an endorsement of any product.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Traditional vs. Cloud-Based Endpoints

What's the difference between traditional and cloud-based endpoints? Endpoints are remote computing devices designed as a human interface to translate data access to and from the network. Traditional endpoints include laptops, desktops, servers, workstations, mobile devices and the IoT. The cloud environment transfers management of the lower layers of the OSI model—physical, data link and network—to a managed service provider that controls system resources and storage while providing the organization with greater control, agility and security over data.

Defining cloud endpoints is challenging because of hybrid architectures that combine physical, virtual and cloud-based assets. The key to identifying cloud endpoints resides in the service-oriented architecture (SOA) used for providing resources as a service in such models as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS). Cloud-based endpoints include provider-hosted servers, databases, instances, services and applications. Cloud-based endpoint security strategies are designed to secure data at rest, in transit and in use. These technologies include capabilities such as antivirus (AV), a host-based intrusion prevention system (HIPS), application blacklisting, machine learning (ML) and UEBA.

Cloud-based endpoint security strategies are designed to secure data at rest, in transit and in use.

Securing endpoints in hybrid and cloud-based hosting models is very different from doing so in a traditional on-premises data center. With SOA, cloud providers assume shared responsibility for providing resources to customers that are leveraging the cloud's economies of scale. Under that model, the customer is at risk of losing visibility into those cloud resources. Naturally, organizations objected to this, because they require visibility into all of their assets, regardless of where they reside.

The traditional data center model leveraged host-based AV and firewalls to secure endpoint data within a defined trust perimeter. The cloud abstracts the concept of on-premises data centers into a decentralized model with a de-perimeterized structure. User endpoints communicate with the cloud network via physical network connections, VPNs, mobile devices and internet-facing web portals. Endpoint communication with management services is critical to enable rapid response for security incidents. While hybrid on-premises security management services integrate with the cloud, best practice recommends leveraging cloud-based SaaS solutions to enhance visibility regardless of where the endpoint lives.

Best practice recommends leveraging cloud-based SaaS solutions to enhance visibility regardless of where the endpoint lives.

Use Case: Cloud Endpoint Migration and Integration in AWS

Moving assets to the cloud requires an evaluation of security requirements. This evaluation begins with choosing an endpoint security solutions provider that can provide support in physical, hybrid and cloud-based computing models. After selecting a provider, the organization must review its security requirements to determine which security features, such as ML, HIPS, application blacklisting and UEBA, are required. The organization must establish centralized visibility into assets and then synchronize threat intelligence with the host, as outlined in Figure 1.

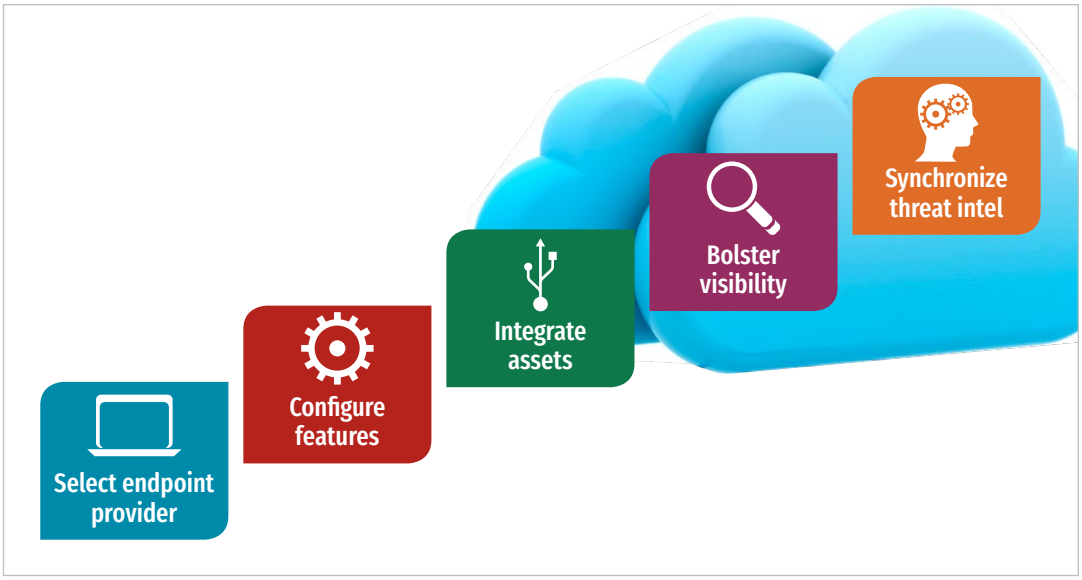


Figure 1. Five Steps of Security Endpoint Migration

The five steps shown in Figure 1 involve these activities:

1. **Select your endpoint security provider** based on business requirements for protection, migration, time, visibility, consistency, complexity, speed and scalability.

2. **Configure endpoint security capabilities to foster integration, and evaluate features** including EDR, signature/heuristic-based AV, firewall, HIPS, application blacklisting, DLP, ML and UEBA. Key activities include:
   - Evaluating endpoint agent visibility for log sources
   - Assessing integration requirements with SIEM
   - Testing AV alerting for false positive rates
   - Testing HIPS for automation capabilities
   - Evaluating UEBA for ease of implementation
   - Determining cost savings of ML capabilities

3. **Identify assets via cloud-based security managers, and deploy endpoint security agents** to physical, virtual and cloud-based assets such as Amazon EC2 instances.

4. **Bolster visibility in a comprehensive view service** such as Amazon CloudWatch event monitoring, where analysts can easily view endpoint activity.

5. **Synchronize threat intelligence** with Amazon GuardDuty agentless monitoring and conduct security monitoring in cloud-based SIEM services such as AWS Security Hub.

Endpoint Detection and Response

EDR agents are a central element of migrating to AWS. Legacy endpoint security products are limited to either blocking or allowing an activity. EDR products add the ability to record endpoint activity and store it for future searches. Capturing IoCs is an ideal feature for integrating EDR agents with threat intelligence services, such as Amazon GuardDuty, which provide continuous threat monitoring and agentless detection for malicious behavior. See Figure 2.

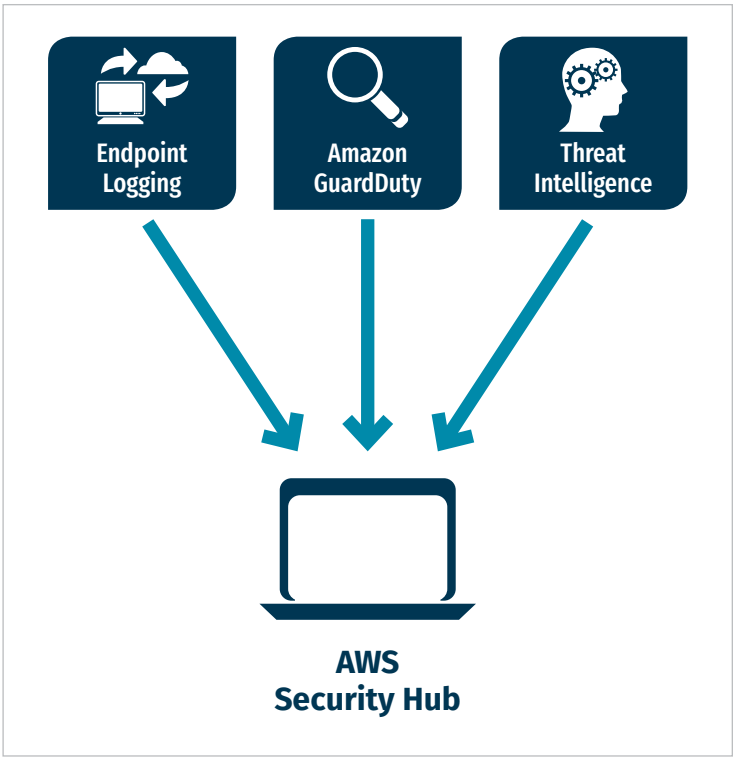


Figure 2. Amazon GuardDuty

EDR agents also enhance cloud-based security operations by integrating system monitoring capabilities and leveraging system monitor logging and OS equivalents to provide detailed information about processes, connections and file changes. Tracing parent-to-child process relationships is key to determining the root cause of a cyber incident. A traditional security agent might report an endpoint infection, whereas an EDR security agent confirms the threat is blocked and, as shown in Figure 3, identifies the spawning process traced to a recent phishing attack.

Signature- vs. Heuristic-Based Antivirus

Endpoint security agents require a robust base of malware file signatures to stop attackers from leveraging known malicious files. Signature detections serve as a baseline of security but are not an assurance of safeguarding data, because an attacker can modify the malware source code in minutes, resulting in a new signature capable of beating signature-based AV. Heuristic- and behavior-based endpoints integrate ML to identify new malware based on behavior instead of signatures.

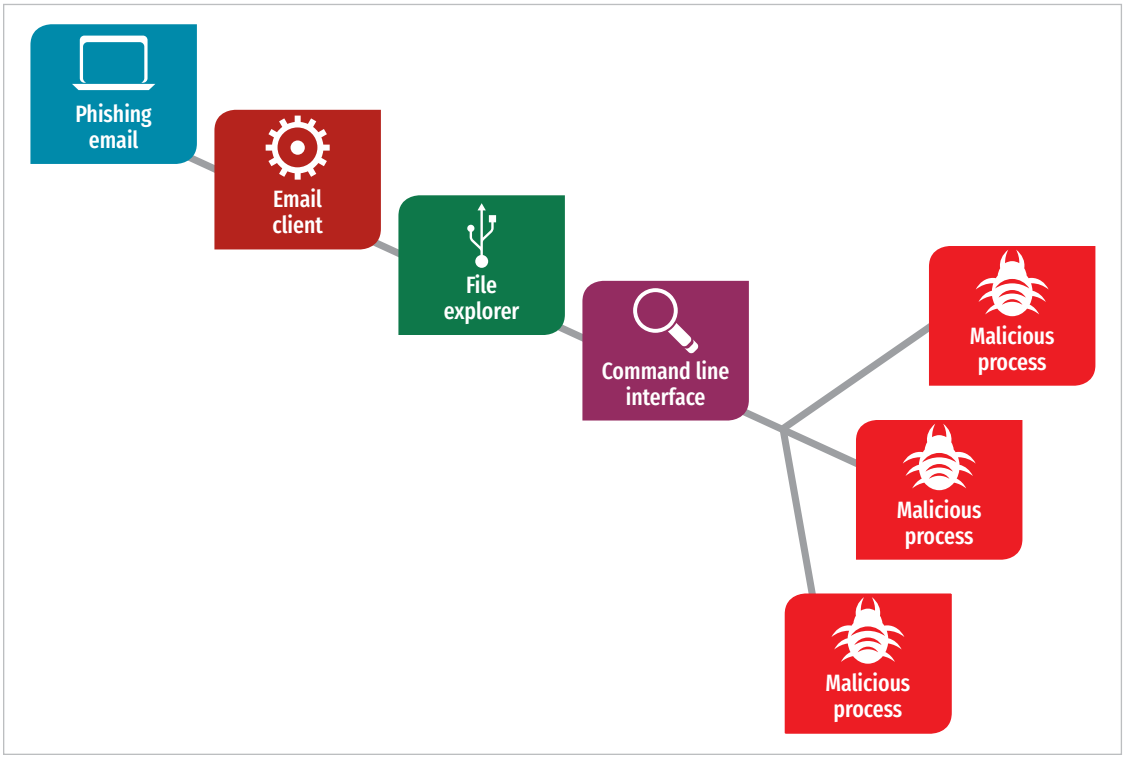


Figure 3. EDR intercepts the attack cycle before malware spreads.

Application Blacklisting

Endpoint security solutions in the cloud require application control through both whitelisting and blacklisting. AWS Systems Manager and AWS Config provide the capability to record inventory data to enable scenarios such as tracking newly installed or removed software applications, assessing security risk and troubleshooting.[3] Endpoint security solutions often include these types of application controls to prevent the use of hacking tools and malicious software. This is often a challenging process because of frequent software updates that change file-based signatures.

User and Entity Behavior Analytics

UEBA is the human equivalent of ML for systems. UEBA leverages the baseline of a user's activity to determine the expected pattern for that user. When a user deviates from the established baseline, or when a user's pattern suddenly aligns with known malicious patterns, UEBA-capable agents trigger alerting and synchronize this data into threat intelligence services such as AWS Security Hub.

Data Loss Prevention

Security teams utilize DLP cybersecurity technology to monitor and alert on data content. This technology supports organizational compliance and data protection requirements for intellectual property, PII and confidential data. DLP technology is a unique solution for PII breach monitoring because of its content inspection capabilities. Cloud-based endpoint security agents with DLP capabilities can alert on the transfer of sensitive data, such as PII or proprietary source code, and alert cyber responders through a centralized monitoring service.

Endpoint Security Solutions in AWS Marketplace

AWS cloud-based endpoint security solutions offer seamless integration. Security solutions currently available in AWS Marketplace offer direct integration with more than 800 security applications from more than 36 leading endpoint vendors. This level of partnership allows organizations to select and integrate the most appropriate endpoint security partner based on business needs and capability requirements. Seamless integration fosters the deployment of endpoint agents across physical, virtual and cloud-based Amazon EC2 instances for total endpoint coverage in the environment.

Amazon GuardDuty allows organizations to take endpoint security further in the cloud through a threat detection service that continuously monitors for malicious activity and unusual behavior to protect AWS accounts and workloads. Amazon CloudWatch provides log visibility to view events and security incidents in greater detail. These capabilities aggregate into a comprehensive view with the AWS Security Hub. Gone are the days of traditional signature-based AV. Today, well-prepared organizations rely on the power of cloud-based endpoint security solutions.

---

[3] "Preventing blacklisted applications with AWS Systems Manager and AWS Config," April 26, 2018, https://aws.amazon.com/blogs/mt/preventing-blacklisted-applications-with-aws-systems-manager-and-aws-config

Summary

The flexibility, elasticity and economy of cloud computing are driving organizations to move from traditional to cloud-centric computing models. Cloud migration requires evaluation of business requirements for protection, migration, time, visibility, consistency, complexity, speed and scalability. Cloud-based endpoint security solutions have moved from simple AV to integrated suites capable of securing assets in any environment with advanced capabilities such as application control, ML and UEBA. Synchronization with AWS services such as Amazon CloudWatch for log visibility, Amazon GuardDuty for threat intelligence and AWS Security Hub for synchronization provides a comprehensive view for responders to combat the threat while upholding organizational security objectives in a distributed cloud environment.

About the Author

Thomas Banasik is a SANS analyst and senior security operations center manager for Veritas Technologies, LLC. He has consulted with numerous organizations in cybersecurity across the government, military and commercial sectors. An incident response expert, Thomas has extensive experience in security operations, threat intelligence, insider threat, and threat vulnerability management. He previously worked as a senior security operations center manager for the U.S. Government Accountability Office and is a retired U.S. Army cyber and military intelligence officer. Thomas holds the GCIH, GCWN, GCIA, GSEC, and CISSP-ISSEP, ISSAP, ISSMP certifications and is currently pursuing a second graduate degree in information systems security engineering from the SANS Technology Institute.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace

aws marketplace

Enhance threat detection in AWS with third-party intelligence

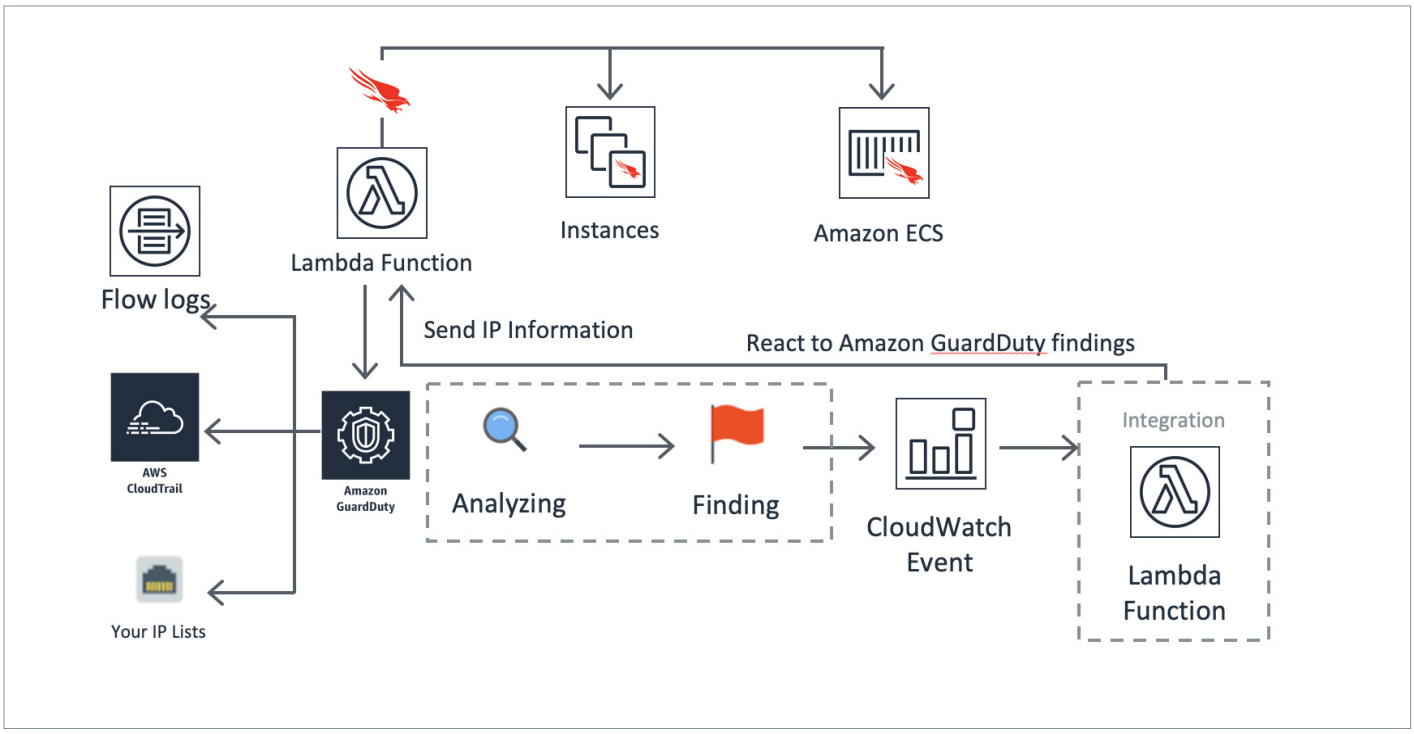
Endpoints represent one of the strongest sources of visibility due to the amount of rich file-level information, such as keyboard strokes and configuration data, that typically isn't available from network-based information in most organizations. Building on foundational endpoint security services in AWS, such as Amazon GuardDuty, AWS Marketplace offers a growing variety of software seller solutions to enhance endpoint security. For instance, CrowdStrike is tightly integrated with both Amazon GuardDuty and AWS Security Hub.

Security teams leveraging CrowdStrike gain a threat intelligence feed that seamlessly integrates with Amazon GuardDuty. This provides an additional layer of protection by offering an indicator of attack (IOA)-based threat prevention designed to stop known and unknown threats in real time. Security teams are also integrating CrowdStrike's endpoint security solutions with AWS Security Hub through AWS Lambda.

How AWS customers are using CrowdStrike to enable key endpoint security use cases

CrowdStrike's Falcon Endpoint Protection Premium solution is a cloud-delivered platform which helps stop breaches by unifying next-generation antivirus (NGAV), endpoint detection and response (EDR), managed threat hunting, and threat intelligence automation. This is all delivered through a single lightweight agent. Security teams are using this multi-faceted platform to make various operations more secure, including:

- **Offering security at the speed of DevOps:** CrowdStrike is simple to implement, allowing security teams to secure CI/CD processes without decelerating the spin up of new Amazon Elastic Compute Cloud (EC2) instances and associated innovation. CrowdStrike can make it easier to rapidly deliver new applications and scale infrastructure to meet changing business needs.
- **Accelerating cloud migrations with secure containers:** Containerizing workloads is an increasingly common practice that can yield higher efficiency and agility, yet it also creates an attack surface that isn't well covered by many existing point solutions. CrowdStrike's Falcon Agent extends visibility to cover not only traditional endpoints, but also threats within Docker containers. This solution can be used as containerized workloads are migrated to AWS.



- **Enabling continuous compliance with automated policies:** Automated compliance rules, fine-grained controls, and flexible configuration management techniques in CrowdStrike make continuous compliance an attainable goal. As shown below, security teams can leverage AWS Lambda and create a joint workflow between Amazon GuardDuty and CrowdStrike to react to findings in real time, which in turn supports continuous compliance.

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, solution 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 ISV 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 steps can help you get started:

Browse CrowdStrike solutions on AWS Marketplace

Falcon Endpoint Protection Premium

Bundled platform with managed services for full protection

Falcon Prevent Next Gen Antivirus

Machine learning to detect and prevent known and unknown malware

Falcon Sandbox

Deep malware analysis of evasive and unknown threats