Trellix | aws

EBOOK

Proactive security for your AWS environments with Trellix

Guide to XDR for AWS

Table of contents

aws PARTNER

Security built in the cloud, for the cloud

When it comes to cybersecurity, change must be met with change. As businesses grow and innovate in the cloud, a patchwork of legacy tools can't keep pace with security demands, requiring teams to switch to more scalable, efficient solutions. The same goes for threat landscapes—as malicious actors invent new tactics and write new software, businesses must evolve their cybersecurity approach to protect their infrastructure and data. Trellix is an Amazon Web Services (AWS) Partner that offers customers solutions that expand security capabilities in the cloud and uncovers cloud-specific threats.

According to Gartner, up to 40% of end-user organizations will use XDR by the end of 2027—and for good reason. Sometimes referred to as the "future of security," XDR is a shift away from a reactive security approach. Instead, XDR allows businesses to adopt a proactive security posture by consolidating their tools and aggregating data for enhanced visibility and threat mitigation.

In this eBook, you'll learn how Trellix and AWS together provide comprehensive security at different points in your cloud journey: migrating assets to the cloud securely, incorporating frameworks for compliance, and integrating AWS tools for a layered, comprehensive XDR security solution.

Trellix provides an open and native extended detection and response (XDR) platform that uses machine learning and automation to empower over 40,000 business and government customers.

aws PARTNER

What is XDR, really?

- ✓ Different solutions on the market label themselves as providing XDR, but this can be a loose interpretation for some. The Trellix approach to XDR is a "living security" model—an adaptive, learning ecosystem that helps businesses stay steps ahead through a combination of telemetry data, artificial intelligence, machine learning, and automation. Living security goes beyond monitoring; it offers robust detection, response, and remediation capabilities so that businesses can minimize risk and efficiently recover. The Trellix platform includes endpoint security and protection, network security, data loss prevention (DLP), email security, cloud security and security operations, and analytics offerings—all of which speak to each other.
- ✓ Another benefit? Smarter insights mean reduced alert fatigue, a comfort SecOps and IT teams can enjoy with a good XDR platform.

Secure your migration with enhanced detection

Move to the cloud safely with Trellix Detection as a Service and Trellix Data Loss Prevention (DLP) Discover

Migrating your workloads to the cloud is not something you have to do alone. With guided expertise from AWS, supplemental security tools from cloud-native partners, and a well-constructed migration plan, you can modernize quickly and securely.

Ensure business continuity with AWS and Trellix

A holistic cloud security strategy should include visibility, continuous monitoring, configuration management, and microsegmentation. It should also incorporate a recovery plan in the event of a natural disaster or breach. Together, AWS and Trellix can provide each of those elements when moving to the cloud.

Visibility

- With Trellix DLP Discover, part of its XDR system, you can locate, classify, and protect your sensitive data for more than 300 content types. The solution scans your resources both on prem and in the cloud to identify sensitive data and uncover potential risks, which is useful for informing policy. If a policy violation does occur, DLP Discover simplifies the repair process to prevent further data leakage.
- AWS users can implement safeguards in their cloud setup by activating API and user activity logging with AWS CloudTrail. The solution monitors and records account activity across your AWS infrastructure for improved control over storage, analysis, and remediation actions.
- The Trellix Cloud Security Platform can also identify potential risks from CloudTrail events.

Prevention is protection

- With Detection as a Service from Trellix, a cloud-native threat detection service, you can enhance the security of your Amazon Simple Storage Service (Amazon S3) buckets. The solution automatically detects whenever a document is uploaded or delivered to a collaboration tool, then pulls it and analyzes it in near-real time. If the file appears malicious, it's sent to a quarantine file and Trellix issues an alert. Trellix Detection as a Service also works alongside Amazon Macie to discover and protect your sensitive data using machine learning and pattern matching.

Ensure business continuity with AWS and Trellix

Continuous monitoring and advanced threat protection

- Trellix Detection as a Service monitors for threats in your cloud infrastructure and Software-as-a-Service (SaaS) products by scanning files for malicious content.
- Monitor your workloads with AWS GuardDuty for organization-wide visibility and ongoing threat detection.
- The Trellix Cloud Security Platform also correlates threat information from AWS GuardDuty for investigation.
- Trellix's Endpoint Protection Platform provides threat protection for devices and endpoints at the network edge, offering enhanced protection against malware and other advanced threats. And because this solution creates a unified view through a simplified console across endpoints, organizations can scale securely.

Configuration management

- Trellix DLP Discover comes with integrated case management so that if policy is violated, the right content owners and admins receive a notification.
- AWS Identity and Access Management (IAM) enables you to create users and groups under your AWS account that control the permissions required to perform tasks using AWS resources.

Microsegmentation

- AWS Web Application Firewall (AWS WAF) enables web application segmentation use-cases by leveraging fine-grained web access control lists.
- Essential to taking a zero-trust approach, Trellix helps customers employ two types of comprehensive microsegmentation. We'll cover this further on the next page.

aws PARTNER

Ensure compliance with automation

End audit surprises with Trellix Cloudvisory

For businesses operating in regulated industries, setting up a control framework around configurations for security and compliance programs is fundamental to meeting regulatory standards. But as a business expands, tracking and scaling configurations can become time-consuming and complex. While AWS offers a breadth of tools for setting permissions at a granular level, there's still room for human error—for example, a DevOps team may manipulate network security controls to test new code. These types of oversights can go undetected until a breach occurs or it's time to conduct an audit, leaving the door open for ransomware in the meantime.

Easily find misconfigurations in your AWS environment

With Trellix Cloudvisory, businesses can immediately detect misconfigurations, otherwise demanding more time and effort from your teams. Built on AWS, Trellix Cloudvisory is a cloud native security solution that provides unified control and centralized visibility over your cloud infrastructure and cloud workloads.

Users can:

- Analyze network and IAM policies to produce compliance reporting using centralized remediation APIs for quarantining assets and users, across the board.
- Apply automation for persistent policy enforcement, network monitoring, and resolution, thus saving time previously spent on constant intervention management.
- Get recommended updates using machine learning, which leverages agentless data collection and analysis to correlate actual network flows and current network policies. You can also conduct a "dry run" to test the impact of changes before implementation.

Control lateral movement with microsegmentation

Microsegmentation enables security architects to define security controls and deliver services for logically created unique security segments that can be as granular as the individual workload level. It is a principle of the zero-trust approach and makes it easier to reduce an attacker's opportunity to further pervade a system. Trellix Cloudvisory offers two types of microsegmentation: "Golden State" and Contextual.

Golden State microsegmentation intuitively restricts machine accounts and user access to resources leveraging a least-privilege model rules based on static policies for IP addresses.

Contextual microsegmentation automatically discovers existing workloads across cloud providers to generate segmentation policies in context, simplifying how organizations manage microsegmentation at scale.

Safeguard workflows with embedded threat protection

Fortify your defenses with Trellix Helix

Disparate tools that don't speak to each other, visibility gaps, contextless alerts, and skillset shortages are some of the challenges that businesses face as they build a security strategy for their cloud operations. AWS and Trellix make your security team better together by offering cloud-native, smart tools that are easy to set up.

Make security part of your cloud DNA

Trellix Helix and Trellix Helix Detect are SaaS security operations platforms that improve visibility and control over your AWS environment. Customers can get a comprehensive assessment across disparate tools via an in-depth dashboard, which displays all AWS metrics. With extensive visibility into cloud usage and data, organizations can continuously adopt best practices to improve their security posture.

Unify your view. The Trellix Helix Detect interface provides immediate situational awareness. Because it aggregates data from more than 650 tools so you can see everything in one place. AWS users can take advantage of this integration by feeding AWS CloudTrail logs into Trellix Helix. This provides a convenient way to search through log data, identify out-of-compliance events, and accelerate security incident investigations.

Reduce alert fatigue. Using advanced artificial intelligence (AI), Trellix Helix spots risky users and behaviors, prioritizing alerts and surfacing the most important threats quickly.

Do more with automation. Automation amplifies the ability of your security teams to respond faster, at scale.

Bring in expertise. Trellix provides guided investigations from teams with extensive frontline experience and helps companies develop pre-built playbooks.

Helix can ingest data from

650

different native and open security tools.

aws PARTNER

Trellix & AWS for everyday security

Trellix and Amazon Web Services (AWS) have come together to expand security capabilities on the cloud and uncover cloud-specific threats by continuously monitoring the network activity and account behavior in your cloud environment.

AWS Security Hub acts as a unified security center that automates security checks and remediation to help organizations improve their security posture. Combined with Helix Detect, this provides a holistic view of all third-party tools and alerts, allowing the customer to focus on top security incidents first.

A layered security approach with Cloudvisory & AWS Config simplifies the assessment, audit, and evaluation processes for configurations of your AWS resources so that it's easier to align with policy and best practices.

Use Amazon Inspector for an easier way to analyze application security. This automated vulnerability management service continually scans AWS workloads for software vulnerabilities and unintended network exposure.

Don't forget hardware protection. AWS IoT Device Defender offers continuous monitoring of your connected devices and sends an alert if it detects any gaps in your IoT configuration.

aws PARTNER

Integrations for ongoing cloud security operations

A foundational aspect of a strong XDR platform is its ability to integrate with, and ingest data from, the tools you're already using. That's great news for AWS customers who use Trellix, as the platform seamlessly integrates with nine commonly used AWS tools—and counting.

Through these integrations, Trellix instantly feeds key telemetry and security findings from AWS into its platform for richer context, improved visibility, and faster responses. With Trellix, AWS customers can detect anomalies and correlate threat information through:

- AWS Network Firewall, a managed service that makes it easy to deploy essential network protections for all your Amazon Virtual Private Clouds (VPCs) by defining firewall rules that give you fine-grained control over network traffic.
- Amazon CloudWatch, a monitoring and observability service that collects monitoring and operational data in the form of logs, metrics, and events.
- Amazon Route 53, a highly available and scalable cloud DNS web service that routes end users to Internet applications by translating domain names into numeric IP addresses.
- Amazon VPC flow logs, a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. You can create flow logs for multiple services in AWS, including Amazon WorkSpaces, Amazon ElasticCache, and Amazon Redshift, among others.

Other integrations include AWS Security Hub, Amazon S3, AWS CloudTrail, Amazon GuardDuty, and Amazon Inspector.

Trellix continues to add integrations with AWS tools each month, making it a great long-term XDR option for AWS customers. It also integrates with hundreds of other cybersecurity vendors.

aws PARTNER

Bring SecOps to life with true XDR

Living Security Starts Here

Visit Trellix on AWS Marketplace ›

Did you know?

Customers who purchase Trellix in AWS Marketplace will also be eligible to draw down against their AWS Enterprise Discount Program commitments.

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.