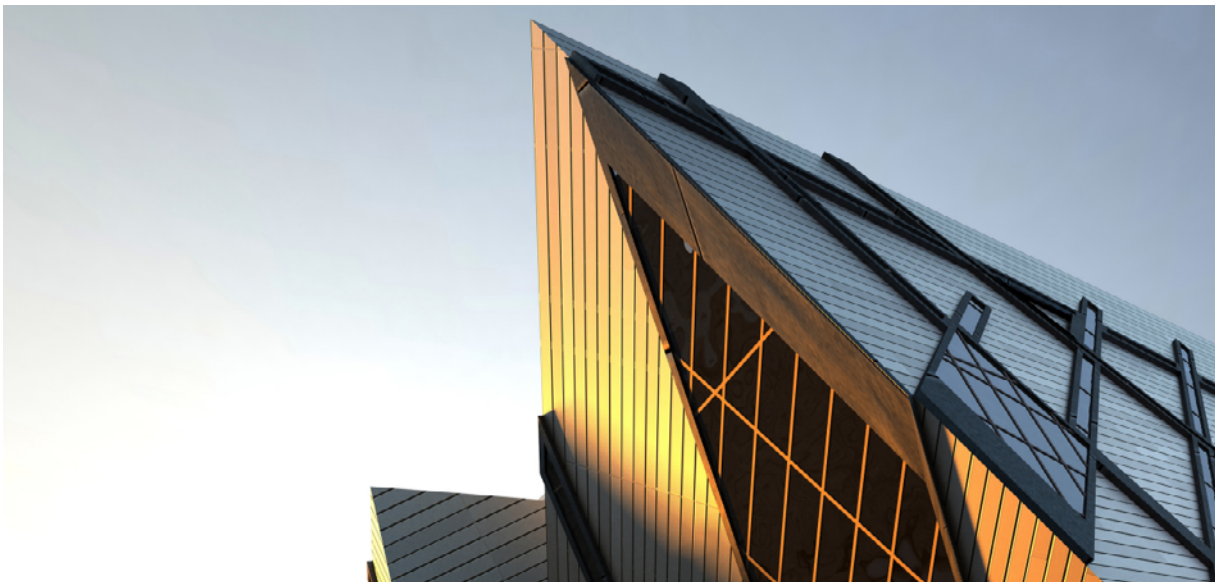
Trellix | aws

SOLUTION BRIEF



Securing Cloud Workloads and Containers with Trellix on AWS

Stay ahead of adversaries with increased resilience and agility

Trellix is a cloud-native security platform that helps organizations achieve cloud security and compliance objectives across Amazon Web Services (AWS) and other cloud environments. By integrating with AWS security services, Trellix enables customers to automate security and compliance workflows, reduce risk, and scale security operations to meet the needs of modern cloud workloads.

As more businesses migrate to the cloud, they face new threats that pose additional challenges to their cyber defense. Security teams encounter new and evolving requirements to track and protect data in various cloud environments. Additionally, your organization may have to deal with misconfigurations, credential abuse, and inadequate visibility into disparate multicloud infrastructures. These vulnerabilities can make your organization susceptible to targeted attacks.

Security in your cloud is only as good as the cloud and on-premises procedures and solutions you use to safeguard access and protect workloads. And while you might have the right tools and security controls in place across your hybrid infrastructure, with built-in asset management, two-factor access controls, and firewalls, your adversaries can still compromise the organization's assets and unintentional misconfigurations.

- Attackers can gain access through phishing, credential stuffing, or other tools of the trade.

- Misconfigurations can occur when a security team member changes a port, protocol, or service, or brings in code in unvetted container images pulled from repositories like GitHub.

As environments and adversaries change, Trellix helps you meet new security challenges and prevent advanced attacks that go undetected by traditional security measures. Trellix Cloud Security solutions protect your cloud infrastructure, wherever it is, and allow your organization to:

- Reduce misconfigurations
- Ensure end-to-end visibility and policy management
- Unify its cloud security landscape through a single console

Key Benefits

- Comprehensive Container Security: Trellix provides a complete solution for securing containerized workloads on AWS, including vulnerability management, runtime protection, and compliance monitoring.
- Automated Security Operations: Trellix integrates with AWS security services to automate security operations and reduce manual effort, such as security event correlation, threat prioritization, and compliance reporting.
- Cloud-Native Security: Trellix is built for the cloud and provides scalable security that can adapt to the needs of modern cloud workloads.
- Simplified Compliance: Trellix provides pre-built compliance policies and automated compliance reporting, making it easier for organizations to achieve and maintain compliance across their cloud workloads.

Trellix Cloud Security Benefits

Your organization can use Cloud Security solutions to:

Protect against threats with comprehensive security

To protect against advanced threats in the cloud, Cloud Security solutions include state of the art, signatureless detection and protection to stop targeted or evasive attacks that hide in internet traffic.

Eliminate blind spots with overarching management of environments

Cloud Security solutions protect your organization from attacks across multicloud and on-premises infrastructures. If you use products from multiple cloud platforms, you need to collect data from all of them to ensure comprehensive monitoring. Cloud Security interfaces and streamlined management help you manage and secure these distributed and dynamic environments, so you can perform analytics and correlation in one consolidated place.

Scale easily as you grow with flexible security

You get always-right-sized security with a solution you can turn off and on as needed, so you only pay for what you need, when you need it. This helps you optimize costs, improve efficiency, and reduce misconfigurations. The rapid and adaptable threat detection service in Cloud Security also scans files and content to identify threats in the cloud, security operations center (SOC), security information and event management (SIEM), or in files that have been uploaded to web applications.

Proactively protect your cloud assets and data wherever they are

Having full visibility means being able to detect threats across your environment. Use Cloud Security solutions to collect usage data logs from across your environment in a central place and normalize this information into usable data points.

Cloud Security solutions also keep all your cloud assets, data at rest, and data in motion safe from cloud-native threats, malware, and fileless attacks. They automatically protect your organization against ransomware and software as

a service (SaaS) threats while mitigating risks, and provide unified user and data protection across endpoints, networks, and cloud services.

Incorporate your existing solutions seamlessly

Your organization may be using cloud-based solutions to handle everything from human resources to accounting, payroll, and sales. Cloud Security saves you time by allowing you to perform analytics and correlation for all your cloud solutions in one centralized location. Trellix solutions natively integrate with cloud providers to add protection, detection, and visibility for existing cloud workloads at scale.

Integrate with CASB and SWG solutions

Trellix Cloud Security integrates with leading CASB solutions to protect your assets in the cloud from advanced threats. Our solutions also integrate with leading SWG providers to protect your users from zero-day threats and enact data protection everywhere.

Trellix Cloud Security featured solutions

Trellix Cloudvisory is a control center for cloud security management that delivers visibility, compliance, and governance to any cloud environment. It runs cloud-native microservices for asset discovery and compliance scanning to enable end-to-end automation of detection and response for complex multicloud environments. With Cloudvisory, you can automate security compliance monitoring with over 1,300 built-in checks and apply microsegmentation and policy guardrails automatically.

Trellix Detection as a Service (formerly Detection On Demand) is a cloud-native threat detection service that rapidly scans submitted content to identify resident malware. To protect your cloud infrastructure, you must be able to actively monitor files for the presence of malicious content. Detection as a Service uncovers harmful objects in the cloud. You get intelligence-backed, validated threat detection capabilities with enough contextual analysis to act on alerts with confidence.

Container Security: Containers are a popular choice for deploying cloud applications due to their flexibility, portability, and scalability. However,

containers also introduce new security challenges, such as container image vulnerabilities, runtime security, and container orchestration security. Trellix provides a comprehensive container security solution that includes vulnerability scanning, runtime protection, and compliance monitoring across containerized workloads on AWS.

AWS Integration: Trellix integrates with AWS security services, such as AWS Security Hub, AWS Identity and Access Management (IAM), and Amazon GuardDuty, to provide real-time security insights and automate security operations. For example, Trellix can leverage AWS Security Hub to ingest security findings from multiple AWS accounts and regions, correlate findings with threat intelligence, and prioritize remediation based on business impact. Trellix can also integrate with AWS IAM to enforce least privilege access control policies and manage access to AWS resources.

Secure your cloud with Trellix

The effectiveness of your overall cloud security posture requires traditional security solutions that cover network, endpoint, and email, enhanced with comprehensive visibility and analytics-based capabilities. Our holistic approach to cloud security helps you monitor and defend your hybrid infrastructure with advanced protection and detection technologies. For example, we offer extended detection and response (XDR) and analytics in a comprehensive XDR platform. Trellix XDR gives you the ability to seamlessly interconnect and correlate detection across your security ecosystem.

Trellix and AWS provide a comprehensive solution for securing cloud workloads and containerized applications. By leveraging the scalability and flexibility of the cloud, organizations can achieve their security and compliance objectives while reducing operational overhead and improving business agility.

To learn more, visit trellix.com

Trellix Available Now in AWS Marketplace

Advanced Protection Features

Features	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Centralized Management (Trellix ePO Platform)	✓	✓	✓
Role-based access controls allow multiple permissions in Trellix ePO	✓	✓	✓
Multiple Cloud Support (AWS, VMware)	✓	✓	✓
Use Micro-segmentation to Quarantine Workloads and Containers	✓	✓	✓
Trellix MOVE (Agentless and Multi-platform)	✓	✓	✓
Threat Prevention: ENS for Servers OS (Windows and Linux)	✓	✓	✓
Host-based firewall	✓	✓	✓
Native Firewall Management for AWS (Security Groups)	✓	✓	✓
Host Intrusion and Exploit Prevention	✓	✓	✓
Cloud Encryption Management	✓	✓	✓
Trellix Management for Optimized Virtual Environments (Agentless and Multiplatform)	✓	✓	✓
Import AWS tag information into Trellix ePO	✓	✓	✓
Auto-remediation to automatically quarantine workloads without security policies	✓	✓	✓
Adaptive Threat Protection with Behavioral Analysis	✓	✓	✓
Native Network Traffic Analysis for AWS		✓	✓
Network Traffic Visualization and Micro-segmentation		✓	✓
Cloud-native network traffic analysis combined with Trellix GTI reputation score		✓	✓
Trellix Virtual Intrusion Prevention System Integration		✓	✓
Dynamic whitelisting for servers via Trellix Application Control			✓
Continuous audit logging via Trellix File Integrity Monitoring			✓
File and folder protection via Trellix Change Control for Servers			✓
Trellix Cloudvisory	✓		

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.

072022-05