DATASHEET

Trellix Cloud Workload Security

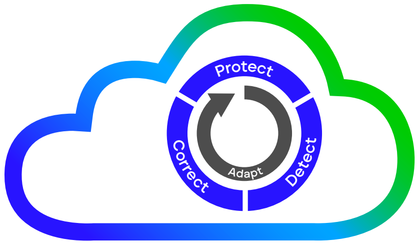
Secure your hybrid infrastructure workloads.

As corporate data centers evolve, more workloads are migrated to cloud environments every day. Most organizations have a hybrid environment with a mixture of on-premises and cloud workloads, including containers, which are constantly in flux. This introduces a security challenge as cloud environments (private and public) require new approaches and tools for protection. Organizations need central visibility of all cloud workloads with complete defense against the risk of misconfiguration, malware, and data breaches.

Trellix Cloud Workload Security (CWS) automates the discovery and defense of elastic workloads and containers to eliminate blind spots, deliver advanced threat defense, and simplify multicloud management. Trellix provides protection that makes it possible for a single, automated policy to effectively secure your workloads as they transition through your virtual private, public, and multicloud environments, enabling operational excellence for your cybersecurity teams.

Key Benefits

- Continuous visibility of elastic workload instances eliminates operational "blind spots"
- Centralized management and automated workloads drastically reduce the complexity of hybrid and multicloud environments.
- Visualize and discover network threats without installing an agent.
- Virtual machine-optimized threat defenses deliver multilayer countermeasures.
- Integration with automation tools like Chef and Puppet apply security to hybrid cloud workloads.
- Discover and monitor Docker containers, and secure them with microsegmentation.



Cloud Workload Security

Comprehensive visibility and control

Modern Workload Security: Use Cases

Automated discovery

Unmanaged workload instances and Docker containers create gaps in security management and can give attackers the foothold they need to infiltrate your organization. Trellix CWS discovers elastic workload instances and Docker containers across Amazon Web Services (AWS), Microsoft Azure, OpenStack, and VMware environments. It also continuously monitors for new instances. You gain a centralized and complete view across environments and eliminate operational shortcomings that lead to risk exposure.

Gaining insights into network traffic

By utilizing native network traffic provided from the cloud workloads, Trellix CWS is able to augment and apply intelligence from Trellix Global Threat Intelligence (GTI) data feeds. The enriched information is able to display properties such as risk score, geo-location, and other important network information. This information can be used to create automated remediation actions to protect workloads.

Integration into deployment frameworks

Trellix CWS creates deployment scripts to allow the automatic deployment and management of the Trellix agent to cloud workloads. These scripts allow integration into tools such as Chef, Puppet, and other DevOps frameworks for deployment of the Trellix agent to workloads running by cloud providers, such as AWS and Microsoft Azure.

Consolidate events

Trellix CWS allows organizations to use a single interface to manage numerous countermeasure technologies for both on-premises and cloud environments. This also includes integration into additional technologies, like AWS GuardDuty, Trellix Policy Auditor, and Trellix Intrusion Prevention System.

- Administrators can leverage the continuous monitoring and unauthorized behaviors identified by AWS GuardDuty, providing yet another level of threat visibility. This integration allows Trellix CWS customers to view GuardDuty events, which include network connections, port probes, and DNS requests for EC2 instances, directly within the Trellix CWS console.

- Trellix Policy Auditor performs agent-based checks against known or user-defined configuration audits for compliance such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Center for Internet Security Benchmark (CIS Benchmark), or other industry standards. Trellix CWS reports any failed audits for instant visibility into misconfiguration for workloads in the cloud.
- Trellix Instrusion Prevention System (IPS) is another cloud security platform that performs network inspection for traffic in hybrid as well as AWS and Microsoft Azure environments. It performs deeper packet-level inspections against network traffic, and it reports any discrepancies or alerts through Trellix CWS. This provides single-pane visibility against multicloud environments for remediation.

Enforcement of network security group policies

Trellix CWS permits users and administrators to create baseline security group policies and audit the policies that are running on the workloads against these baselines. Any deviations or changes from the baseline can create an alert in the Trellix CWS console for remediation. Administrators also can manually configure native network security groups from Trellix CWS, which enables them to directly control cloud-native security group policies.

What Sets Trellix Cloud Workload Security Apart

Cloud-native build support

Using Trellix CWS, customers can consolidate management of multiple public and private clouds in a single management console, including AWS EC2, Microsoft Azure Virtual Machines, OpenStack, and VMware Vcenter. Trellix CWS can import and allow customers to run in the cloud with new cloud-native build support for Amazon Elastic Container Service for Kubernetes (Amazon EKS) and Microsoft Azure Kubernetes Service (AKS).

Simple, centralized management

A single console provides consistent security policy and centralized management in multicloud environments across servers, virtual servers, and cloud workloads. Administrators can also create multiple role-based permissions in Trellix ePolicy Orchestrator (ePO) - On - prem, enabling them to define user roles more specifically and appropriately.

Network visualization with microsegmentation

Cloud-native network visualization, prioritized risk alerting, and micro-segmentation capabilities deliver awareness and control to prevent lateral attack progression within virtualized environments and from external malicious sources. Single-click shutdown or quarantine capability help alleviate the potential for configuration errors and increases the efficiency of remediation.

Superior virtualization security

Trellix CWS suite protects your private cloud virtual machines from malware using Trellix Management for Optimized Virtual Environments AntiVirus (Trellix MOVE AntiVirus). And it does this without straining underlying resources or requiring additional operating costs. Trellix MOVE AntiVirus allows organizations to offload security to dedicated virtual machines for optimized scanning of their virtualized environment.

Users gain anti-malware protection via Trellix Endpoint Security for Servers. This solution can intelligently schedule resource-intensive tasks, such as on-demand scanning, to avoid impact to critical business processes.

Tag and automate workload security

Assign the right policies to all workloads automatically with the ability to import AWS and Microsoft Azure tag information into Trellix ePO - On-prem and assign policies based on those tags. Existing AWS and Microsoft Azure tags synchronize with Trellix ePO - On-prem tags so they're automatically managed.

Auto-remediation

The user defines Trellix ePO - On-prem policies. If Trellix CWS finds a system that is not protected by the Trellix ePO - On-prem security policies, and it is found to contain a malware or virus, this system will automatically be quarantined.

Adaptive threat protection

Trellix CWS integrates comprehensive countermeasures, including machine learning, application containment, virtual machine-optimized anti-malware, whitelisting, file integrity monitoring, and micro-segmentation that protect your workloads from threats like ransomware and targeted attacks. Trellix Advanced Threat Protection defeats sophisticated attacks that have never been encountered before by applying machine learning techniques to convict malicious payloads based on their code attributes and behavior.

Application Control

Application whitelisting prevents both known and unknown attacks by allowing only trusted applications to run while blocking any unauthorized payloads. Trellix Application Control provides dynamic protection based on local and global threat intelligence, as well as the ability to keep systems up to date, without disabling security features.

File integrity monitoring (FIM)

Trellix File Integrity Monitoring continuously monitors to ensure your system files and directories have not been compromised by malware, hackers, or malicious insiders. Comprehensive audit details provide information about how files on server workloads are changing and alert you to the presence of an active attack.

Appropriate Security Coverage for Your MultiCloud Environment

Trellix CWS ensures that you maintain the highest quality of security while taking advantage of the cloud. It covers multiple protection technologies, simplifies security management, and prevents cyberthreats from impacting your business—so you can focus on growing it. Below is a feature comparison of the available package options.

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, Azure, 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 and Azure (Security Groups)	✓	✓	✓
Host Intrusion and Exploit Prevention	✓	✓	✓
Cloud Encryption Management	✓	✓	✓
Trellix Management for Optimized Virtual Environments (Agentless and Multiplatform)	✓	✓	✓
Import AWS and Azure 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 and Azure		✓	✓
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	✓		

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.