McAfee Cloud Workload Security

Secure your hybrid infrastructure workloads. Safer. Faster. Simpler.

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.

McAfee® Cloud Workload Security (McAfee® CWS) automates the discovery and defense of elastic workloads and containers to eliminate blind spots, deliver advanced threat defense, and simplify multicloud management. McAfee 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.

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. McAfee 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 and security blind spots that lead to risk exposure.

Gaining insights into network traffic

By utilizing native network traffic provided from the cloud workloads, McAfee CWS is able to augment and apply intelligence from McAfee® Global Threat Intelligence (McAfee® 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.

Key Benefits

- Continuous visibility of elastic workload instances eliminates operational "blind spots" while automating once laborious policy deployments.
- 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 public and private cloud workloads at the time of deployment.

Connect With Us

Integration into deployment frameworks

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

Consolidate events

McAfee 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, McAfee® Policy Auditor, and McAfee® Network Security Platform.

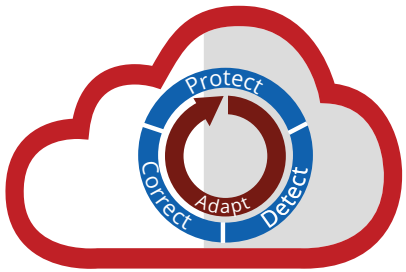
- Administrators can leverage the continuous monitoring and unauthorized behaviors identified by AWS GuardDuty, providing yet another level of threat visibility. This integration allows McAfee CWS customers to view GuardDuty events, which include network connections, port probes, and DNS requests for EC2 instances, directly within the McAfee CWS console.
- McAfee 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. McAfee CWS reports any failed audits for instant visibility into misconfiguration for workloads in the cloud.
- McAfee Network Security Platform 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 McAfee CWS. This provides single-pane visibility against multicloud environments for remediation.

Enforcement of network security group policies

McAfee 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 McAfee CWS console for remediation. Administrators also can manually configure native network security groups from McAfee CWS, which enables them to directly control cloud-native security group policies.

Key Benefits continued

- Get easy multilayer protection from advanced malware and intrusion.
- Discover and monitor Docker containers, and secure them with microsegmentation.
- Secure your environment by taking corrective actions directly from within the solution.



Cloud Workload Security

Comprehensive **visibility** and **control**

What Sets McAfee Cloud Workload Security Apart: Key Features and Technologies

Cloud-native build support

Using McAfee 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. McAfee 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 McAfee® ePolicy Orchestrator® (McAfee ePO™) software, 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

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

Users gain anti-malware protection via McAfee® 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 McAfee ePO software and assign policies based on those tags. Existing AWS and Microsoft Azure tags synchronize with McAfee ePO software tags so they're automatically managed.

Auto-remediation

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

Adaptive threat protection

McAfee 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. McAfee® 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. McAfee® 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)

McAfee® 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

McAfee 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.

Features	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
Centralized management (McAfee ePO platform)	✓	✓	✓
Multiple cloud support (AWS, Microsoft Azure, VMware)	✓	✓	✓
Use microsegmentation to quarantine workloads and containers	✓	✓	✓
McAfee MOVE (agentless and multiplatform)	✓	✓	✓
McAfee Endpoint Security Threat Prevention for Server OS (Windows and Linux)	✓	✓	✓
Host-based firewall	✓	✓	✓
Native firewall management for AWS and Microsoft Azure (security groups)	✓	✓	✓
Host intrusion and exploit prevention	✓	✓	✓
Import AWS and Microsoft Azure tag information into McAfee ePO software	✓	✓	✓
Auto-remediation on noncompliant workloads	✓	✓	✓
Adaptive Threat Protection with machine learning		✓	✓
Network traffic visualization and microsegmentation		✓	✓
Cloud-native network traffic analysis combined with McAfee GTI reputation score		✓	✓
McAfee® Virtual Network Security Platform (McAfee® vNSP) integration		✓	✓
Dynamic whitelisting for servers via McAfee Application Control			✓
Continuous audit logging via McAfee File Integrity Monitoring			✓
File and folder protection via McAfee® Change Control for Servers			✓

Learn More

For more information, visit: **https://www.mcafee.com/us/products/cloud-workload-security.aspx**.

McAfee Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com