McAfee Cloud Workload Security

Secure your private and public cloud 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-premise 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 automates the discovery and defense of elastic workloads and containers to eliminate blind spots, deliver advanced threat defense, and simplify multi-cloud 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 hybrid environments, enabling operational excellence for your cyber security teams.

Real-Time Visibility

Automated Discovery

Unseen workload instances and Docker containers create gaps in security management and can give attackers the foothold they need to infiltrate your organization. McAfee Cloud Workload Security discovers elastic workload instances and Docker containers across Amazon Web Services (AWS), Microsoft Azure, and VMware environments and 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.

Modern Workload Security

Advanced Threat Protection

McAfee Cloud Workload Security 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. Advanced Threat Protection, including machine learning, 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.

Key Benefits

- Continuous visibility of elastic workload instances eliminates operational "blind spots" while automating once laborious policy deployments.
- Discover and monitor Docker containers and secure them with micro-segmentation.
- Virtual Machine-optimized threat defenses deliver multilayer countermeasures.
- Centralized management and automated workflows drastically reduce the complexity of hybrid and multi-cloud environments.
- Integration with automation tools like Chef and Puppet apply security to public and private cloud workloads at the time of deployment.

Connect With Us

Consolidate Events

McAfee Cloud Workload Security allows organizations to use a single interface to manage numerous countermeasure technologies for both on-premises and cloud environments. This also includes third-party technologies, like AWS GuardDuty. Administrators can leverage the continuous monitoring and unauthorized behaviors identified by AWS GuardDuty, providing yet another level of threat visibility. This integration allows McAfee Cloud Workload Security customers to view GuardDuty events, which include network connections, port probes, and DNS requests for EC2 instances, directly within the McAfee Cloud Workload Security console. GuardDuty network connection events are mapped in a flow graph when the traffic corresponds to traffic discovered by McAfee Cloud Workload Security.

Superior Virtualization Security

McAfee Cloud Workload Security protects your private cloud virtual machines from malware without straining underlying resources or requiring additional operating costs. You gain anti-malware protection that intelligently schedules resource-intensive tasks, such as on-demand scanning, when the hypervisor is not overloaded.

Network Visualization with Micro-Segmentation

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 helps alleviate the potential for configuration errors and increases the efficiency of remediation.

File Integrity Monitoring (FIM)

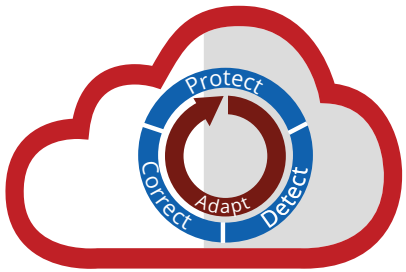
FIM continuously monitors to ensure your system files and directories have not been compromised by malware, hackers, or malicious insiders. Comprehensive audit details provide information about how files on server workloads are changing and alert you to the presence of an active attack.

Application Control

Application whitelisting prevents both known and unknown attacks by allowing only trusted applications to run while blocking any unauthorized payloads. 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.

Key Benefits continued

- Gain multi-layer protection from advanced malware and intrusion with ease of use.
- Visualize and discover network threats without installing an agent.
- Secure your environment by taking corrective actions directly from within the solution.



Cloud Workload Security

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

Simplify Management

Consistency Through Centralized Management

A single console provides consistent security policy and centralized management in multi-cloud environments across servers, virtual servers, and cloud workloads.

Role-based Controls

Define user roles more specifically and appropriately with the ability to create multiple role-based permissions in the McAfee® ePO™ platform.

Tag and Automate Workload Security

Assign the right policies to all workloads automatically with the ability to import AWS and Azure tag information into McAfee ePO software and assign policies based on those tags. Existing AWS and Azure tags synch with McAfee ePO software tags so they're automatically managed.

Automated Deployment

With support for deployment automation tools from organizations like Chef, Puppet, and Ansible, you can automatically deploy security technology in multiple cloud environments.

Auto-remediation

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

Cloud-native Build Support

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 Azure Kubernetes Service (AKS).

Improved Security Coverage

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

Features	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Centralized Management (McAfee ePO Platform)	✓	✓	✓
Role-based access controls allow multiple role-based permissions in the McAfee ePO console	✓	✓	✓
Multiple Cloud Support (AWS, Azure, VMware)	✓	✓	✓
Use Micro-segmentation to Quarantine Workloads and Containers	✓	✓	✓
Threat Prevention for Server OS (Windows and Linux)	✓	✓	✓
Host Intrusion and Exploit Prevention	✓	✓	✓
Cloud Encryption Management	✓	✓	✓
Native Firewall Management for AWS and Azure (Security Groups)	✓	✓	✓
McAfee® Management for Optimized Virtual Environments (Agentless and Multiplatform)	✓	✓	✓
Host-based Firewall	✓	✓	✓
Import AWS and Azure tag information into McAfee ePO software	✓	✓	✓
Auto-remediation on workloads which are non-compliant	✓	✓	✓
Adaptive Threat Protection with Machine Learning		✓	✓
Network Traffic Visualization and micro-segmentation		✓	✓
Cloud-native Network Traffic Analysis Combined with Global Threat Intelligence Reputation Score		✓	✓
McAfee® Virtual Network Security Platform Integration		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
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