McAfee Public Cloud Server Security Suite

Comprehensive security for AWS and Azure cloud-workloads

Key Advantages

- Designed for AWS and Azure workloads.
- Instant discovery.
- Security assessment and threat remediation.
- Scalable security.
- Comprehensive protection.
- Leverages the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console.
- Deployment options include Chef, Puppet, and OpsWorks.
- Demonstrate compliance.
- Integrates with other Intel Security solutions.

As enterprises shift their data center strategy to include and often lead with public cloud server instances, they are mindful that a shared responsibility model[1] for protection is a key consideration. Public cloud providers, like Amazon Web Services (AWS) and Microsoft Azure, protect the perimeter, and users must secure the content. But how can forward-thinking enterprises protect their cloud workloads against zero-day and advanced persistent threats (APTs) while keeping costs in line with their cloud strategy? Some of the key challenges for enterprises while adopting cloud are:

- It's getting harder to keep up with zero-day and advanced threats.
- Lack of visibility and centralized management make it extremely challenging with multiple cloud infrastructure.
- Performance degradation is a concern for cloud workload security.

McAfee® Public Cloud Server Security Suite offers instant discovery and control of AWS and Azure workloads and threats for complete, consistent, and continuous protection with minimal impact on performance. You can discover multiple cloud data centers, cloud accounts, virtual machines, and emerging threats.

The comprehensive security provided by McAfee Public Cloud Server Security Suite includes foundational antivirus and intrusion prevention along with advanced whitelisting to protect from zero-day threats, change control to meet regulatory compliance requirements, and encryption management for data protection. A single management console makes it easy to manage multiple clouds and enforce policies. Flexible deployment options with Chef, Puppet, and OpsWorks DevOps tools provide a seamless experience with minimal impact.

Figure 1. Single management console for multiple cloud infrastructures and multiple Intel Security technologies.

intel Security

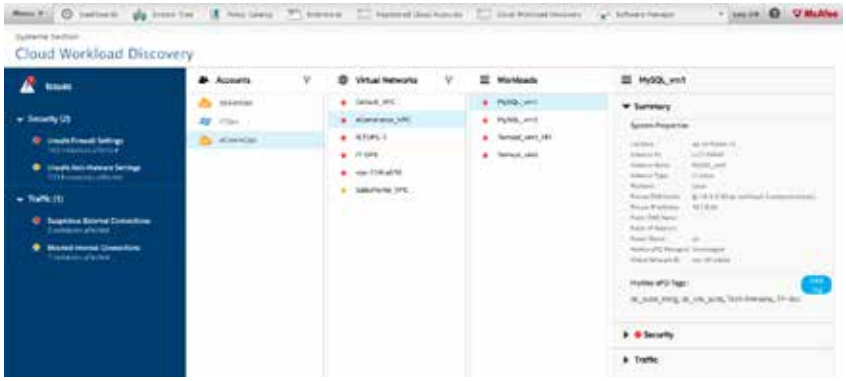

Figure 2. Discover and monitor multiple cloud infrastructures and emerging threats.

Supported Platforms

- Windows 2008, 2008 R2, 2012, 2012 R2
- Linux (Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

Discover Cloud infrastructures and Threats

To have better control over cloud infrastructure and threats you need better visibility across them.

- Discover all virtual networks or virtual private clouds (VPCs), templates, and workloads across AWS and Azure cloud infrastructure in minutes. Having detailed information about cloud infrastructure accounts, knowing which users have access to what parts of the cloud infrastructure, understanding how workloads are assigned to templates and VPCs, and having a quick snapshot of the system tree associated with cloud infrastructure are the first steps towards adequately protecting your cloud infrastructure.
- Get security visibility across multiple clouds in one place. Leverage end-to-end threat information, including attack sources for better security control.
- View traffic across workloads, and manage how information is flowing between them and is accessed from outside the organization.

Monitor the Cloud, and Take Faster Actions on Security Alerts

Because faster remediation is becoming increasingly important, with this solution you can quickly assess security issues at a deeper level and take immediate actions.

- Identify issues that require urgent attention, and take appropriate actions using color-coded threats.
- Create custom tags, and assign them to workloads based on your unique requirements.
- Take corrective measures to curb security issues, and adopt policies or define threat reputations to defend the infrastructure from future security incidents.
- Manage the cloud firewall with customized policies for individual workloads or groups of workloads. Manage policies for AWS Security Groups to control traffic for one or multiple instances.
- Identify suspicious traffic occurring in VPCs, and take remediation steps to block critical information from falling into the wrong hands

Comprehensive Threat Protection

McAfee Public Cloud Server Security Suite leverages a single agent that provides multiple layers of security that can be managed using a single management console across multiple cloud platforms. This solution can also be deployed with DevOps-friendly tools, thus providing the best possible experience.

To learn more

Visit product page: **http://www.mcafee.com/us/products/public-cloud-server-security-suite.aspx**.

Also available for purchase on **AWS Marketplace**.

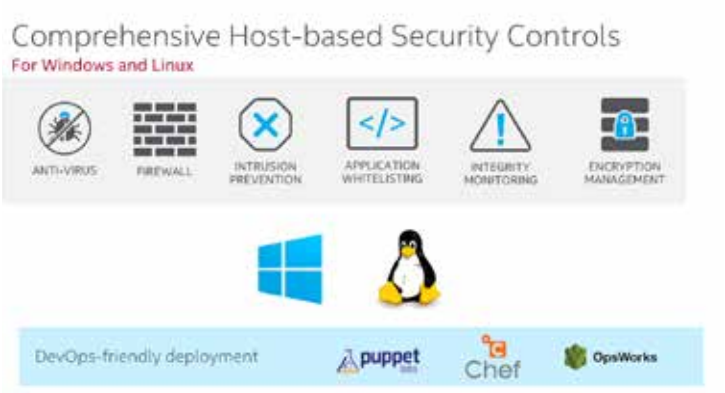

Figure 3. Comprehensive security for public cloud workloads.

Feature	Benefits
Chef, Puppet, and AWS OpsWorks deployment options	• DevOps deployment tools allow security to be considered ahead of time with ease of deployment. • Security can be built in as part of operations.
Cloud workload discovery	• Instant visibility into the cloud infrastructures discovers virtual data centers, cloud workloads, and cloud firewalls. • Quick threat alerts notification with automatic security posture assessment. • Faster remediation of threats with prioritized alerts based on the criticality of threats and steps to quickly act on those alerts.
Single management console for multiple cloud infrastructure security solutions (McAfee ePO software)	• Extremely beneficial for a hybrid environment setting. • Single-pane manageability for physical, virtual, and cloud workloads and policies. • Integrates Intel Security and partner's cloud and on-premises security technologies • Lowers total cost of ownership with integrated security processes and quick resolution steps
Anti-malware	• Maximum defense against malware. Safeguards systems and files from viruses, spyware, worms, Trojans, and other security risks. It detects and cleans malware, and allows users to easily configure policies to manage quarantined items.
Host firewall	• Protect workloads from unauthorized access and attack.
Host intrusion prevention	• Blocks unwanted or harmful network traffic, and proactively blocks zero-day and known attacks with patented, award-winning technology. • Prevents unwanted changes to workloads by restricting access to specified ports, files, shares, registry keys, and registry values. • Memory protection prevents abnormal programs or threats from overrunning the buffer's boundary and overwriting adjacent memory while writing data to a buffer. Exploited buffer overflows can execute arbitrary code on your computer.
Application whitelisting	• Protects against zero-day and advanced persistent threats without signature updates. • Strengthens security and lowers ownership costs with dynamic whitelisting, which automatically accepts new software added through trusted channels. • Reduces patch cycles through secure application whitelisting and advanced memory protection.
File integrity monitoring	• Provides continuous detection of system-level changes across distributed and remote locations. • Prevents tampering by blocking unauthorized changes to critical system files, directories, and configurations. • Tracks and validates every attempted change in real time on the workload, enforcing change policy by a time window, source, or an approved work ticket.
Encryption management	• Encrypts data stored in AWS EBS volumes with AWS Advanced Encryption Standard (AES). • Volumes with pre-existing data can be encrypted conveniently. • Integrates with Amazon's Key Management Service (KMS) for encryption.

1. **http://www.mcafee.com/us/resources/white-papers/wp-cloud-security-primer-techtarget.pdf**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com