McAfee

Together is power.

McAfee Server Security Suite Advanced

Comprehensive security for physical, virtual, and cloud deployments with whitelisting and change control.

In today's complex IT environment, it's getting harder to protect new servers and cloud workloads from increasingly sophisticated threats without a holistic approach. McAfee® Server Security Suite Advanced offers consistent and continuous protection across physical, virtual, and public cloud deployments. Comprehensive security includes foundational antivirus, firewall protection, intrusion prevention, whitelisting to protect from zero-day threats, and change control to meet regulatory compliance requirements. Advanced protection minimizes performance impact on physical and virtual servers and auto-scales with your dynamic cloud workloads.

Instant Discovery and Control

Tracking down security gaps in your ever-expanding hybrid data center does not have to be hard, thanks to Cloud Workload Discovery for hybrid cloud, a key feature of McAfee Server Security Suite Advanced. Cloud Workload Discovery for hybrid cloud, covering VMware, OpenStack, AWS, and Microsoft Azure, provides end-to-end visibility into all workloads and their underlying platforms. Insights into weak security controls, unsafe firewalls and encryption settings, and indicators of compromise, such as suspicious traffic, lead to faster detection. McAfee® ePolicy Orchestrator® (McAfee ePO™) software or DevOps tools enable quick remediation.

Cloud security can be challenging because there are a lot of different cloud workloads with unique risk profiles and security requirements. Cloud Workload Discovery's policy-driven assessment makes it easy to compare exactly what security controls these diverse workloads require, versus what they actually have, to ensure adequate protection and compliance. Once you have discovered security risks, you can move to complete protection with just a few clicks.

Cloud Workload Discovery's integration with the McAfee ePO management console gives organizations effective control to help implement secure solutions across physical, virtual, and cloud environments. With this

Key Advantages

- Unifies security management across endpoints, networks, data, and compliance solutions from McAfee and third-party solutions through McAfee ePO software
- Provides deep visibility, risk assessment, and remediation through Cloud Workload Discovery for hybrid cloud
- Combines blacklisting and intrusion prevention with advanced whitelisting and change control to protect physical and virtual servers from malware
  - Protects from unknown threats by preventing unwanted applications from running
  - Continuously detects system-level changes across distributed and remote locations to help meet compliance requirements
- Blocks zero-day, unknown threats in seconds using local reputation data combined with sandbox analytics
- Delivers optimized physical and virtual security with minimal performance impact

integration, security administrators can use a single management platform with simplified workflows to address threat alerts and enforce policies, reducing the time to identify and resolve security issues.

McAfee Server Security Suite Advanced assures that dynamic cloud environments that support DevOps don't sacrifice security for agility. Our security scales elastically with cloud workloads so that you're always protected. With elastic provisioning in private clouds, offline scan servers can be automatically added to or removed from the resource pool as workloads are spun up or down. For AWS and Azure workloads, users can configure security at the template level so that it auto-scales with changing workloads.

Comprehensive Protection

McAfee Server Security Suite Advanced offers the most comprehensive protection for your servers, whether physical, virtual, or in the cloud. In addition, its protection against memory buffer overflow attacks on Windows 32- and 64-bit systems, along with a unique combination

Figure 1. Derive a sustainable advantage with Cloud Workload Discovery.

of blacklisting, whitelisting, and change control, are unmatched in the industry. The suite includes:

- **McAfee Application Control for Servers:** This whitelisting solution allows only authorized software to run on servers to protect against unknown malware and zero-day and advanced threats. This centrally managed whitelisting solution uses a dynamic trust model to eliminate labor-intensive list management.

- **McAfee Change Control for Servers:** Provides continuous detection of system-level changes across distributed and remote locations to help ensure compliance with laws and regulations, such as Sarbanes Oxley and Payment Card Industry Data Security Standard (PCI DSS)

- **McAfee Endpoint Security Threat Prevention:** Part of a collaborative, extensible framework that protects Microsoft Windows and Linux servers against zero-day exploits and advanced attacks

- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus):** This anti-malware solution is designed specifically for virtual environments. It is available as an agentless, tuned option for VMware NSX and VMware vCNS and as a multiplatform option that can be deployed for all major hypervisors, including Microsoft Hyper-V, VMware, KVM, and Xen.

- **McAfee Host Intrusion Prevention for Servers:** Safeguards businesses against complex security threats by monitoring the behavior of code on your server, analyzing events for suspicious activity
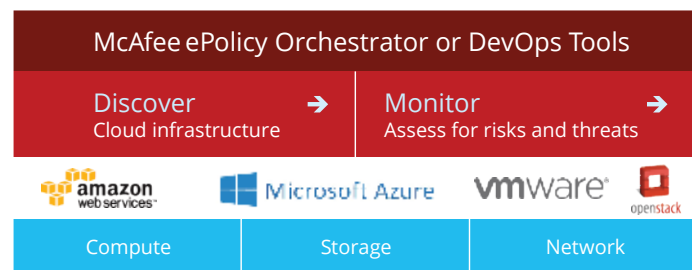
- McAfee Endpoint Security Firewall: Monitors network and internet traffic and intercepts suspicious communications

McAfee Server Security Suite Advanced can enhance global reputation intelligence from McAfee Global Threat Intelligence (McAfee GTI) with local data from McAfee Threat Intelligence Exchange, an additional module sold separately, to instantly identify and combat the ever-increasing unique malware samples. Using McAfee Threat Intelligence Exchange, solutions in the suite coordinate with McAfee Advanced Threat Defense to dynamically analyze the behavior of unknown applications in a sandbox and automatically immunize all endpoints from newly detected malware.

McAfee partners with Rapid7 for vulnerability management. Rapid7's Nexpose solution discovers and prioritizes vulnerabilities and confirms when exposures are fixed.

Minimal Performance Impact

Although security is top of mind for most companies, some are hesitant to move forward with server protection due to concerns over its impact on performance. McAfee Server Security Suite Advanced makes it possible to protect your physical and virtual servers without sacrificing performance even when scanning for malware.

Unlike many anti-malware products, McAfee Endpoint Security and McAfee MOVE AntiVirus don't make significant demands on computing resources. McAfee Endpoint Security provides fast scans and optimizes its use of CPU and memory while protecting better than other anti-malware products. McAfee MOVE AntiVirus offloads malware scanning from virtual machines for instant protection with low impact on memory and processing. Separate policies for on-access and on-demand scanning allow greater control of performance turning and security.

Optimize Your Server Security, Optimize Your Business

The enormous potential of virtualization and cloud computing is only fully realized if both are sufficiently secured. McAfee provides server security solutions that support options for growth as organizations move forward. Whether physical, virtual, or in the cloud, we offer a suite of solutions to keep servers and cloud workloads secure in increasingly dynamic environments.

Feature	Why You Need It
Single-console management	• Centrally manage physical, virtual, and cloud deployments for better security control, including policy management, deployment, visibility, and security management across all platforms. • Simplify operational aspects and time investment for administrative staff.
Instant discovery and control	• Discover physical servers and get a complete view into your VMware vSphere, OpenStack, AWS, and Microsoft Azure workloads and platforms. • Make sure that you are always protected with security that scales elastically with your dynamic cloud workloads.
Virtualization security	• Optimize security of workloads deployed in virtual infrastructures without compromising performance and resource utilization. • Choose multiplatform (all major hypervisors) or agentless deployment for VMware NSX and VMware vCNS to deliver great performance and virtual machine density.
Public cloud security	• Audit platform security, including firewall and encryption settings, for AWS and Microsoft Azure. • Ensure complete protection with traffic and network threat visibility for AWS.
Application whitelisting	• Significantly lower host performance impact over traditional server security controls. • Protect against zero-day and advanced persistent threats (APTs) without signature updates, resulting in quicker time-to-protection. • Lower operational overhead with dynamic whitelisting.
Change control	• Prevent tampering by blocking unauthorized changes to critical system files, directories, and configurations, saving time for administrators in troubleshooting security breaches. • Track and validate every attempted change in real time on the server, enforcing change policy by a time window, source, or approved work ticket.
Core server protection	• Implement anti-malware protection that protects against zero-day exploits and advanced attacks. • Safeguard against complex security threats that may otherwise be unintentionally introduced or allowed with McAfee Host Intrusion Prevention System.
Local reputation intelligence	• Block zero-day, unknown threats in seconds through integration with McAfee Threat Intelligence Exchange (an additional module sold separately).

Learn More

Learn more about the benefits of McAfee Server Security Suite Advanced at

http://www.mcafee.com/us/products/server-security-suite-advanced.aspx.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com