McAfee Server Security Suite Advanced

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

Key Advantages

- Secures all physical and virtual assets, including those in the cloud with single-pane-of-glass management from a central console.
- Provides end-to-end visibility into the security status of all virtual machines in the private cloud through McAfee Data Center Connectors for VMware vSphere and OpenStack.
- Offers public cloud visibility, assessment, and remediation through Cloud Workload Discovery for Amazon Web Services (AWS) and Microsoft Azure.
- 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.

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 instant discovery and control for consistent and continuous protection across physical, virtual, and public cloud deployments. Comprehensive security includes foundational antivirus and 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

Lack of centralized management and visibility makes it nearly impossible to discover all servers and workloads and then apply proper security policies across physical, virtual, and cloud deployments. We make protection of all these environments easy with a single console—McAfee® ePolicy Orchestrator® (McAfee ePO™) software—to centrally manage all Intel Security solutions, provide end-to-end visibility, and report on security and compliance issues. McAfee Data Center Connectors for VMware vSphere and OpenStack provide a complete view of private cloud environments to monitor virtual machine state and apply granular security policies. Cloud Workload Discovery for AWS and Microsoft Azure offer full visibility into infrastructure, workloads, traffic, and threats to ensure complete protection. Cloud Workload Discovery also automates security posture assessment of AWS security groups to identify unsafe firewall, encryption, and anti-malware settings and lets users discover Amazon Elastic Block Store (Amazon EBS) storage volumes. Users can then encrypt these volumes with just a few clicks using McAfee ePO software.

McAfee Server Security 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 scanning demand fluctuates. For AWS and Azure workloads, users can configure security at the template level so that it auto-scales as workloads are spun up or down.

intel Security

Key Advantages, cont.

- 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.

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

- **McAfee Application Control for Servers:** A whitelisting solution that 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 VirusScan® Enterprise:** A traditional anti-malware solution for Microsoft Windows and Linux servers that protects against zero-day exploits and advanced attacks.
- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus):** An anti-malware solution 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 Server Security Suite Advanced can enhance global reputation intelligence from McAfee Global Threat Intelligence (McAfee GTI) with local data from McAfee Threat Intelligence Exchange (McAfee TIE), an additional module sold separately, to instantly identify and combat the ever-increasing unique malware samples. Using McAfee TIE, 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.

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 VirusScan Enterprise and McAfee MOVE AntiVirus don't make significant demands on computing resources. McAfee VirusScan Enterprise scans faster, uses less memory, and requires fewer CPU cycles 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. Intel Security 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.

Learn more about the benefits of McAfee Server Security Suite Advanced at **http://www.mcafee.com/us/products/server-security-suite-advanced.aspx**.

Feature	Why You Need It
Single-console management	• Obtain single-pane-of-glass manageability and end-to-end visibility for physical and virtual servers in the private and public cloud for greater protection. • Establish a common security posture across physical and cloud deployments. • 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 environments. • 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	• Ensure complete protection with visibility into AWS and Microsoft Azure infrastructure, workloads, traffic, and threats. • Automate security posture assessment of AWS security groups. • Discover and encrypt Amazon EBS storage volumes.
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 for physical servers 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 TIE (an additional module sold separately).

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

62502ds_sss-advanced_0616_ETMG