McAfee Server Security Suite Advanced

Advanced server security for physical, virtual, and cloud deployments with whitelisting

The data center has been in the midst of major transition over the last few years across storage, server, networks, and the applications it delivers. The diverse nature of the data center and the rapid evolution towards cloud computing require new ways to secure this environment. The challenge for enterprise IT and security professionals is to create a unified and strong security posture for physical, virtualized, and cloud environments to help ensure agility and cost effectiveness. McAfee® Server Security Suite Advanced delivers the most comprehensive server protection and management for physical, virtual, and cloud deployments while providing additional advanced server security, such as whitelisting and change control, to help maintain compliance.

Key Advantages

- Discover all physical and virtual assets, including those in the cloud with single-pane management from a central console.
- The unique combination of blacklisting and whitelisting protects physical and virtual servers from malware. Virtualization security is optimized for minimal performance impact, and you are ensured that only trusted virtual machines are running.
- Connect public cloud credentials with McAfee ePO software through McAfee Data Center Connector for Amazon Web Services and get complete visibility into VMware vSphere environments with McAfee Data Center Connector for VMware vSphere.
- Protect from unknown threats by ensuring that hosts are kept secure by preventing unwanted applications from running.
- Continuous detection of system-level changes across distributed and remote locations helps you meet compliance requirements.

Discover All Workloads

It is often a challenge to discover workloads so that you can apply the proper security policies across physical, virtual and cloud deployments. Through connectors into McAfee® ePolicy Orchestrator® (McAfee ePO™) software, McAfee Server Security Suite Advanced enables you to discover physical and virtual servers. In addition, with McAfee Data Center Connector for VMware vSphere, you get visibility into private cloud environments to see the ESXi to vCenter relationship, as well as determining the host on which a given machine is running. This enables you to monitor virtual machines so you can apply fine-grained policy management as a means of delivering a strong security posture across virtual machines.

Protect Servers

McAfee Server Security Suite Advanced adds McAfee Application Control, a whitelisting solution that allows only authorized software to run on system devices. Whitelisting significantly lowers host performance impact by protecting against zero-day and advanced persistent threats without signature updates.

The suite offers traditional anti-malware solutions for Microsoft Windows and Linux servers, including McAfee VirusScan® Enterprise, ranked number one by NSS Labs against zero-day exploits and evasion attacks. In addition to traditional anti-malware, the suite also offers a separate solution specialized for virtual environments. McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus optimizes antivirus for those virtualized environments, minimizing performance impact and providing support for all major hypervisors.

Though antivirus is key to security, additional solutions may be necessary to protect against advanced threats. McAfee Host Intrusion Prevention safeguards business against complex security threats that may otherwise be unintentionally introduced or allowed. Moreover, Intel Trusted Execution Technology (TXT) attests that only trusted and certified applications are able to boot up. The Intel partnership also allows McAfee to offer hardware-assisted security for physical servers through McAfee Deep Defender, which goes below the operating system to address the most sophisticated attacks of both today and the future.

Expand into the Cloud

As you expand into the cloud, it is increasingly difficult to ensure that proper security policies are applied to newly provisioned workloads. McAfee addresses these challenges by automatically discovering virtual machines as they are provisioned in the private cloud with McAfee Data Center Connector for VMware vSphere, which can then be protected automatically with appropriate security policies. McAfee Data Center Connector for Amazon Web Services allows for visibility into these environments, easing concerns associated with the shift to the public cloud. You can register

an Amazon Web Services account in McAfee ePO software and discover both running and stopped virtual machines. In addition, you can gain full visibility of protection status and security incidents in Amazon Web Services environments by deploying and configuring McAfee security solutions using the McAfee Data Center Security Dashboard.

Optimize Your Servers, Optimize Your Business

The enormous potential of virtualization and cloud computing can only be fully realized if they are sufficiently secured. McAfee provides server security solutions that support options for growth as organizations move forward. Whether physical, virtualized, or in the cloud, McAfee offers a suite of solutions to keep servers secure while maintaining flexibility. McAfee Server Security Suite Advanced delivers physical, virtual, and cloud server security with advanced solutions to establish and maintain a strong security posture across an organization.

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
Whitelisting	• Significantly lower host performance impact over traditional endpoint security controls. • The industry's strongest malware protection, which allows only authorized software to run on devices that use the solution.
File integrity	• Prevents tampering by blocking unauthorized changes to critical system files, directories, and configurations. • Tracks and validates every attempted change in real time on the server.
Single-console management	• Single-pane management for physical and virtual servers, including those in the private and public cloud. • Create a data center dashboard within McAfee ePO software.
Core server protection	• A highly effective set of core antivirus technologies designed to block threats to servers. In addition, McAfee Host Intrusion Prevention safeguards businesses against complex security threats.
Virtualization security	• Improve security of virtual workloads without compromising advantages of performance and resource utilization. • Agentless and multiplatform deployment choices: ◦ Agentless deployment for VMware environments means no McAfee agents are installed in each virtual machine and no agent updates are needed; this reduces complexity and greatly improves usability. ◦ Multiplatform deployment for mixed-vendor virtualization environments (VMware, Citrix, and others). • Use Intel TXT to verify that only trusted applications are referenced when booting VMware ESXi hypervisors on host servers for attestation.
Full visibility of virtual machines in the private and public cloud	• Automatically discover virtual machines in the private cloud (VMware vSphere). View Amazon Web Services environments to expand visibility to the public cloud.
Hardware-assisted protection	• Protection beyond the operating system provides significantly greater security coverage against the most advanced rootkits for physical servers. This was developed in concert with Intel to address the most sophisticated attacks, including stealth malware.

McAfee
An Intel Company

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

60764ds_sss-adv_0114_fnl_ETMG