Data Sheet

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.

Discover All Workloads

It is often a challenge to discover all workloads and then apply the proper security policies across physical, virtual, and cloud deployments. Manageability is easy with scan reports that let you detect unprotected endpoints and determine security compliance. Through connectors for McAfee® ePolicy Orchestrator® (McAfee ePO™) software, McAfee Server Security Suite Advanced enables you to discover all physical and virtual servers including those in the private and public cloud. The solution also includes McAfee Data Center Connectors for VMware vSphere, Amazon AWS, Open Stack, and Microsoft Azure. Together, these enable you to monitor all virtual machines both on-premises and off-premises and apply fine-grained security policies that deliver a strong security posture. The dashboards provide security posture including operating system memory protection, hypervisor host to virtual machine relationships, the location where each virtual machine is located, and more.

Protect Servers

The McAfee Server Security Suite Advanced offers the most comprehensive protection for your servers, whether physical, virtualized or in the cloud. In addition, it provides change control and a unique combination of blacklisting and whitelisting protection technologies unmatched in the industry.

McAfee Server Security Suite Advanced includes McAfee Application Control for Servers, a whitelisting solution that allows only authorized software to run on servers. This centrally managed whitelisting solution uses a dynamic trust model and innovative security features that block unauthorized applications and foil

Key Advantages

- Discovers all physical and virtual assets, including those in the cloud with single-pane management from a central console.
- Combines blacklisting and whitelisting to protect physical and virtual servers from malware.
    - Delivers dynamic whitelisting to protect from unknown threats by ensuring that hosts are kept secure by preventing unwanted applications from running via McAfee Application Control for Servers.
    - Detects continuously system-level changes across distributed and remote locations to help meet compliance requirements.
- Delivers optimized virtualization security for minimal performance impact, with McAfee MOVE AntiVirus.
- Ensures that only trusted virtual machines are running.
- Provides complete visibility into security status of all virtual machines in the private and public cloud through McAfee Data Center Connectors for VMware vSphere, Amazon Web Services, OpenStack, and Microsoft Azure.
- An agentless host-based firewall which leverages VMware vCNS App to organize virtual machines into secure network groups or to isolate them.

advanced persistent threats (APTs)—without labor-intensive lists to manage. Whitelisting significantly lowers host performance impact through protection against threats without signature updates.

As part of the core server protection, the suite offers traditional anti-malware solutions for Microsoft Windows and Linux servers, including McAfee VirusScan® Enterprise software, 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 virtualized environments, minimizing performance impact even for very large environments and providing support for all major hypervisors. McAfee MOVE AntiVirus is available as an agentless, tuned option for VMware deployment environments or a multiplatform option that can be deployed for KVM, Microsoft Hyper-V, VMware, and Xen based hypervisor environments.

Establishing trusted compute pools with Intel® Trusted Execution Technology (Intel® TXT), a feature of the Intel® Xeon® processor, is critical in a highly virtualized data center. Intel TXT establishes a root of trust through measurements when the hardware and pre-launch software components are in a known good state. McAfee Boot Attestation service utilizes Intel Trusted Execution Technology (TXT) to determine the trustworthiness of the hypervisors boot with display of the trust status in McAfee ePO software. With the information about the trust status, a security administrator is able to create policies such as “secure VM policies” based on the status that can be used for compliance and regulatory reporting.

Though antivirus is key to security, additional solutions may be necessary to protect against advanced threats. McAfee Host Intrusion Prevention safeguards businesses against complex security threats that may otherwise be unintentionally introduced or allowed.

McAfee Agentless Firewall is now available due to integration with VMware’s vCNS App firewall. It allows the admin to manage one or more VMware vShield App Firewall instances, all within the McAfee ePO platform, and provides a single interface for managing firewall policies across virtual data centers. This extension also provides an easy-to-use workflow for users to isolate groups of resources without the need to manually create complex individual firewall rules. In addition, it can detect any modifications made by other tools, and provide the admin with a simple one-click repair option.

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 both running and stopped virtual machines with McAfee Data Center Connectors as they are provisioned in the private and public clouds. To enable that, you simply register a public cloud account in the McAfee ePO platform. Virtual machines can then be protected automatically with appropriate security policies. In addition, the McAfee Data Center Security dashboard provides full visibility of protection status and security incidents in your private and public clouds.

Optimize Your Servers, 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, 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
Application whitelisting	• Significantly lower host performance impact over traditional endpoint security controls. • Protects against zero-day and APTs without signature updates resulting in quicker time-to-protection. • Dynamic whitelisting requires lower operational overhead compared to legacy whitelisting techniques.
Change control	• Prevents tampering by blocking unauthorized changes to critical system files, directories, and configurations, saving time for administrators in troubleshooting security breaches. • Tracks and validates every attempted change in real time on the server, enforcing change policy by a time window, source, or approved work ticket. • Continuous control minimizes the impact from ad hoc or unauthorized changes.
McAfee Agentless Firewall	• Allows visibility into all virtual network isolations via McAfee ePO reports. • Ability to control and isolate virtual machines and data due to integration with VMware vCNS App Firewall.
Single-console management	• Single-pane manageability for physical and virtual servers including those in the private and public cloud for greater security visibility. • Simplify operational aspects and time investment for administrative staff. • Lower hardware costs due to reduced server footprints needed.
Core server protection	• Anti-malware protection for physical servers that is number one ranked by NSS Labs[1] against zero-day exploits and evasion attacks. • Host Intrusion Prevention (HIPS) safeguards business against complex security threats that may otherwise be unintentionally introduced or allowed.
Virtualization security	• Optimized security of workloads deployed in virtual infrastructures without compromising performance and resource utilization. • Protection for multiple hypervisors in the data center to have a common security posture for all types of hypervisors used. • Optimized agentless deployment for VMware based environment to help deliver great performance and VM density. • McAfee Boot Attestation Service that utilizes Intel TXT to determine trust worthiness of VMware ESXi hypervisor boot with display of trust status in McAfee ePO software and the ability to create policies based on the status that can be used for compliance and regulatory reporting.
Full visibility of virtual machines in the private and public cloud	• Discover not just physical servers but also hypervisors and virtual machines in the VMware vSphere, Amazon AWS, OpenStack, and Microsoft Azure environment for full visibility of what needs to be secured. • Discover when virtual machines are provisioned which can then be automatically protected with security policies to ensure proper security posture for these virtual machines.

[1] NSS Labs, Inc. Protection & Evasion Test, 2013

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