McAfee Server Security Suite Essentials

Foundational Server Security for Physical, Virtual, and Cloud Deployments

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 Essentials addresses these concerns by integrating the essential security components to discover workloads in the cloud, protect servers, and expand security into the cloud.

Key Advantages

- Discovers all physical and virtual assets, including those in the cloud, with single-pane management from a central console.
- 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.

Discover All Workloads

It is often a challenge to discover all workloads and then to 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 Essentials enables you to discover all physical and virtual servers including those in the private and public cloud. Included are McAfee Data Center Connectors for VMware vSphere, Amazon AWS, OpenStack, and Microsoft Azure. These enable you to monitor each virtual machine—on premises and off premises— and apply fine-grained policy management that delivers strong security posture. Additional visibility includes OS memory protection, the ability to see which host each virtual machine is running, in which data center or in what cloud each virtual machine located, and more.

Protect Servers

McAfee Server Security Suite Essentials includes McAfee VirusScan® Enterprise software, ranked number-one by NSS Labs against zero-day exploits and evasion attacks.[1] 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 technology for virtualized environments, minimizing performance impact even for very large and dynamic 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 Security

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 TXT to determine the trustworthiness of the hypervisor's 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 is included to safeguard businesses against complex security threats that may otherwise be unintentionally introduced or allowed.

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 McAfee ePO software. 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.

Feature	Why You Need It
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 ranked #1 by NSS Labs 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 trustworthiness of VMware ESXi hypervisor boot with display of trust status in McAfee ePO software and 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.

Optimize Your Servers, Optimize Your Business

The enormous potential of virtualization and cloud computing is only fully realized if they are sufficiently secured. McAfee provides server security solutions that will not hinder the 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 Essentials delivers the essential foundation for physical, virtual, and cloud server security.

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

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