Solution Brief

Future-Focused Security

Life after Microsoft Windows Server 2003 EOS

You migrated from Microsoft Windows Server 2003 for good reasons. To prevent immediate security threats. To take advantage of new capabilities. And to set your business up for success long into the future. Now is the opportune time to evaluate technologies that will enable your business to do it all.

Whether you've migrated your Windows 2003 workloads to Windows Server 2012 R2 in a physical or virtual environment, or migrated workloads to the public cloud, Intel Security offers an end-to-end solutions portfolio to satisfy your migration path. Intel Security has developed specific recommendations to ensure that your business can migrate securely—whichever migration path you've chosen.

As you build out your new environment, use this brief to understand how to optimize your environment for a secure and productive future.

Path 1: Upgrading to a Modern Physical Server Environment

Running Windows Server 2012 R2 in a physical environment offers several benefits, including improved manageability through PowerShell enhancements, greater ease of access from server-side technologies, and an updated Server Message Block protocol extending support to commodity hardware and storage devices. But leveraging these new and improved capabilities requires security that can keep pace with what is possible.

Intel Security offers innovative and integrated solution suites that empower you to both secure and optimize your physical environment.

McAfee® Server Security Suite Essentials provides complete security visibility and protects workloads with desired security policies, enabling you to:

- Discover all physical servers with single-pane management from a central console.
- Import physical server instances.
- Apply security policies for comprehensive protection.

McAfee Server Security Suite Advanced builds on the capabilities of McAfee Server Security Suite Essentials, delivering the most comprehensive server protection and management for physical deployments.

- Protect your traditional endpoints with highly effective anti-malware and antivirus security.
- Safeguard against known and zero-day attacks.
- Defend servers from unknown, advanced persistent threats through centrally managed whitelisting.

As you secure your Windows Server 2012 R2 environment, you may have certain security solutions already in place but lack comprehensive protection. Intel Security can help you fill those gaps.

For advanced desktop and file server protection
McAfee VirusScan® Enterprise is on the front line to keep viruses and other threats out of your Windows operating systems.

McAfee Host Intrusion Prevention for Desktop safeguards your desktops and laptops against complex security threats that may be unintentionally introduced or allowed.

For improved application and change control
McAfee Application Control blocks unauthorized executables on servers, corporate desktops, and fixed-function devices.

McAfee Change Control eliminates change activity in server environments that can lead to security breaches, data loss, and outages, making it easier to meet regulatory compliance requirements with confidence.

Path 2: Migrating Physical Workloads to a Virtualized Environment

Microsoft designed Windows Server 2012 R2 to support private cloud-based deployments, offering a truly mature hypervisor product to Microsoft customers. In addition to numerous improvements for boosting Hyper-V capabilities and Microsoft Active Directory consistency, Windows Server 2012 R2 makes it possible to connect virtual machines (VMs) to a physical network, adding flexibility as to where VMs can be deployed. This presents greater virtualization possibilities than ever before and, at the same time, greater security questions.

Intel Security offers innovative and integrated solution suites that empower you to both secure and optimize your virtual environment.

McAfee Server Security Suite Essentials delivers foundational server security protection and management for virtual deployments, enabling you to:

- Optimize virus protection with one efficient server antivirus solution.
- Gain complete visibility into all virtual networks.
- Easily manage VMs with a single console.

McAfee Server Security Suite Advanced builds on the capabilities of McAfee Server Security Suite Essentials, delivering the most comprehensive server protection and management for virtual deployments.

- Gain dynamic blacklisting and whitelisting to protect servers from malware.
- Achieve optimized virtualization security with minimal performance impact.

As you secure your Windows Server 2012 R2 environment, you may have certain security solutions already in place but lack comprehensive protection. Intel Security can help you fill those gaps.

For optimized security in virtualized environments
McAfee Management for Optimized Virtual Environments (McAfee MOVE) AntiVirus brings advanced virus protection to virtualized desktops and servers, both on premises and in the cloud.

For greater VM visibility
McAfee Data Center Connector for vSphere enables you to discover and import your virtual infrastructure from the cloud into McAfee® ePolicy Orchestrator® (McAfee ePO™) software.

Use Case: Managing Windows Server 2003 Phase-Out

An internationally known, multibillion-dollar manufacturing company is intent on phasing out more than 5,000 Windows Server 2003 servers over the next three years. Already a satisfied Intel Security customer for endpoint solutions, the company enlisted Intel Security to develop a solution based on moving to a virtualized server resource pooling.

Intel Security offered a two-phased approach: cost effectively secure Windows Server 2003 servers with McAfee Application Control and McAfee Change Control in the near term; then, as physical servers dwindle, add licenses of McAfee MOVE AntiVirus to support the company's increasingly virtualized infrastructure.

Intel Security also helped the company model their needs and their use of each product over time, empowering the company to administer their pool without risking under-deployment or over-deployment of any solution.

Path 3: Migrating On-Premises Server Workloads to the Public Cloud

Migrating workloads to the public cloud can be advantageous for businesses interested in lowering capital expenditures and boosting scalability. However, whether you opt for Microsoft Azure, Amazon Web Services (AWS), or another platform, the public cloud's shared security model warrants additional security from the operating system level and above.

Intel Security offers innovative solution suites and tailored technologies that empower you to further secure your public cloud environment.

Securing Infrastructure-as-a-Service (IaaS)
McAfee Public Cloud Server Security Suite delivers comprehensive cloud security to help extend and manage security policies for servers in AWS, Azure, and other public clouds.

McAfee Server Security Suite Advanced builds on the capabilities of McAfee Server Security Suite Essentials, delivering the most comprehensive server protection and management for public cloud deployments.

McAfee Application Control blocks unauthorized executables on servers, corporate desktops, and fixed-function devices.

McAfee Change Control eliminates change activity in server environments that can lead to security breaches, data loss, and outages, making it easier to meet regulatory compliance requirements with confidence.

McAfee Data Center Connectors enable you to discover and import your virtual infrastructure from the public cloud into McAfee ePO software. You can then view virtualization properties and protection status of your VMs wherever they are. McAfee Data Center Connectors are available for Azure, AWS, OpenStack, and vSphere.

McAfee Data Protection for Cloud encrypts data to protect it from data theft and data loss, exclusively for Amazon Elastic Book Store (EBS) volumes.

Securing Software-as-a-Service (SaaS)
McAfee Security for Email Servers provides award-winning in-memory and incremental on-demand scanning to remove viruses, worms, Trojans, phishing, and other threats from incoming and outgoing email—in real time, 24/7.

Optimizing Security at the Application Level

As you continue on your migration path, it's important to also consider your business-critical applications. Intel Security offers industry-leading solutions for databases, Microsoft SharePoint, and email protection.

For databases
McAfee Data Center Security Suite for Databases provides you with complete visibility into your database landscape and security posture to fully align database security policy administration while efficiently maintaining regulatory compliance. No architecture changes, costly hardware, or database downtime required.

For Microsoft SharePoint
McAfee Security for Microsoft SharePoint ensures that your corporate SharePoint deployment does not spread malware, store inappropriate content, or lead to data loss.

For email
McAfee Security for Email Servers provides comprehensive content security, including detecting and blocking viruses, spam, and other unwanted programs on inbound and outbound emails on Microsoft Exchange and Lotus Domino servers.

You've Made Your Move. Now Achieve Integrated Security.

Now that you've moved from the immediate risk of running Windows Server 2003 to the tangible reward of your new environment, make the most of your decision by fully securing it. Whichever path you've chosen, Intel Security can help you secure and optimize it.

For more information, please visit **www.mcafee.com/windowsserver2003eos**.

62159brf_migrated-windows-2003-eos_1115_ETMG

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