Solution Brief

The 1-2-3 Security Approach for Windows Server 2003 EOS

Prepare now for Windows Server 2003 end of support.

End of Support (EOS) Is Coming

As of July 14, 2015, Microsoft Windows Server 2003 is no longer supported. If your business still runs server instances on Windows 2003, that means big changes.

- **No support.** There will be no patches or security updates for Windows Server 2003, compared to the 37 critical security updates issued in 2013 alone.
- **No compliance.** Your business will no longer pass a compliance audit, and without compliance, you will no longer be able to do business with Visa, MasterCard, and other providers.
- **No protection.** Your physical and virtualized server instances will be vulnerable to any new security threats.

What You Can Do

Reaching EOS is not the end of the world, but it does require attention. It may even create advantages, as migrating to newer solutions can result in new efficiencies, improved performance, reduced maintenance costs, and increased agility—while keeping your business safer.

Three migration paths

Three migration paths are available to your business. After taking an inventory of all Windows 2003 servers and the applications deployed on them, you can select the best migration path for each application.

- **Path #1: Upgrade to a newer version of Windows Server.** Microsoft recommends upgrading to Windows Server 2012 R2. This path includes virtual servers in the private cloud.
- **Path #2: Migrate workloads to the public cloud.** Microsoft recommends Microsoft Azure. Other public cloud options, such as Amazon Web Services, are also available.
- **Path #3: Delay migration.** Continue using Windows Server 2003 for now and upgrade at a later time.

Prioritize security for your business

Before choosing the right migration path, or paths, for your business, it is essential to recognize the security concerns associated with each option:

- **Path #1:** How should you protect server workloads—including virtualized and in the cloud? What is the best way to protect hybrid compute environments?

Know the Risks

As of July 14, 2015, businesses running Windows Server 2003 no longer receive security updates to protect them from malware. That raises a significant security concern, especially given the rising number and sophistication of malware attacks:[1]

- Average of 345,000 unique malware samples each day (about 240/minute).
- Over 260 million samples in the Intel® Security malware zoo as of July 1, 2014.

- **Path #2:** How should you protect server workloads running in the public cloud? How do you secure Infrastructure-as-a-Service (IaaS) and/or Software-as-a-Service (SaaS) environments?
- **Path #3:** Are there add-on security solutions available, since Microsoft no longer issues security updates? Which solutions offer the most value and will keep applications safest?

The Intel Security Recommendations to Secure the Server Environment after Migration

Intel Security has developed specific recommendations to ensure that your business can migrate securely—whichever migration path(s) you choose.

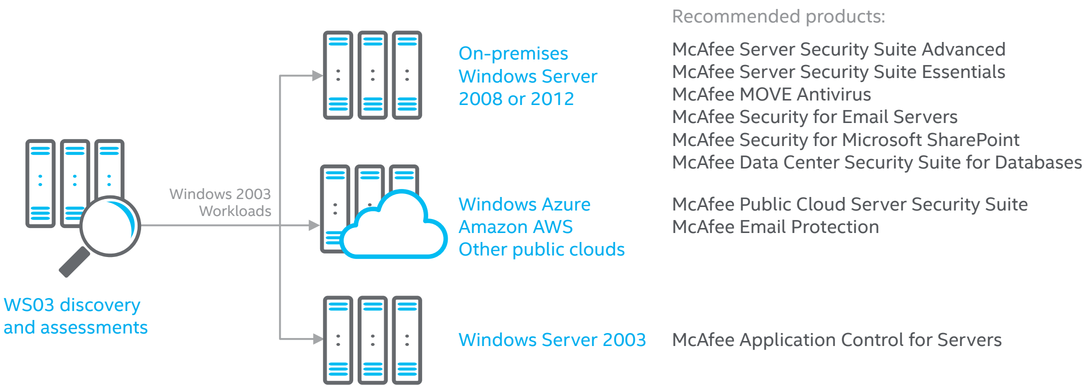
Recommended products:
On-premises
Windows Server
2008 or 2012
McAfee Server Security Suite Advanced
McAfee Server Security Suite Essentials
McAfee MOVE Antivirus
McAfee Security for Email Servers
McAfee Security for Microsoft SharePoint
McAfee Data Center Security Suite for Databases
Windows 2003
Workloads
Windows Azure
Amazon AWS
Other public clouds
McAfee Public Cloud Server Security Suite
McAfee Email Protection
WS03 discovery
and assessments
Windows Server 2003
McAfee Application Control for Servers

Figure 1. Overview of recommended security solutions for Windows Server 2003 migration.

Recommendation for Path #1: Upgrade to a newer version of Windows Server

This will typically involve buying new servers, virtualizing the servers, and deploying workloads in the private clouds to maximize compute resources efficiently. These target compute environments need to be properly secured, and for that we recommend the following Intel Security products.

For all servers:

- **McAfee® Server Security Suites** discover all virtual and physical servers, including those in the private and public clouds, and then provide comprehensive protection for all servers. Included in these suites is McAfee MOVE AntiVirus for Virtual Servers, which provides antivirus protection optimized for virtual environments. McAfee Server Security Suite Essentials provides comprehensive server security, and Advanced Server Security Suite extends that with protection from known and unknown threats while ensuring continued compliance.

For email servers:

- **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.

For SharePoint servers:

- **McAfee Security for Microsoft SharePoint** provides industry-leading protection. It keeps SharePoint deployments from spreading malware, storing inappropriate content, or facilitating data loss.

For database servers:

- **McAfee Data Center Security Suite for Databases** offers real-time protection for databases from internal, external, and intra-database threats, with no costly architectural changes, hardware, or downtime.

Recommendation for Path #2: Migrate workloads to the public cloud

Many workloads may be appropriate for moving to the public cloud, thereby reducing capital expenditures and boosting scalability. To make sure you are protecting your workloads in the public cloud, we recommend the following Intel Security products.

For all servers in the cloud (IaaS):

- **McAfee Public Cloud Server Security Suite** provides deep visibility into server instances in the public cloud and comprehensive security to help extend and manage security policies. You can deploy comprehensive protection with a mix of blacklisting and whitelisting technologies, and dynamically manage the environment with McAfee ePolicy Orchestrator® (McAfee ePO™) software. This suite provides comprehensive anti-malware, firewall, intrusion prevention, and data protection for Azure, AWS, and other cloud deployments.

For email in the cloud/Office 365 (SaaS):

- **McAfee Email Protection solutions** provide enterprise-grade security for Microsoft Office 365, so you can defend against phishing attacks, achieve greater reliability, and improve email continuity.

Recommendation for Path #3: Delay migration

For financial or other reasons, some businesses may choose to stay with Windows Server 2003 beyond the EOS date. If you do, it is essential that you add security protection to all of your servers since Microsoft will no longer issue security updates, potentially exposing you to new malware.

To address this concern, we recommend **McAfee Application Control for Servers**, our centrally managed whitelisting product. It allows only “known good” applications to run while blocking others—including advanced threats—without requiring signature updates. That helps keep costs down by eliminating the manual support requirements common with other whitelisting techniques.

McAfee Application Control for Servers is an industry-leading, proven application control for servers that can help provide additional levels of security by:

- Significantly lowering host performance impact over traditional endpoint security controls.
- Protecting against zero-day and advanced persistent threats (APTs) without signature updates.
- Providing dynamic whitelisting that requires lower operational overhead compared to legacy whitelisting techniques.

Make Your Move—Securely

If your business is still running Windows Server 2003, you must act now to keep your business secure. Choose one or more of the three migration paths above, and talk with your Intel Security sales representative for more details on how to plan a strategic—and secure—migration.

[1] McAfee Labs Q2 2014.

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