Procrastinators Guide to Windows Server 2003 End of Support
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>The Facts about Windows Server 2003 End of Support</td>
<td>3</td>
</tr>
<tr>
<td>The Status of and Barriers to Upgrading</td>
<td>4</td>
</tr>
<tr>
<td>The Impact on Compliance</td>
<td>5</td>
</tr>
<tr>
<td>The Consequences</td>
<td>5</td>
</tr>
<tr>
<td>Application Control as a Compensating Control</td>
<td>6</td>
</tr>
<tr>
<td>The Advantages of Carbon Black</td>
<td>7</td>
</tr>
<tr>
<td>Software Approvals Made Easy With Carbon Black</td>
<td>7</td>
</tr>
</tbody>
</table>
Introduction

Microsoft ended support for Windows Server 2003 on July 14, 2015, but many organizations have not yet been able to upgrade the operating system due to budgetary or other constraints. Do you have Windows Server 2003 systems but unable to upgrade to Windows Server 2012 or can’t afford to pay Microsoft for out-of-band support? If so, read this eBook to learn how you can continue to run Windows Server 2003 while keeping your systems secure and compliant.

The Facts About Windows Server 2003


For those still running WS2K3, this means:

- There are NO MORE security updates or critical patches available without paying Microsoft $600/year per server for extended support.
- No support for moderate or low priority security updates.
- AV solution software is ineffective in covering Windows Server 2003 systems and many AV providers are longer be supported.

FACTS ABOUT WINDOWS SERVER 2003

- **July 14, 2015**
- **There are NO MORE** security updates and critical patches available unless you pay Microsoft for custom support.
- **$200,000**
  - The estimated average amount for custom support.
The Status of and Barriers to Upgrading

Experts have been warning business leaders about the risks associated with Windows Server 2003 end of life for years. Despite this, many organizations have yet to migrate away from the server platform and are exposed to vulnerabilities as a result.

An estimated 1 in 3 enterprises continued to run WS2K3 after the July 14th deadline, leaving an estimated 2.7 million servers unprotected.

14 percent of enterprises do not yet have an upgrade plan for WS2K3.

Research by Carbon Black found that one in three organizations planned to run Windows Server 2003 unsupported, leaving an estimated 2.7 million servers unprotected. If you are in this boat, you are not alone and this eBook will outline steps you can take now to ensure your systems remain secure and compliant.

BARRIERS TO UPGRADING

Hardware Upgrade
Application Compatibility
Time & Budget
The Impact on Compliance

Organizations required to meet PCI, HIPAA, SOX, or NERC that continue to run Windows Server 2003 unsupported have found themselves out of compliance. With a significant uptick in malware attacks and annual audits, this should be of primary concern to industry CISOs or CIOs.

More than likely, you have servers for record management, HR, finance, payment processing or other business critical functions still running Windows Server 2003. This leaves you facing a full hardware upgrade and/or upgrading the legacy applications running on the Windows Server 2003. Unplugging them simply is not an option, leaving you in needing to find a way to ensure the confidentiality of electronic customer information and audit proof that information to meet changing regulatory requirements.

The Consequences

Unpatched 2003 systems lead to “zero-day forever scenarios” – that is, there are no patches for zero-day attacks so new vulnerabilities will never be remediated and can be exploited by attackers. And since Windows Server 2003 lacks the memory protection features found in later Windows operating systems, the lack of support can make your situation worse.

Without updates and patches, you may be cited for noncompliance and/or failure to pass assessment and regulatory audits. Further, if you have systems running Windows Server 2003, it’s likely that you have other operational and security issues as well. Therefore, a thorough review and inventory of all your IT systems to identify risks and vulnerabilities, is recommended.

Once you have an operating system that can’t be patched and new malware is discovered, your organization will be out of compliance and the effects can be devastating:

- Breach and data compromise: Malware authors can get access to highly confidential information such as your patient healthcare records.
- Financial penalties: Your organization can be fined for failure to pass compliance audits or for being in a noncompliant state (e.g., PCI: Requirement 6.1; HIPAA: 42 USC § 1320d-5)
- Damage to your patient healthcare records: This is often the most devastating consequence and can be difficult to remediate. Your organization’s public image can suffer from a breach or failure to operate in a compliant state.
Application Control as a Compensating Control

If you are late in addressing a solution to WS2K3 end-of-life, you should actively begin looking at possible compensating controls that can ensure the continued security and compliance of these critical systems.

For those unfamiliar with the concept of a compensating control, the Payment Card Industry Data Security Standard offers this definition:

“Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:

1) Meet the intent and rigor of the original stated PCI DSS requirement;

2) Provide a similar level of defense as the original PCI DSS requirement;

3) Be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and

4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.”

One of the most common and widely accepted compensating controls for end-of-life systems is the enforcement of an application whitelist. Application whitelisting is a computer administration process used to prevent unauthorized programs from running. The purpose is to protect computers and networks from running harmful applications and ensure unauthorized change. This is done by establishing a positive security model, usually through the use of software, by which execution of software is controlled and enforced to only allow software explicitly allowed (either specifically or policy) on a machine or set of machines. This is the opposite approach taken by antivirus or HIPS solutions which rely on negative security models focused on identifying “known bad” applications or activity rather than “known good”.

Because of its focus on “known good” applications and controlling change, application control is a common solution for addressing malware or software vulnerabilities to meet compliance requirements. In the case of Windows Server 2003, it may be ideally suited because “known good” state can be typically identified and easily implemented in a controlled environment, such as servers.
The Advantages of the Carbon Black Enterprise Protection

While highly effective, application control can be difficult to establish and manage. Many traditional application control solutions (i.e.: Applocker) require administrators to create and manage a static list of approved applications; even for small organizations this can be extremely challenging. Rather than forcing administrators to manage static whitelists, Cb Enterprise Protection uses a trust-based and policy driven dynamic approach to automate and dramatically simplify the management of a “default-deny” policy environment and is why Cb Enterprise Protection is the world’s most widely deployed application control solution.

Software Approvals Made Easy With Cb Enterprise Protection

Combining a trust-based and policy-driven approach to application control with real-time threat intelligence, Cb Enterprise Protection continuously monitors and records all endpoint and server activity to prevent, detect and respond to cyber threats that evade traditional security defenses. With open APIs and a broad partner ecosystem, Cb Enterprise Protection provides unmatched flexibility to seamlessly integrate with both in-house and third-party tools.
Instant Visibility: Once installed, the Cb Enterprise Protection agent provides administrators with real-time visibility into all executable-type files running across their environment. Working with Carbon Black Threat Intel, the Cb Enterprise Protection agent provides administrators with trust ratings and actionable intelligence to easily identify and automatically take action against those files most likely to be malicious.

Unmatched Prevention: Instead of requiring a “one size fits all” threat prevention strategy that leaves systems under-protected and users frustrated, Cb Enterprise Protection allows security teams to dial-up and dial-down protection strategies to match line of business, user, and system policies that balance organizational culture and risk posture. Only Cb Enterprise Protection delivers the world’s most effective and widely adopted application whitelisting capabilities alongside several other prevention strategies that drive policies and rules based on threat detection and detonation processes.

Advanced Detection: Cb Enterprise Protection includes powerful automated and cloud delivered advanced threat detection technologies to quickly identify and stop attacks. Leveraging Advanced Threat Indicators from Cb Threat Intel, Cb Enterprise Protection continuously monitors and examines endpoints to identify potential patterns of compromise and detect malicious activity across every endpoint device in the organizations environment.

By leveraging real-time endpoint data, Cb Enterprise Protection’s advanced threat indicators go beyond “indicators of compromise” by combining endpoint activity, cloud delivered threat intelligence, and heuristics to identify threats based on patterns rather than single event-based indicators of compromise. This combination of detection mechanisms enables Cb Enterprise Protection to reduce the number of false positive alerts and detect threats both at initiation and while they are in progress, unlike poll-based detection methods which can only detect compromise after it has occurred.

Rapid Response: Once an attack is detected, Cb Enterprise Protection provides a variety of tools to help you rapidly respond, log and investigate security incidents. Cb Enterprise Protection’s unique “Detect-and-Deny” protection capabilities enable administrators to quickly respond to malicious activities by terminating active processes and immediately banning any future execution of the attack in your environment. Additionally, Cb Enterprise Protection’s full historical record of endpoint activity quickly provides administrators with a full impact assessment of where malware has executed, where it started, how it spread, and ultimately what systems were impacted and what actions/data, if any, was taken.

Open API Architecture: As the first next-generation endpoint protection solution to integrate with network security solutions and the only solution to integrate with Microsoft System Center Endpoint Protection, Cb Enterprise Protection’s open architecture helps organizations quickly deliver more value by integrating with the entire security stack to automate and simplify the security process. Through Cb Enterprise Protection’s restful API and unrivaled partner integration ecosystem, Cb Enterprise Protection provides organizations with unmatched openness and extensibility to integrate their security solutions for improved automation, reporting and faster security response times, via third-party security products (SIEM, Network, Endpoint, Operations) or custom in-house tools.

About Carbon Black
Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker’s every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs. Carbon Black has been named #1 in endpoint protection, incident response, and market share. Forward-thinking companies choose Carbon Black to arm their endpoints, enabling security teams to: Disrupt. Defend. Unite.