End of support doesn’t have to mean end of security

How Trend Micro can secure your end of life servers, and enable a safe transition to new platforms and the cloud
INTRODUCTION

The End of Support (EOS) of major enterprise platforms like Windows XP and Windows Server, and Windows Server 2003 are a major challenge for organizations running mission-critical applications necessary for day-to-day business. For example, in July 2015, when Microsoft ended support for Windows 2003, it put millions of enterprise servers at risk. According to a study about EOS by leading analyst firm Enterprise Strategy Group (ESG), “More than 80 percent of enterprise and midmarket organizations still support Windows Server 2003 to some extent”. If your organization was using Microsoft Server 2003 at that time, the EOS likely introduced serious security risks, unless you were fully prepared to migrate to a new platform or put compensating controls in place. Hackers know that platform providers like Microsoft will no longer acknowledge or patch vulnerabilities, so these systems quickly become a favorite target for attacks, and the risks of running an unsupported platform after EOS will increase over time as more issues are found and not patched.

This white paper reviews the risks facing organizations running end of life (EOL) platforms like Windows Server 2003 and the options available to them to address those risks. It specifically focuses on how Trend Micro™ Deep Security™ can provide protection for EOL platforms. Delivered by the market leader in server security and powered by XGen™ security, Deep Security includes a cross-generational blend of security controls that can be used to protect platforms like Windows 2003 that are at or past EOL, enabling organizations to plan and execute a transition that makes sense to the business. It also lets organizations avoid expensive custom support agreements for security patches from Microsoft and helps to extend the life of legacy systems and applications. Deep Security can also help to provide a smooth migration path to securing systems beyond Windows 2003, including Windows 2012, 2016, Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform, and other leading cloud providers.

1 Enterprise Strategy Group, Microsoft Windows Server 2003: The End is Nigh, Feb. 2015
UNDERSTANDING THE RISKS OF END OF LIFE SYSTEMS

Even with an organized EOS process from Microsoft, many organizations still ran Windows Server 2003 when they announced EOS. For EOS on any platform used extensively in an enterprise, migration can be a challenge. Most organizations cite a lack of time, resources, and/or have critical business applications that simply can’t be migrated in the foreseeable future. This can result in these organizations being at increased risk and a strategy to address security for vulnerable systems might be required.

Ignoring the challenges associated with the continued use of EOL systems introduces many risks, not the least of which is that newer, supported platforms also often share code with previous platforms. A new exploit like EternalRocks (using the Microsoft SMB 1.0 vulnerability) on a supported platform, like Windows 2012 or 2016, can also affect an older out-of-support system that shares its code. And with no updates typically delivered to the EOL systems, it is also a clear attack vector for malicious hackers.

Running EOL systems that are unprotected introduces risks beyond that single platform. A compromised server can make the entire network vulnerable to malicious attacks, data loss, and malware like ransomware. In addition, addressing compliance with regulations like PCI DSS, HIPAA, and GDPR or compliance frameworks like the SANS/CIS Top 20 Critical Security Controls, NIST 800-53, and others, will not be possible without some plan of action.

STAYING SECURE BEFORE, DURING, AND AFTER MIGRATION

While enterprises should plan for the sunsetting of any EOS platform, like Windows Server 2003 and XP systems, the reality is that plans are frequently impacted by budgetary constraints or technical limitations. Organizations need to be able to migrate away from out-of-support systems on their schedule while cost-effectively maintaining the security of these EOL systems. Regardless of your migration plan – to Windows Server 2012 or 2016, Microsoft Azure, or other leading cloud environments like AWS – security solutions need to be able to address not only the EOS system, but newer environments, including containers and hybrid cloud deployments. When looking at options, this should be a critical consideration from both an operational and security perspective.

Sunsetting may take time, so plans should include the entire time horizon for complete migration. Nine months after official EOS, an industry survey highlighted that there were still many servers out there, and it would still take some time to complete the transition. The latest information that we have observed shows there are still many organizations running Windows Server 2003 and Windows XP, over two years later.

Source: Osterman Research, April 2016
CONTINUED USE OF AN END OF LIFE PLATFORM: WHAT TO DO?

There are several options available to organizations once the EOS date has passed for platforms like Windows Server 2003 and Windows XP. Like most options, there are positive and negative aspects that must be considered as part of the planning process. Although organizations need to weigh the risks and costs associated with each option, there are some clear winners that should come at the top of the list.

1. STATUS QUO: LEAVE THE DEPLOYMENTS “AS IS”

There is always the option to “do nothing” with all risk analysis, which would translate into no increased costs associated with migration or additional security controls. However, the risks introduced by an unpatched system to an organization would be untenable. An EOS system like Windows Server 2003 or Windows XP is a natural target for attackers, and once compromised, could be the path for attackers to do considerable damage to an organization. For completeness, this option has been included; however, with the ready availability of approaches that are both secure and cost-effective, this is not recommended.

2. CUSTOM SUPPORT AGREEMENTS FROM THE PLATFORM PROVIDER

Microsoft may offer custom and extended support agreements for Windows Server 2003, entitling customers to emergency security patches. However, such agreements are typically cost-prohibitive, often more than $200,000 per year\(^3\), driving customers to find alternative methods to mitigate the risk or, in some cases, accept the risk of a potential compromise. In addition, there may be qualifiers to the extended support contract. For example, for an organization to qualify for a Custom Support Agreement, Microsoft requires that they have a clear migration plan in place, which may not be possible for many organizations in the foreseeable future.

3. ISOLATION

One approach to managing risks associated with out-of-support software like Windows Server 2003 is to make them hard for hackers to reach. Isolating these systems on separate networks or VLANs, or segmenting them using network or host-based firewalls, adds a layer of difficulty that hackers may decide is simply too much trouble. However, network isolation may not be practical for essential business systems. Making out-of-support systems hard to reach adds a layer of security but may also prevent them from being used effectively, removing the reason for retaining them in the first place. While this may work for a small percentage of deployed servers, this will not likely be a practical solution for most.

4. SYSTEM HARDENING

Hardening a system like Windows 2003 Server or Windows XP (e.g., removing unnecessary services, disabling vulnerable service versions like SMB 1.0, user accounts) is a good way to minimize risk. However, authorized users will still need access to these systems, so restricting user accounts alone may not be practical for business reasons.

For Windows Server 2003, organizations should leverage the built-in software restriction policies that can be deployed through global policy in order to minimize risks of applications executing erroneous commands. While not trivial, this is a good approach to help protect servers from compromise via an application, so long as it is done in conjunction with additional protection measures.

It should be noted that hardening through removal of unnecessary services and ports is not a simple process, especially when business applications are designed to run on general-purpose operating systems with a variety of application services and ports (e.g. RPC ports, web services). It is a very real possibility that hardening may break the application. Restricting application ports may also render stateful packet-filtering firewalls ineffective, since many applications dynamically allocate ports as needed.

\(^3\) Trend Micro Customer Interviews, 2017
5. DEPLOY ADDITIONAL SECURITY CONTROLS

In order to address potential vulnerabilities on an EOS system like Windows Server 2003, additional security controls can be put in place to detect attacks and protect from them. Host-based solutions are ideal for this, as perimeter solutions simply cannot provide an effective set of protection mechanisms for each individual server, especially in the context of the modern data center and cloud. Key host-based controls that should be considered include:

- Intrusion detection and prevention (IDS/IPS) to protect against network attack vectors, like EternalRocks, that was used in the recent WannaCry and Erebus ransomware attacks
- Monitoring the integrity of system files, registry settings, and other critical application files to ensure that unplanned or suspicious changes are flagged
- Malware prevention, including anti-malware and behavioral analysis to protect against new forms of malware, especially ransomware

Given the need for multiple controls, the recommended approach is to deploy a solution that can address them all in a single product that can be centrally managed. It is also important to ensure that the same product can apply to new deployments as well, regardless of the server environment (Windows or Linux) and deployment approach (physical, virtual, cloud, and/or containers).

THE BEST APPROACH: A PROVEN SECURITY SOLUTION

While implementing some aspects of server hardening will help, including Windows built-in software restriction policies, it is clear that without a platform provider acknowledging vulnerabilities and providing patches, organizations must deploy additional security controls. For example, with no planned patches coming for Microsoft for Windows Server 2003, it is absolutely critical that vulnerabilities are still addressed. Trend Micro™ Deep Security™ can provide this protection. Deep Security delivers a cross-generational set of security controls that have been used by thousands of global organizations to protect millions of physical, virtual and cloud servers, including servers still using EOL platforms like Windows XP and Windows Server 2003. It can provide the critical capabilities needed to ensure a secure transition for organizations, enabling the business to dictate how and when the migration occurs, without introducing unnecessary risk or undue cost.

TREND MICRO DEEP SECURITY

Deep Security delivers a cross-generational blend of security techniques that can be used to protect server and application workloads across physical, virtual, cloud, and container environments. Managed through a central security console, it can be deployed as a single workload agent, and also at the hypervisor level with VMware NSX for increased efficiency for resource-intensive controls, like anti-malware. To ease operational impacts, policy can enable the automatic application of security, including scanning systems for changes that may require additional protection measures and applying them automatically.

Deep Security includes proven network security controls that can shield critical systems from vulnerabilities –like the Microsoft SMB vulnerability that enabled WannaCry ransomware to be delivered—until a patch is available and deployed—or as protection before and during migration for out-of-support systems.

To protect against changes in a system that no longer has patches available, Deep Security also delivers robust system security capabilities. Integrity monitoring enables the detection of out-of-policy changes, including alerts when updates happen, where there should no longer be any. To help ensure that servers are fully protected, Deep Security also includes malware prevention capabilities like anti-malware and behavioral analysis to detect and remediate attacks from malicious software like ransomware.
WHAT DEEP SECURITY DOES AND WHY IT MATTERS

Deep Security is a host-based security product that delivers multiple security controls through a single agent. As recommended, it includes key capabilities to protect systems that have reached their EOL—like Windows Server 2003 and Windows XP—and, as organizations migrate, includes important features that reduce risk and operational costs across physical, virtual, cloud, and hybrid deployments. Based on deep integration with VMware, Deep Security can also protect virtual desktop infrastructures (VDI), including those where EOL systems like Windows XP may be deployed.

While this white paper focuses on the key security controls that will help to protect vulnerable EOS systems like Windows Server 2003, Deep Security also provides additional security capabilities through the single workload agent. Application control, log inspection and scanning for applications like SAP can also be leveraged to secure servers and applications using supported systems across the hybrid cloud.

NETWORK SECURITY: SHIELDING SERVERS AND APPLICATIONS FROM ATTACK

Deep Security’s network security controls can shield enterprise servers against known and unknown vulnerabilities—for example the recent WannaCry ransomware attack that leveraged EternalRocks to use an SMB vulnerability in Windows, and older, still available ones like Shellshock and Heartbleed— from being exploited.

Leveraging intrusion detection and prevention capabilities (IDS/IPS), Deep Security includes thousands of proven rules that apply to network traffic in layers 2-7. These rules can be automatically applied based on a deployment environment (e.g., Windows Server 2003) to protect unpatched, network-facing system resources and enterprise applications. As one layer of protection against new attacks like ransomware, Deep Security’s network protection can shield servers from vulnerabilities that could be used to infect and spread across the data center with devastating results.

* Older vulnerabilities continue to be an issue today on EOS and other systems
Protection applies to both the underlying operating system, as well as common enterprise applications deployed on those servers. Deep Security includes out-of-the-box vulnerability protection for hundreds of applications, including database, web, email, and FTP servers. In addition, it provides zero-day protection for known vulnerabilities that have not been issued a patch, and unknown vulnerabilities using smart rules that apply behavioral analysis and self-learning to block new threats.

Deep Security web application protection rules defend against the most common web attacks, including SQL injection, cross-site scripting, and other web application vulnerabilities—shielding these vulnerabilities until code fixes are completed. Security rules enforce protocol conformance and use heuristic analysis to identify malicious activity. To help with critical issues like lateral movement across the data center, Deep Security also includes robust rules that can be used to detect potential malicious activity and block it. Leveraging the IDS/IPS engine, Deep Security can detect attacker activities, including the use of remote administration tools to control and perpetuate movement across the data center, and then block them.

To help with enforcement of IPS rules, Deep Security leverages its built-in, bi-directional and stateful firewall. The enterprise-grade firewall can also help to control communication over ports and protocols necessary for correct server operation, and blocks all other ports and protocols. This can further reduce the risk of unauthorized access to a deployment that includes EOS servers, like Windows Server 2003. The host firewall can also help with key compliance requirements from regulations, like PCI DSS, HIPAA, and GDPR, particularly in cloud deployments where there is no access to the firewall logs for network events.
SYSTEM SECURITY: INTEGRITY MONITORING

Deep Security’s system security controls include integrity monitoring, which can alert organizations in real time to any unexpected changes to an operating system and application files, including key attack points like host files, directories, and registry key values. For virtualized deployments on VMware, the solution uses Intel TPM/TXT technology to perform VMware hypervisor integrity monitoring for any unauthorized changes, extending security and compliance to yet another layer. Deep Security can also simplify administration by greatly reducing the number of known good events through automatic cloud-based whitelisting from the Trend Micro Certified Safe Software Service.

Central dashboard gives instant notification of malicious changes to sensitive files and applications

For systems that are past EOS, there are many areas in both the operating system as well as applications that should no longer be changed. Integrity monitoring allows organizations to quickly understand what has changed and how, and lets them take action immediately if there is an issue. With trusted event tagging that automatically replicates actions for similar events across the entire data center, the administrative overhead is minimized.

Deep Security’s integrity monitoring capability can also help with incident detection and potential indicators of compromise (IOC). It includes specialized rules that were developed by Trend Micro’s Threat Research and Incident Response teams. With almost no false-positives, Deep Security can detect and report on hundreds of potential Indicators of Compromise (IOCs). Examples of attacks that can be detected include Flamer, Gauss, Duquu, Confiker, and more. This type of alerting can help the incident response teams to detect attacks faster and more easily tie them to a specific attack or threat.

MALWARE PREVENTION

Deep Security’s malware prevention capabilities like anti-malware and behavioral analysis provides protection from malicious software including ransomware, viruses, spyware, worms, and Trojans across physical, virtual, cloud, and container workloads. Integration with the Trend Micro™ Smart Protection Network™ global threat intelligence for Web Reputation capabilities also strengthens protection for servers and virtual desktops.

RECOMMENDATION SCANNING

Deep Security can be configured by policy to automatically scan systems and deploy appropriate rules; it can also simply notify administrators of the recommended rules and allow them to be applied when ready. Recommendation scanning streamlines security update management by automatically recommending which rules need to be deployed to protect a given system. Deep Security scans the system to identify which of the thousands of IDS/IPS rules need to be deployed to optimize protection based on the OS version, service pack, patch level, and installed applications. Policy can be used to schedule regular scans on systems (e.g., weekly) for potential new vulnerabilities and automatically apply appropriate shielding. Once a rule is activated, particularly for newly discovered vulnerabilities like SMB 1.0 on Windows or Struts 2, and even older vulnerabilities like Shellshock and Heartbleed, it is seamlessly deployed where needed, automatically protecting applicable systems and removing the need for emergency patching. In the case of EOL systems, like Windows Server 2003, with no patches forthcoming, this is a critical protection mechanism.
SECURITY UPDATES

Security updates are delivered by a dedicated team of security experts that monitor threats 24x7, ensuring that the latest in protection is available to Deep Security customers. This team continuously monitors multiple sources of vulnerability disclosure information, including more than 100 sources such as SANS, CERT, Bugtraq, VulnWatch, Packet Storm, and SecuriTeam. It also draws information from the more than 150 million endpoints protected in the Trend Micro Smart Protection Network. This information is used to identify and correlate new relevant threats and vulnerabilities, and then create relevant rules to protect at-risk systems. For example, Trend Micro delivered protection for both Heartbleed and Shellshock within 24 hours of public disclosure, enabling the instant protection of servers using Deep Security. As well, protection from the SMB 1.0 vulnerability announced in March 2017 was released in under 24 hours, which provided protection from WannaCry months in advance of the actual attack. Illustrative of Trend Micro’s commitment to security, Deep Security also started to protect unpatched vulnerabilities for Windows Server 2003 even before EOS, whereas Microsoft did not patch a known vulnerability based on the date proximity to EOS (three weeks before EOS).

For vulnerability shielding specifically, the research team focuses on the risks to server and desktop software that are likely to exist within a customer environment. This includes operating systems such as Microsoft Windows, Linux, and Unix, as well as enterprise software such as web browsers, web servers, application servers, backup software and databases.

HOW DEEP SECURITY WORKS

Deep Security provides critical security capabilities for securing enterprise servers, including network, system, and malware prevention controls. Deployed at the host, it provides server, application, and data security across physical, virtual, cloud, and container deployments, and protects businesses from breaches and business disruptions without the need for emergency patching.

Unlike legacy perimeter security approaches, taking a host-based approach enables Deep Security to protect servers from the traditional “North-South” traffic in a data center, as well as the “East-West” traffic that is increasing with the use of virtualization and cloud technologies. Having security at the host enables organizations to protect each specific server environment, which for out-of-support operating systems, like Windows Server 2003, will be critical with no new patches coming. It also helps to protect systems from attack from another compromised server inside the network via lateral movement, which would not be addressed by perimeter security. For elastic cloud deployments, the ability to instantly scale horizontally is best served by automatically securing each virtual server instance as it comes online, not by forcing all traffic through a single chokepoint that will be limited in its ability to react and scale. This is especially true for multi-cloud deployments across leading cloud service providers (CSPs) like AWS and Microsoft Azure.

The solution consists of the Deep Security Manager and a Deep Security Agent. For VMware deployments, there is also the Deep Security Virtual Appliance, which integrates seamlessly with VMware ESX and NSX and helps to automate the deployment of security across a software-defined data center.
DEEP SECURITY MANAGER
The Deep Security Manager enables administrators to create security profiles and apply them to servers—across physical, virtual, cloud, and hybrid deployments. It has a centralized console for monitoring alerts and preventive actions taken in response to threats, and can be configured to automate or distribute security updates to servers on demand. The Manager can be used to generate reports to gain visibility into activity to meet compliance requirements. Event tagging functionality streamlines the management of high-volume events and enables workflow of incident response.

For VMware environments, there is a hypervisor-level component, the Deep Security Appliance, which enables the deployment of resource intensive security controls like anti-malware for servers deployed on an ESX host. In addition, where organizations have chosen to deploy VMware NSX, Deep Security can be used in conjunction with the micro-segmentation capabilities enabled through software-defined networking to achieve a secure virtualized data center.

DEEP SECURITY AGENT
The Deep Security Agent is a small intelligent software component that is deployed on the server or virtual machine being protected and enforces the security policy. This is a single security agent that integrates all of the Deep Security modules being used, streamlining deployment and management. For vulnerability shielding, the Deep Security Agent integrates with the system’s network driver (stack) to evaluate network packets against Deep Security rules. Should the rules engine identify an exploit, the network connection is dropped to terminate and prevent the attack. The agent can be automatically deployed via scripting with PowerShell or orchestration tools like Chef, Puppet, Ansible, and SaltStack, and only deploys security components dictated by policy, streamlining the size of the agent and maximizing workload performance.
WHY TREND MICRO

As discussed in this white paper, Deep Security delivers a broad set of integrated security controls that can be used to protect EOS systems like Windows Server 2003. Available as software, as-a-Service, and through the AWS and Azure marketplaces, it can be leveraged across all environments—physical, virtual, cloud, and containers—to enable streamlined management and consistent security as organizations migrate. Deep Security’s host-based approach to security fits the needs of the modern data center and cloud, protecting workloads based on their specific configurations and wherever they are deployed, including a multi-cloud deployment.

Organizations around the world trust Trend Micro to protect their data center and cloud deployments with our unique vulnerability shielding capabilities, helping to protect their sensitive enterprise systems running current and EOS platforms, including Windows XP and Windows Server 2003 deployments. In fact, Trend Micro has committed support for protecting Windows Server 2003 and Windows XP deployments until the end of 2020 to allow for a smooth migration while still keeping systems secure.

Deep Security is the only solution that integrates this breadth of server security into a single product, enabling the coordination of multiple security controls for a highly-effective server security solution for EOS systems like Windows Server 2003, as well as other deployments across the hybrid cloud. This integrated approach to security can also help to accelerate compliance with key regulations like PCI DSS, HIPAA, and Europe’s GDPR.

In addition, leading analyst firms clearly view Trend Micro as a market leader in server security. In their most recent Gartner Endpoint Protection Platform Magic Quadrant, Gartner placed Trend Micro furthest to the right in the leaders quadrant for our security vision. And, for the past seven years, IDC has named Trend Micro the global market share leader in server security, demonstrating that more organizations trust Trend Micro to secure their sensitive IT infrastructures.

CONCLUSION: YOUR SYSTEM MAY BE END OF SUPPORT BUT THERE IS A SECURE WAY FORWARD

If you are running an unsupported system like Windows Server 2003 or Windows XP today, you are likely concerned about how you can consistently and cost-effectively protect your enterprise applications and data on those systems. This is especially critical with the recent escalation of ransomware and attacks like WannaCry, Erebus, and more. With many organizations continuing to run some amount of Windows Server 2003 systems after EOS, it’s clear that you are not alone. Given the complexity of migrating an enterprise server platform, organizations should consider a multi-pronged approach to protecting systems that have gone beyond support, including for Windows Server 2003 the use of Microsoft’s built-in software restriction policies, along with the deployment of additional security controls.

Deep Security’s virtual patching protects us from legacy vulnerabilities—those that are not patchable or that the vendor will never fix. Deep Security discovers the holes and protects us until we can replace those older systems.

Jeremy Mello
Network Systems Specialist
City of Fresno

---

If you are running a system that is out of support, Deep Security is the ideal solution to protect all of your servers before, during, and after migration. It delivers the key security controls needed to protect sensitive enterprise deployments, including network security with IPS for vulnerability shielding, system security through integrity monitoring of sensitive server resources, and malware prevention through anti-malware and behavioral analysis to protect against the latest in malicious attacks like ransomware. Deep Security includes a cross-generational blend of security techniques along with central management, enabling IT operations to better manage systems and accelerate compliance, protecting vulnerable systems until a patch can be applied. With out-of-support systems like Windows Server 2003, Deep Security can protect against the latest in vulnerabilities where there are no patches being delivered, helping to prevent data breaches. It helps to ensure business continuity, while enabling compliance with important standards and regulations such as PCI DSS, HIPAA, and GDPR, as well as security frameworks like NIST 800-53 and the SANS/CIS Top 20 Critical Security Controls.

Trusted by thousands of customers to secure millions of servers around the world, Deep Security has made Trend Micro the market leader in server security across the hybrid cloud. If your organization is running an EOS system like Windows Server 2003, Deep Security can help you quickly and cost-effectively ensure that your organization is secure – today and tomorrow.

**FIND OUT MORE ABOUT HOW TREND MICRO CAN PROTECT YOUR END OF SUPPORT SYSTEMS**

visit [http://www.trendmicro.com/SecureEOS](http://www.trendmicro.com/SecureEOS)