A Trend Micro White Paper | July 2019

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 Microsoft® Windows® Server 2008 and 2008 R2 are a significant 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. 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. Now, EOS for Windows Server 2008 and 2008 R2 is coming in January 2020, and hackers know that platform providers like Microsoft will no longer acknowledge or patch vulnerabilities. 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 2008 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[2] and powered by XGen™ security, Deep Security includes a cross-generational blend of powerful, automated security controls that can be used to protect platforms like Windows 2008 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 until and beyond their migration to newer platforms or public cloud providers such as Microsoft® Azure™, Amazon Web Services® (AWS), and Google Cloud™—protecting the entire hybrid cloud with a single, streamlined solution.

[1] Enterprise Strategy Group, Microsoft Windows Server 2003: The End is Nigh, Feb. 2015

[2] IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, November 2016

UNDERSTANDING THE RISKS OF END OF LIFE SYSTEMS

Even with an organized EOS process from Microsoft, many organizations still ran Windows Server 2003 past the EOS, and the same will apply for the Windows Server 2008 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 newer 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.

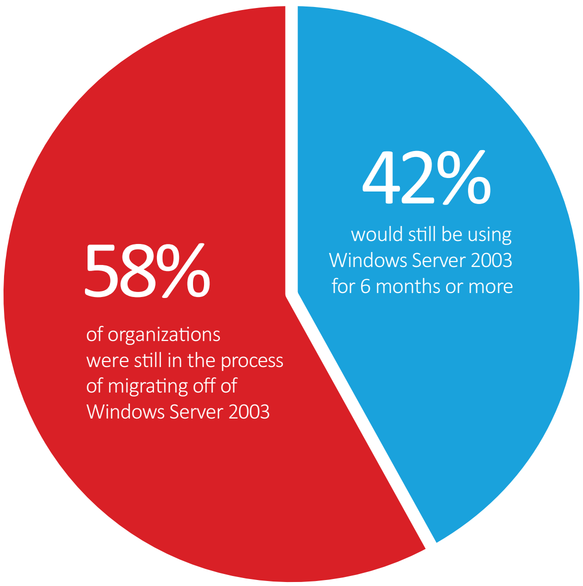
Running EOL systems that are unprotected introduces risks beyond that single platform. A compromised server can make the entire network vulnerable to malicious attacks, data loss, and malware like ransomware, crypto mining attacks, and more. In addition, addressing compliance with regulations like PCI 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, 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 2016 or 2019, 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 of Windows 2003, an industry survey highlighted that there were still many servers out there, and it would still take some time to complete the transition to a new platform or cloud.

Nine months after the end of support



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 2008 and Server 2003. 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 2008 and Windows 2003 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 2008, 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 security updates, such as requiring a Software Assurance (SA) or subscription license.

3. ISOLATION

One approach to managing risks associated with out-of-support software like Windows Server 2008 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 Server 2008 or 2008 R2 (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 2008, 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.

5. DEPLOY ADDITIONAL SECURITY CONTROLS

In order to address potential vulnerabilities on an EOS system like Windows Server 2008, 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 hybrid cloud. Key host-based controls that should be considered include:

- Intrusion detection and prevention (IDS/IPS) to protect against network attack vectors, like the Apache Struts 2 vulnerability, which led to the catastrophic Equifax security breach
- 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 and crypto mining attacks

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. New critical vulnerabilities continue to be found, and must be addressed even after the platform provider stops delivering patches.

Trend Micro™ Deep Security™ can provide this protection. Deep Security delivers powerful, automated 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 Server 2008. 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 seamlessly 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 lightweight agent, and also at the hypervisor level with VMware NSX for increased efficiency. Built for automation, Deep Security helps reduce manual processes and operational overhead with automated deployment, policy management, and a rich set of RESTful APIs.

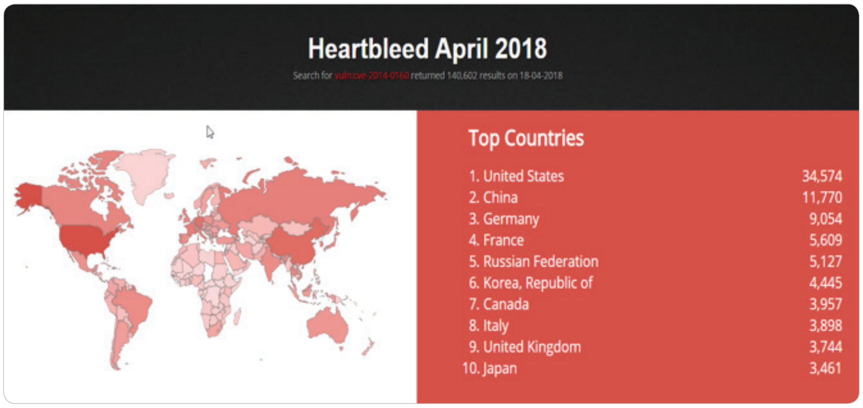
Deep Security includes proven network security controls that can shield critical systems from vulnerabilities – like the Apache Struts 2 vulnerability or the Microsoft SMB vulnerability that enabled delivery of the WannaCry ransomware—until a patch is available and deployed—or as protection before and during migration for out-of-support systems.

WHAT DEEP SECURITY DOES AND WHY IT MATTERS

Deep Security is a host-based security solution that delivers powerful, automated security controls through a single agent. As recommended, it includes key capabilities to protect systems that have reached their EOL—like Windows Server 2008 and 2008 R2 and Windows XP—and, as organizations migrate, includes important features that reduce risk and operational costs across physical, virtual, cloud, and container 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.

NETWORK SECURITY: SHIELDING SERVERS AND APPLICATIONS FROM ATTACK

Deep Security's network security controls can shield enterprise servers against known and unknown vulnerabilities— these include new critical vulnerabilities like Bluekeep as well as older vulnerabilities like the Apache Struts 2 vulnerability, Shellshock, and Heartbleed, which still present a threat to many systems to this day.



Heartbleed April 2018

Search for vuln:cve-2014-0160 returned 140,602 results on 18-04-2018

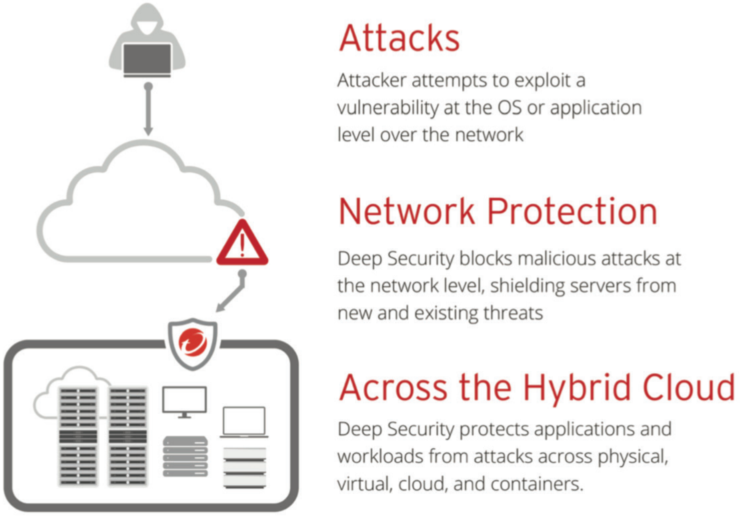
Top Countries

1. United States	34,574
2. China	11,770
3. Germany	9,054
4. France	5,609
5. Russian Federation	5,127
6. Korea, Republic of	4,445
7. Canada	3,957
8. Italy	3,898
9. United Kingdom	3,744
10. Japan	3,461

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 to protect unpatched, network-facing system resources and enterprise applications. As one layer of protection against new attacks, Deep Security's network protection can shield servers from vulnerabilities that could be used to infect and spread across the data center or hybrid cloud with devastating results.

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. For organizations running containers, Deep Security's IPS engine will scan all container traffic, including inter-container "east-west" traffic, to proactively detect and block any attacks and lateral movement attempts.



Attacks

Attacker attempts to exploit a vulnerability at the OS or application level over the network

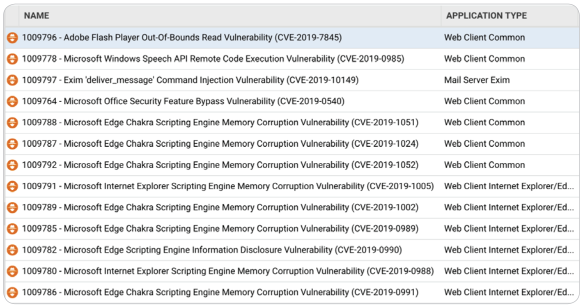
Network Protection

Deep Security blocks malicious attacks at the network level, shielding servers from new and existing threats

Across the Hybrid Cloud

Deep Security protects applications and workloads from attacks across physical, virtual, cloud, and containers.

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 2008 or 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.



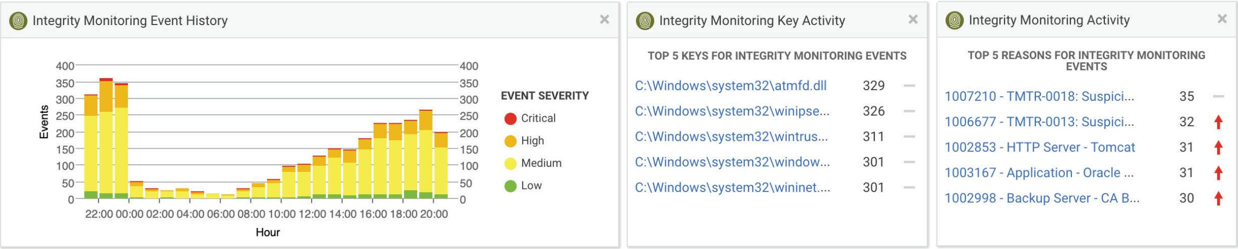
NAME	APPLICATION TYPE
1009796 - Adobe Flash Player Out-Of-Bounds Read Vulnerability (CVE-2019-7845)	Web Client Common
1009778 - Microsoft Windows Speech API Remote Code Execution Vulnerability (CVE-2019-0985)	Web Client Common
1009797 - Exim 'deliver_message' Command Injection Vulnerability (CVE-2019-10149)	Mail Server Exim
1009764 - Microsoft Office Security Feature Bypass Vulnerability (CVE-2019-0540)	Web Client Common
1009788 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1051)	Web Client Common
1009787 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1024)	Web Client Common
1009792 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1052)	Web Client Common
1009791 - Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2019-1005)	Web Client Internet Explorer/Ed...
1009789 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-1002)	Web Client Internet Explorer/Ed...
1009785 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-0989)	Web Client Internet Explorer/Ed...
1009782 - Microsoft Edge Scripting Engine Information Disclosure Vulnerability (CVE-2019-0990)	Web Client Internet Explorer/Ed...
1009780 - Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2019-0988)	Web Client Internet Explorer/Ed...
1009786 - Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-0991)	Web Client Internet Explorer/Ed...

Detect and stop lateral movement

SYSTEM SECURITY: INTEGRITY MONITORING

Deep Security’s system security controls include integrity monitoring, which analyzes vast amounts of telemetry data and can alert organizations in real time to any unexpected changes to an operating system and application files, including key attack points like files, directories, registry keys, processes, user activity, and more. These rules also include container-specific protection, to detect attacks on deployed containers as well as attacks against the container platform (e.g. Docker) and orchestration tools (e.g. Kubernetes).

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 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, Duqu, 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.



TOP 5 KEYS FOR INTEGRITY MONITORING EVENTS

C:\Windows\system32\atmfd.dll	329	—
C:\Windows\system32\winipse...	326	—
C:\Windows\system32\wintrus...	311	—
C:\Windows\system32\window...	301	—
C:\Windows\system32\wininet....	301	—

TOP 5 REASONS FOR INTEGRITY MONITORING EVENTS

1007210 - TMTR-0018: Suspici...	35	—
1006677 - TMTR-0013: Suspici...	32	↑
1002853 - HTTP Server - Tomcat	31	↑
1003167 - Application - Oracle ...	31	↑
1002998 - Backup Server - CA B...	30	↑

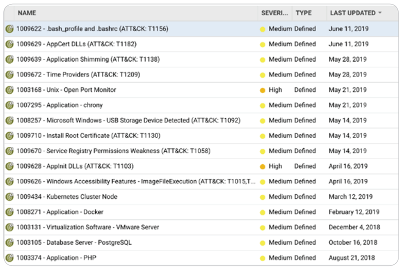
Central dashboard gives instant notification of malicious changes to sensitive files and applications

MALWARE PREVENTION

Deep Security’s malware prevention capabilities like anti-malware, behavioral analysis, and web reputation provides protection from malicious software including ransomware, crypto-mining attacks, viruses, spyware, worms, and Trojans across physical, virtual, cloud, and container workloads. Integration with the Trend Micro™ Smart Protection Network™ global threat sensors ensures the most up-to-date threat intelligence, powered by Trend Micro’s world-class threat and vulnerability research.

AUTOMATED VULNERABILITY SHIELDING

Deep Security can be configured by policy to automatically scan systems and deploy appropriate rules. 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. Like with Deep Security’s system security rules, the intrusion prevention rules will also proactively analyze and block container-specific traffic to deliver full-stack container security. 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 BlueKeep, Oracle WebLogic 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 2008 and Server 2003, with no patches forthcoming, this is a critical protection mechanism.



NAME	SEVERI...	TYPE	LAST UPDATED
1009622 - .bash_profile and .bashrc (ATT&CK: T1156)	Medium	Defined	June 11, 2019
1009629 - AppCert DLLs (ATT&CK: T1182)	Medium	Defined	June 11, 2019
1009639 - Application Shimming (ATT&CK: T1138)	Medium	Defined	May 28, 2019
1009672 - Time Providers (ATT&CK: T1209)	Medium	Defined	May 28, 2019
1003168 - Unix - Open Port Monitor	High	Defined	May 21, 2019
1007295 - Application - chrony	Medium	Defined	May 21, 2019
1008257 - Microsoft Windows - USB Storage Device Detected (ATT&CK: T1092)	Medium	Defined	May 14, 2019
1009710 - Install Root Certificate (ATT&CK: T1130)	Medium	Defined	May 14, 2019
1009670 - Service Registry Permissions Weakness (ATT&CK: T1058)	Medium	Defined	May 14, 2019
1009628 - AppInit DLLs (ATT&CK: T1103)	High	Defined	April 16, 2019
1009626 - Windows Accessibility Features - ImageFileExecution (ATT&CK: T1015,T...	Medium	Defined	April 16, 2019
1009434 - Kubernetes Cluster Node	Medium	Defined	March 12, 2019
1008271 - Application - Docker	Medium	Defined	February 12, 2019
1003131 - Virtualization Software - VMware Server	Medium	Defined	December 4, 2018
1003105 - Database Server - PostgreSQL	Medium	Defined	October 16, 2018
1003374 - Application - PHP	Medium	Defined	August 21, 2018

Built-in ability to detect and alert to a potential compromise

WORLD-CLASS THREAT INTELLIGENCE

Deep Security's threat feed updates are delivered by a dedicated team of security experts that monitor threats 24/7, ensuring that the latest in protection is available to customers. This team continuously monitors from multiple sources of vulnerability disclosure information, as well as data coming directly from Trend Micro's global threat research centers. Trend Micro Research also receives information from the Zero Day Initiative™ (ZDI), the world's largest vendor-agnostic bug bounty program, employing over 3,500 external threat researchers worldwide who submit new vulnerabilities to Trend Micro. ZDI has been the leader in vulnerability discovery since 2007, disclosing over 1,400 vulnerabilities in 2018 alone.

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).

Global Sensor Network

Collects more information in more places

- 250M+ sensors
- 8 billon threat queries daily

Global Threat Intelligence

Accurately analyzes and identifies threats faster

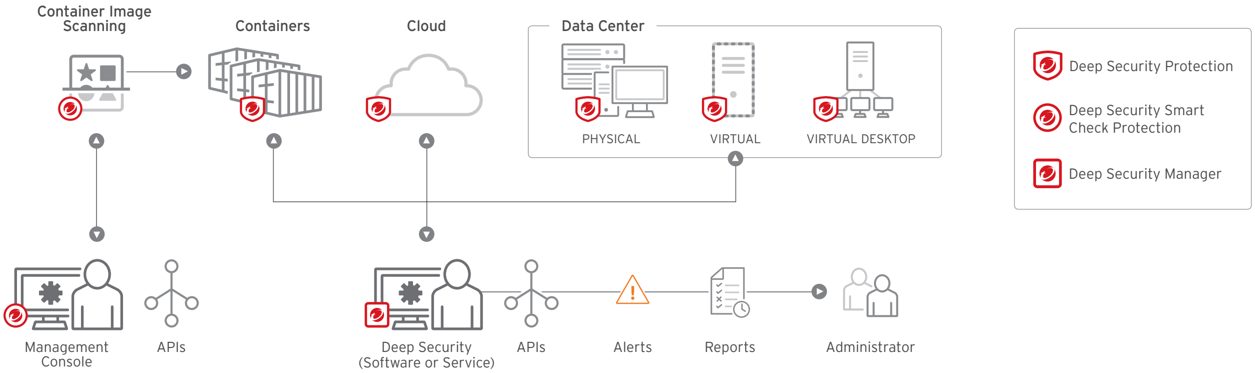
- 450+ internal researchers and 3,500+ external ZDI vulnerability researchers
- 24/7 monitoring

Proactive Protection

Blocks real-world threats sooner

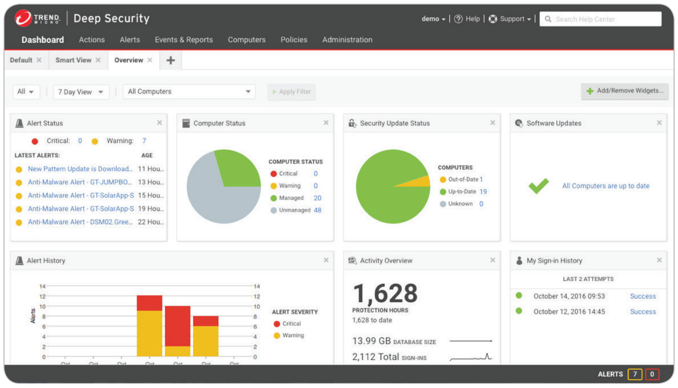
- Leader in vulnerability research, disclosing 1,400+ vulnerabilities in 2018 via the Zero-Day Initiative
- Rapid response to new threats like BlueKeep, Apache Struts, WannaCry, and Heartbleed
- 18M new threats identified and 180M blocked daily

CONTROL SECURITY ACROSS THE HYBRID CLOUD



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 2008. 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 throughout and beyond the migration to a new system or infrastructure. Deep Security's broad platform support and tight integration with leading platform providers enables unified visibility and protection across hybrid and multi-cloud deployments.



Critical: 0 Warning: 7

LATEST ALERTS:	AGE
New Pattern Update is Download...	11 Hou...
Anti-Malware Alert - GT-JUMPBO...	13 Hou...
Anti-Malware Alert - GT-SolarApp-S	15 Hou...
Anti-Malware Alert - GT-SolarApp-S	19 Hou...
Anti-Malware Alert - DSM02.Gree...	22 Hou...

COMPUTER STATUS	
Critical	0
Warning	0
Managed	20
Unmanaged	48

COMPUTERS	
Out-of-Date	1
Up-to-Date	19
Unknown	0

All Computers are up to date

1,628 PROTECTION HOURS
1,628 to date
13.99 GB DATABASE SIZE
2,112 Total SIGN-INS

LAST 2 ATTEMPTS	
October 14, 2016 09:53	Success
October 12, 2016 14:45	Success

Central dashboard gives full visibility of all security controls

Organizations around the world trust Trend Micro to secure their data center and hybrid cloud deployments, leveraging Deep Security's automated vulnerability shielding capabilities to protect their workloads across new and EOS platforms.

In addition, Trend Micro is viewed as a market leader not only by customers and partners, but also leading analyst firms. Ranked as the global market share leader in server security by IDC for seven years in a row, Trend Micro also delivers on all eight of **Gartner's core cloud workload security control layers** as measured by Trend Micro.

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

If you are running an unsupported system a system that is past or approaching end of support like Windows Server 2008 or Server 2003, you are likely concerned about how you can ensure consistent and cost-effective protection for the workloads and data on those systems. With many organizations continuing to run some amount of Windows Server 2008 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 the use of Microsoft's built-in software restriction policies, along with the deployment of additional security controls.

TREND MICRO INC.

U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1408.257.2003