SOLUTION BRIEF

PROTECT YOUR END OF LIFE WINDOWS AND LINUX OPERATING SYSTEMS

END OF SUPPORT IS NOT THE END OF BUSINESS

When software vendors announce a product end-of-life (EOL), customers typically have 24 to 30 months to plan and execute their migration strategies. This period is typically referred to as limited support. After the last day of support (also known as "end of support life date"), the product becomes obsolete, and the vendor will no longer automatically issue security patches. Customers have the option to purchase "extended or custom support" from the vendor after this date.

In many instances, the window for the availability of vendor support for the EOL product could be shorter than the time it would take for the customer to effectively migrate applications and processes to a new platform.

Customers may also be running custom applications that may not be compatible with the new platform. These gaps potentially expose unsupported systems to zero-day threats and new malware attacks. In order to address these potential risks, businesses will need to make some hard decisions:

- Run the applications in the unsupported platform.
- Execute an aggressive migration strategy for the mission-critical applications.
- Purchase an expensive extended support contract from the software vendor.
- Implement a security solution to harden and monitor the unsupported systems.

Businesses running enterprise-wide business applications on Microsoft Windows Server 2008 face this dilemma today. Extended support for Windows Server 2008 and Windows Server 2008 R2 ended on January 14, 2020. Microsoft will no longer automatically issue security patches for Windows Server 2008, leaving these systems highly vulnerable to zero-day attacks and other forms of malicious code.

Businesses may choose to continue running their applications on unsupported Windows servers for a multitude of reasons, such as:

- Minimize downtime for mission-critical applications and manage their budgets by staggering the migration to the new supported platform.
- Support a mission-critical, legacy, proprietary application that is not currently supported by the new platform.

Challenges of Legacy Systems

The following security and compliance issues influence how businesses will execute their Windows Server 2008 EOL migration and risk mitigation strategies:

1) Security threats from zero-day vulnerabilities and sophisticated malware

Security researchers continue to find new vulnerabilities in out-of-support operating systems (OS), which malicious entities are very eager to exploit.

Malicious hackers have been known to target unsupported systems as a method for gaining entry into a business's IT infrastructure. As large enterprises beef up their security protection, hackers are also using the unsupported systems in a large enterprise's supply chain ecosystem to gain entry.

2) Regulatory compliance and cyber security governance

Regulations like PCI-DSS and HIPAA-HITECH demand businesses take the necessary precautions to protect information and processes running on potentially vulnerable systems.

The Securities and Exchange Commission (SEC) has been very vocal in issuing guidelines and obligations for reporting on data breaches. In its Priorities letter, the SEC's Office of Compliance Inspections and Examinations (OCIE) included governance and supervision of information technology systems, operational capability, market access, information security, and preparedness to respond to sudden malfunctions and system outages.

Cyber security is now considered a primary risk factor and company annual

RECENT DATA BREACHES HAVE SHOWN THAT MALICIOUS HACKERS ARE TAKING ADVANTAGE OF VULNERABILITIES IN UNSUPPORTED SYSTEMS TO GAIN A BACKDOOR ENTRY FOR LAUNCHING THEIR ATTACKS.

reports must now reflect this. Running unprotected systems, therefore, exposes the business to compliance violations, resulting in hefty fines, sanctions and penalties.

3) Reputation damage and remediation associated with data breach

Unprotected systems makes the business more susceptible to data breaches, loss of critical, confidential data, and business disruption such as an inability to run mission-critical transactions or deliver customer services—all of which damage the brand and the customer's trust. On top of that, businesses will incur the costs associated with system remediation, investigation, and customer care following the attack.

4) Costs associated with testing and validating "custom" Microsoft patches

Customers also have to consider the investment to test and validate patches to the business applications running on top of the legacy servers. Even if the customer purchases patches from Microsoft, most application vendors won't support the patches as they cannot test that the patch will not impact their application. The onus on testing and validating the Microsoft custom patches rests on the customer. The customer will also have to assume the risks of application outages resulting from incompatibility with the patch. This leads to increased operational cost and risks.

What Options Are There?

Customers have four options for addressing their potential security exposure from running unsupported Windows Server 2008 systems after its last day of support:

Option 1: Do nothing. Some customers may choose to continue running applications on the unsupported platform when these applications are not considered as mission critical. Recent data breaches have shown that malicious hackers are taking advantage of vulnerabilities in unsupported systems to gain a backdoor entry for launching their attacks.

Doing nothing is not an option when the applications are mission critical but not compatible with the new platform. In this instance, customers will need to decide between executing an aggressive platform migration, purchasing a Customer Support Agreement, or enabling a server security hardening solution.

Option 2: Migrate applications into the new Windows Server Systems platform. This option is most suitable for taking advantage of the benefits of a new OS and its associated applications, or for minimizing the operational and management costs of IT systems by standardizing its hardware and software. Customers will be able to eliminate the risks and vulnerabilities associated with end-of-life systems.

Even though a migration can eventually lead to significant productivity, security and control benefits, it can still be an intimidating task. In the past, migrations involved manually collecting inventory and configuration data, throwing together solutions from disparate tools, writing and testing scripts to handle endless contingencies and dependencies, plus a thousand other endless routines that exhausts time, energy, money, motivation and executive patience.

Customers planning their platform migrations also need to take into account the impact an aggressive migration strategy would have on their operational budgets.

Option 3: Purchase "Custom Support Agreements (CSA)" from Microsoft. There are several critical issues to consider for customers evaluating this option:

- Only customers with a Premier Support Contract are eligible to purchase a CSA.
- Quotes can be expensive.
- Access to "custom support" for legacy platforms like Windows Server 2008 are not distributed automatically.

OPTION 4 CLEARLY PROVIDES THE BEST CHOICE, WITH BETTER AND MORE CONSISTENT HOST SECURITY, LOWER OVERALL COSTS AND MORE CONTROL WITH REGARDS TO LEGACY SYSTEM REPLACEMENT.

- Even if Microsoft rates a vulnerability at the highest critical level, Microsoft will commit to a patch but there are no strict SLAs for the responsiveness to deliver this patch. Other incidents not deemed as critical by Microsoft may or may not be fixed, but workarounds and suggestions may be given. This means that zero-day vulnerabilities remain unaddressed, opening systems to attack during instances of patch unavailability and other windows of exposure.
- CSAs are approved at a high management level within Microsoft on a case by case basis. The costs are not just the support fees – lengthy legal negotiations and approvals can be required for large corporations and this has to be taken into account.
- This option is not intended to be a long-term solution as "custom support" programs are specifically designed to help customers bridge the support gap as they migrate to new operating systems.
- This option also incurs a higher cost due to costly "custom support" and frequent testing and deployment of patches.

Option 4: Protect, Monitor, and Harden your legacy systems with Server Hardening Solutions. With this approach, the customer deploys HIPS/HIDS based security to harden the servers, monitor for any activities in the application and OS kernels, and lock down admin rights and access to applications.

This option will enable customers the ability to execute a server refresh and migration plan that fits their operational and budget objectives, and still protect their server infrastructure. Customers can minimize downtime and protect applications that are not currently compatible with the new OS platform.

Benefits of this approach:

- Improves the security posture of your servers by protecting them against known and unknown (zero-day) malware.
- Eliminates emergency patching, and minimizes downtime and IT expenses related to patching through proactive protection that does not require continuous updates.
- Reduces security incidents and remediation costs with continuous protection even if the server is unable to get the latest patches in a timely fashion.

Option 4 clearly provides the best choice, with better and more consistent host security, lower overall costs and more control with regards to legacy system replacement.

Symantec® Data Center Security

Symantec® Data Center Security: Server Advanced will help customers secure their Windows Server 2008 and other legacy systems effectively, so they can:

- Minimize downtime and business disruption
- Execute a platform migration plan that fits their operational and budget constraints
- Maintain compliance to security standards and fulfill regulatory obligations.
- Automate and orchestrate a microsegmentation strategy, thus applying security hardening policies at the application-level instead of relying on rigid network and security zones. This "application-level" security approach provides an additional layer of protection for mission-critical applications in the event a Windows Server 2008 system is compromised.

TODAY'S THREAT LANDSCAPE IS EVOLVING FAST. POWERFUL FEATURES IN THE DSC:SA LINUX AGENT PROTECTS LINUX SYSTEMS EFFECTIVELY IN REAL-TIME FROM EMERGING THREATS.

DCS:SA PROVIDES OUT-OF-THE-BOX HOST INTRUSION DETECTION AND PREVENTION POLICIES ACROSS PHYSICAL AND VIRTUAL SERVERS. IT ALSO EXTENDS SECURITY PROTECTION AND MONITORING INTO THE PUBLIC AND PRIVATE CLOUD AND ALL MODULES OF THE OPENSTACK CLOUD.

Symantec Data Center Security: Server Advanced offers the following features to protect the customers' legacy Windows Server 2008 systems:

Symantec Data Center Security Also Protects Legacy/EOL Linux Systems

Today's threat landscape is evolving fast. Powerful features in the DSC:SA Linux agent protects Linux systems effectively in real-time from emerging threats. DSC:SA Linux agent supports and protects end of life and exotic Unix/Linux platforms like AIX, HP-UX, Solaris and Red Hat 5. etc. The complete list of EOL DCS supported operating systems is available here.

EOL Unix/Linux systems can be protected with complete lockdown – no patching is required. Prime example that simply whitelisting trusted applications is insufficient. Bash is a trusted application that is core to Unix operating systems and applications and Application behavior control is required to ensure trusted applications can only perform their required functions, DCS:SA out of the box policy ensures Apache and other Unix processes are preconfigured to only have system and network access required.

DCS Linux Capabilities:

- Increased monitoring, detection and prevention security capabilities
- Behavioral Cotnrol mitigates zero-day attacks
- Policy enhancements deliver threat response to mitigate threats
- Centralized management for legacy Linux and UNIX platforms

For more information on Symantec Data Center Security: Server Advanced, download the Symantec Data Center Security: Server Advanced data sheet. As with any migration, the challenge is to execute it in an efficient, cost-effective, and sustainable manner while protecting end-user productivity. Symantec can meet that challenge with migration and deployment solutions that streamline processes to cut the expense, delay, and disruption of migration, keeping it in control.

SYMANTEC'S SOLUTIONS OFFER SIMPLIFIED, COMPREHENSIVE AND COST-EFFECTIVE PROTECTION AND MIGRATION OF WINDOWS SERVER 2008 SYSTEMS.

Secure or migrate with Symantec today.

The challenges of running unsupported legacy systems are not insignificant. But they are not insurmountable either. Just because OS support has ended does not necessarily mean businesses are left vulnerable to security threats or at the mercy of costly end-of-life support.

Symantec's solutions offer simplified, comprehensive and cost-effective protection and migration of Windows Server 2008 systems. Business operations continue uninterrupted and industry compliance regulations are still met. Companies also gain control and set the pace of system migration based on their business needs and schedule.

For more information on securing your legacy systems, visit us.

To learn more about Symantec Data Center Security: Server Advanced, visit: https://www.broadcom.com/products/cyber-security/endpoint/hybrid-cloud/data-center-security

About Us

Broadcom® Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software has an extensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com

November 23, 2022