DI PROTECT™

Windows 7 Support Ends January 2020: Digital Immunity Can Help

DIGITAL IMMUNITY

Stay Productive. Stay Secure.

Windows 7/Server 2008 Support Ends January 2020

These days, many of us want to know more about a product or service before engaging a vendor. To that end, Digital Immunity is creating a collection of concise documents - an Education Series - to educate and engage potential customers. During this learning process, you may want to engage with our staff to delve deeper into the product, delivery models, licensing and more. Once you contact us, we will ensure the right team members are engaged to help you finalize your assessment and demonstrate the associated Return-On-Investment.

The topic of this document is Windows 7/Server 2008 and Microsoft's plans to discontinue security patches after January 14, 2020. This sets up a challenge for companies as to how to best protect systems in manufacturing.

NOT PATCHING ANYWAY

In manufacturing, patches are inconsistently applied and hard to track, making it difficult to determine the current risk posture.

Coupled with the difficulty in getting downtime to apply patches, site teams may choose to delay patching - and delay, and delay. Patching is not a panacea for sure, but not having up-to-date patching does increase risk.

NETWORK SEGMENTATION IS HELPFUL BUT INSUFFICIENT

As with all cybersecurity mitigations, network segmentation is important but insufficient. It is an important part of a defense-in-depth strategy.

Remember NotPetya? The EternalBlue exploit was specifically designed to flow through firewalls to deliver the ransomware payload.

Once inside a segmented zone, a well-developed exploit will then flow from vulnerable system to vulnerable system creating a cascading effect of implications.

PAY MICROSOFT

Microsoft is working to improve the security of the Windows 10 operating system by implementing an automated patching service. However, in most manufacturing environments, automated patching is not feasible due to potential production impacts. Therefore the challenges of patching still exist even after an upgrade to Windows 10.

For Windows 7 and Server 2008, Microsoft will offer an extended support program, much like what was offered with Windows XP/2003. The costs for each year are:

- Year One: 5% of license cost,
- Year Two: 7% of license cost
- Year Three: 12% of license cost

HOPE IS NOT A STRATEGY

Everyone knows patching has its limitations. It is apparent every day in the news that new variants, Zero Days, are increasingly reaching their targets.

To significantly increase protection of Windows-based devices, workstations or servers, implementing DI PROTECT™ is the best answer in the marketplace.

Malware propagating around a network, aka "hacker-less", follows a two-stage process:

1. Exploit takes advantage of an opening or vulnerability and makes its way onto a system
2. Payload executes and negatively impacts the system

With DI PROTECT™ in Protect Mode, the file can get placed on the system but when it tries to execute, the binary code has not been verified as good so it will be stopped from executing before causing damage. A significant architectural advantage DI PROTECT™ provides that is not possible with the leading AV/NGAV vendors.

IS PATCHING NECESSARY?

Applying functional and security patches is a good practice in keeping the system updated so the integration of OS, apps and services continue to function well together.

Above, we discussed "hacker-less" malware and how DI works. Only allowing known good binary code to execute stops this type of malware from executing. This architectural approach is so powerful in protecting manufacturing operations.

Each company will need to make the risk call as to whether patching is necessary. Especially whether emergency patching is necessary. DI PROTECT™ reduces risk of "hacker-less" malware to the point that companies likely will choose to wait for planned outages or upgrades.

SUMMARY

Companies have much to think about when it comes to Windows 7 and Windows Server 2008 running in their manufacturing networks.

Is an upgrade possible between now and January 2020? Cost? Resource requirements? Validation requirements?

Does it make financial sense to extend support? The following URL provides some information as to the time period and cost estimates for extended support: https://www.itprotoday.com/windows-78/windows-7-extended-support-costs-revealed

Even with up-to-date security patching, many vulnerabilities still exist. Is it time to consider an alternative? An alternative that has a novel architectural approach to protecting Windows endpoints? An approach that accounts for the yet to be discovered malware/ransomware/Zero Days. Sleep better. Stay Productive. Stay Secure – DI PROTECT™.

What Makes Digital Immunity Different?

- In memory at run time prevention
- Works in air-gapped environments - completely self-contained
- Real prevention, unlike traditional AV detection - no preexisting knowledge of threats needed
- Hardening of OS and Applications
- No false positives
- No patch fatigue
- No extraction of data for analysis in the cloud
- Provide threat intelligence in context via the Control Center dashboard
- Remediation takes place on the device
- Works on “gray” systems as well due to DNA mapping process
- Doesn’t need to learn or update – not dependent on AI or machine/behavioral learning

About Digital Immunity

Digital Immunity, Inc. is an award-winning cybersecurity company that is redefining Endpoint Protection with its Bioinformatic based solution DI PROTECT™, a revolutionary technique that continuously verifies the integrity of executing code in memory at runtime.

Our patented Digital DNA Mapping technology prevents advanced threats, including APT's and zero-day attacks, from executing in memory at runtime, hardening your mission critical operating systems and applications, with no disruption of good processes or production. Using Digital Immunity's Control Center, you can mobilize your security team with real time actionable alerts and forensics artifacts in context.

Contact Us

60 Mall Road, Suite 309,
Burlington, MA 01803

Phone: (781) 425-8655
Email: Sales@digitalimmunity.com
Web: www.digitalimmunity.com