Carbon Black.

Avoid the Liability Associated with Running End-of-Life Operating Systems

Attacks like WannaCry and Petya/NotPetya have demonstrated that hackers are more familiar with the vulnerabilities of your unsupported systems than you are. When new patches are released for new systems, attackers easily reverse engineer the update and quickly find all the weaknesses in your end-of-life (EOL) systems. Traditional security solutions are powerless in detecting and preventing advanced attacks and unknown threats.

These systems often run critical business functions, have access to sensitive data, and have high performance and availability requirements making it difficult to upgrade or replace when vendors discontinue security support. As a result, they are perfect targets for bad actors to exploit due to the lucrative data they can hold and the difficulty of securing them with patch updates.

In addition to security threats, many of the regulatory and compliance mandates that organizations have to govern to in ensuring security and meeting data privacy statutes, involve rigorous levels of security that EOL systems, just aren't equipped to meet. When systems go EOL, they can easily be infiltrated due to the lack of patch management or effective endpoint protection. Vulnerabilities exist on those systems that will never be fixed. This is a critical area of focus for compliance professionals due to the substantial risk the organization is taking by continuing to operate them.

Compensating controls to protect EOL systems from increased liability and threat

There are compensating controls that businesses can implement to help reduce the liability associated with running EOL operating systems and keep them secure. Some of the key methods are network isolation/segmentation, virtualization, and application control/whitelisting.

Network isolation/segmentation

One option to protect EOL devices is to place critical servers on an isolated network to ensure the devices cannot interact with any machines outside of the isolated network or connect to the Internet. With network isolation, EOL devices are protected from threats, but drastically limit access to other critical assets including internet and cloud functions. While this security model can be used as a compensating control to mitigate threats, this option may pose business disruption and impact end-user productivity since most server host critical applications that need to be connected to corporate servers for employee access.

Virtualization

Hosting assets within a virtualized environment can provide a number of security benefits; increased control over critical assets, ease of re-imaging in the event of a compromise, and the ability to limit critical server exposure to an environment. If an asset becomes a target, it can be quickly isolated and re-initialized. but for critical servers running applications that require round-the-clock access, virtualization represents a possibility of increased administration and resources. It can also lead to failed compliance policies by virtue that in-scope data must be controlled or cannot run within a virtual environment.

Application control and whitelisting

Ranked as the #1 mitigation technique against security threats by the "Australian Signals Directorate's Essential Eight" (ASD), application whitelisting, is a security model focused on allowing known "good" applications to run rather than blocking known "bad." By only allowing trusted software to run, application whitelisting will stop exploits and reduce the administration associated with system and application patching and updates. In "default-deny" mode, application whitelisting is a highly effective compensating control to meet regulatory compliance standards and harden out-of-date systems.

Carbon Black.

Carbon Black locks down servers and critical/EOL systems with 100% efficacy

Trusted by more than 2,000 organizations, including more than 25 of the Fortune 100, to protect their corporate endpoints and servers, Cb Protection is a proven solution that can be affordably implemented to ensure the continued security of your devices beyond end of life.

Best Possible Protection

Cb Protection was the only solution to stop 100% of attacks in NSS Labs 2017 Advanced Endpoint Protection (AEP) test.

- Lock down systems: Stop malware, ransomware, and zero-day attacks
- Block unauthorized change: Built-in file-integrity monitoring, device control, and memory protection
- Harden critical systems: Support for embedded, virtual, and physical OSes

Proven Security and Compliance Control Efficacy

Coalfire, an independent qualified security assessor company tested and determined that Cb Protection can provide the flexibility to enable, manage, and meet PCI DSS requirements in such areas as file-integrity monitoring/control, change monitoring and alerting, and audit trail retention. The solution can also support the development of a combination of direct and compensating controls for requirements such as antivirus and patching (protection of unpatched systems).

- Maintain continuous compliance for key frameworks including PCI-DSS, ASD, GDPR, FISMA, NIST, Singapore MAS, and many others
- Monitor critical activity and enforce configurations to assess risk and maintain system integrity
- Secure EOL systems with powerful change-control and whitelisting policies

High Performance, Low Touch

Cb Protection is a proven and scalable application control solution. A single admin can easily manage over 10,000 systems, giving security teams total control with little ongoing effort.

- Out-of-the-box templates keep management overhead low
- In-built workflow and automation mechanisms help accelerate implementations
- Cloud-based reputation and detonation for fast decisions on trusted software
- Automate IT-trusted software to keep administration easy and achieve fast time-to-value