CYLANCE

BUSINESS BRIEF

SECURELY UPGRADING AND UPDATING WINDOWS 10

WHEN UPGRADES CREATE SECURITY RISKS

Migrating to Microsoft Windows 10 provides a unique opportunity to improve security posture and endpoint defenses without disrupting user productivity. Done wisely, organizations can move to a known-good state during migration and avoid security-related post-upgrade headaches.

One issue commonly faced during the upgrade process involves critical hardware and software systems being incapable of integrating with Windows 10. Many organizations respond to this problem by exempting these systems from the upgrade which leaves them permanently vulnerable to known security flaws. Moving to an advanced cybersecurity platform while upgrading to Windows 10 ensures these critical systems are not left defenseless.

ARTIFICIAL INTELLIGENCE ADVANTAGE

CylancePROTECT® and CylanceOPTICS™ offer critical protection to current Windows 10 systems and those exempted from the upgrade process. Cylance® uses artificial intelligence and machine learning models trained on millions of file samples to detect and prevent malicious code. This approach makes Cylance effective against known, unknown, and yet-to-be-created malware. Independent testing by SE Labs showed CylancePROTECT had the ability to detect and prevent current major malware families with an average lead time of over two years.

CylancePROTECT

CylancePROTECT offers several features beyond predictive AI malware prevention, including:

- Configurable device policies for endpoints that cannot upgrade/update
- File safe list allowing legacy and in-house software to run unimpeded
- Full disk scans need not occur with Cylance, prolonging the life of hardware
- Application control offers the option to lock down devices and prevent unsolicited software from being installed
- Providing visibility when PowerShell, Active Scripts, or macros are run, with options to block scripts entirely
- Device control that can be used to block Android, iOS, and other mass storage devices from transferring data on systems awaiting upgrades or excluded from Windows updates

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

CylanceOPTICS

CylanceOPTICS deploys machine learning models directly on the endpoint and monitors systems for suspicious or malicious behavior. It facilitates easy threat hunting, detailed root cause analysis, remote forensic investigations, and automated threat detection and response. CylanceOPTICS includes powerful research tools for threat responders:

- InstaQuery (IQ) - Allows threat responders to proactively hunt for malicious artifacts on endpoints in an enterprise within seconds
- Focus View - Creates a timeline of events leading up to each detection, providing root cause analysis for security events
- Auto Response – Can be configured to alert security teams to suspicious activity or perform automatic remediation steps upon detection

THREATZERO™

Cylance Consulting ThreatZERO Services offer critical assistance with integrating CylancePROTECT and CylanceOPTICS into environments. Cylance's security professionals ensure organizations achieves a zero-threat level by the end of deployment.

Additional ThreatZERO Services include:

- Complete install and configuration of Cylance products
- Internal resource training through which staff is trained in solution optimization
- Identification and remediation of potentially unwanted programs (PUPs) and malware
- Threat quarantine and alert classification

WINDOWS 10 UPGRADE SECURITY CHECKLIST

Ensuring organizations take advantage of recent enhancements and improved security in the latest Microsoft operating system can dramatically reduce exposure to zero-day vulnerabilities and other attacks targeting older systems. For a smooth transition, keep these five points in mind prior to, during, and after migration:

- What systems are being upgraded?
- What systems are exempt from the upgrade?
- How often will the endpoint/client security stack need updating?
- How long will it take to adequately secure each Windows 10 PC?
- How is security maintained on systems that are exempt from the completed upgrade?

Taking a pragmatic approach to Windows 10 migration will ensure organizations are ready for the unexpected and will cause as little disruption to the business as possible.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

©2018 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20181024-1119