ITPro Today™

EXECUTIVE SUMMARY

Sec Ops Strategies for the Windows Endpoint

Orin Thomas, Contributor, *IT Pro Today*
Dan Richings, Vice President of Solutions and Support, Adaptiva

OCTOBER 11, 2018

KEY TAKEAWAYS

- Ransomware is the most common threat against endpoints.
- Windows includes several protection technologies that improve end-user security.
- Basic endpoint security configuration plays a critical role in protecting the business.
- To remain secure, applications must be hardened, up to date, and audited.
- Adaptiva Client Health is the fastest, most automated way to manage endpoints.

in partnership with

adaptiva

Sec Ops Strategies for the Windows Endpoint

OVERVIEW

An organization's security depends not just on how well protected its servers and networks are, but on security around its endpoints. Attackers who are able to gain access to one unprotected, low-priority endpoint system can quickly find their way to other files and systems. Once inside, attackers have access to an organization's intellectual property or other information, which can result in big problems.

With so many endpoints in any organization—even when just considering Windows workstations—securing these systems can be daunting.

Adaptiva Client Health helps organizations ensure that their systems are healthy and secure.

CONTEXT

Orin Thomas discussed how organizations can secure their endpoints to keep common threats at bay. Dan Richings discussed Adaptiva Client Health, which offers a fast and automated way for businesses to secure endpoints.

KEY TAKEAWAYS

Ransomware is the most common threat against endpoints.

Threats against endpoints change over time as technology evolves. The most prevalent attacks today come from ransomware which monetizes the virus. Coin miners are a candidate to become the most prevalent attacks of the future.

Threats against Endpoints	
Ransomware	Encrypts the computer, requiring payment to unlock the system
Coin miners	Mines cryptocurrencies on infected computers in the background, monetizing the IT infrastructure
Destructive malware	Encrypts and/or destroys systems with the sole objective of demolishing an organization
Phishing attacks	Tricks individuals to reveal personal information using legitimate-looking email, web sites, or files
Remote access Trojans	Installs on a target network, allowing the attacker to use it as a bridging point to a more desired location on the network so that they can find and steal the most valuable data
Unauthorized software deployed by authorized users	Users within the organization deploy software to get around security protections put in place. Many are installed with non-malicious intent, such as a virtual private network (VPN) or BitTorrent Clients. Others, such as exploit tools, are installed with malicious intent.

Windows includes several protection technologies that improve end-user security.

Attackers typically gain access to critical systems through less critical and less protected client systems.

> If you've got well-hardened servers but poorly hardened clients, someone only needs to attack and compromise one client and use it as a bridging point to gain access to a more hardened server.
>
> *Orin Thomas*

Windows offers tools and technologies to increase protection for both client and server systems, making it more difficult for attackers to gain a foothold within the IT environment.

Sec Ops Strategies for the Windows Endpoint

Protection Technologies Built Into Windows Client and Windows Server	
Device Guard	– Virtualization-based protection of Code Integrity – Hardens operating system (OS) kernel against memory attacks – Requires trusted platform module (TPM) and secure boot – Works in conjunction with the Windows Defender (WD) Application Control (previously called Device Guard Configurable Code Integrity Policies)
Credential Guard	– Uses virtualization-based security to isolate secrets – Only specially signed processes can access this virtual container – Mitigates credential theft attacks
WD Application Guard	– Isolates enterprise-defined untrusted sites to protect employees interacting with the internet – Works for websites, cloud resources, and internal networks – If employees browse to untrusted sites in Microsoft Edge or Microsoft Explorer browser or in file explorer, the site is opened in an isolated Hyper-V container – Not to be confused with WD Application Control
WD Application Control	– Restricts applications users can run – Restricts code that runs in the System Core (kernel) – Blocks unsigned scripts and Microsoft installer scripts (MSIs) – Not to be confused with WD Application Guard
System Guard	– Protects and maintains the integrity of the system as it starts up – Protects and maintains the integrity of the system as it is running – Validates that system integrity has been maintained through local and remote attestation – Built into Windows 10, Sever 2016, and Server 2019
Exploit Guard	– Exploit protection uses OS security features to run applications in a more constrained way, making it less likely they can be used for an attack – Attack surface reduction reduces the number of points where an attacker can enter the system; requires WD Anti-Virus – WD Network Protection provides malware and social engineering protection; requires WD Anti-Virus – Controlled folder access controls which applications are able to access sensitive folders; provides ransomware protection

Basic endpoint security configuration plays a critical role in protecting the business.

Organizations can further improve system security and better protect the business by configuring endpoints to be more secure. Basic endpoint security configuration includes:

- **Lock down the pre-boot environment** to ensure the basic input/output system (BIOS) and unified extensible firmware interface (UEFI) settings cannot be modified without a password and that the device will not boot in a pre-boot execution environment (PXE) or from a USB without authorization.
- **Protect storage from offline attack** by encrypting storage so that the attacker cannot remove it and mount it elsewhere.
- **Lock down services** that should not be running and disable those that are not necessary
- **Understand needed local accounts,** including which local accounts and local groups should exist, and implement a Local Administrator Password Solution (LAPS).
- **Configure the local firewall** to block outbound traffic by default and greenlight exceptions.
- **Improve password protection** by disabling picture password policy and PIN sign-on and following current character minimums and age maximums. For example, the Australian Signals Directory (ASD) recommends 10 characters minimum and 90 days maximum age.
- **Configure caching group policies related to credential quotient.** Store only one previous logon in cache where the domain controller isn't available and do not store passwords for network authentication.
- **Improve authentication** with biometric or two-factor authentication, and by allowing authentication only during authorized hours.

Sec Ops Strategies for the Windows Endpoint

- **Regularly inspect systems** for physical devices, such as keyloggers.
- **Implement Internet Protocol Security (IPSec) on local networks,** encrypting network traffic.

To remain secure, applications must be hardened, up to date, and audited.

IT teams need to continuously maintain systems—including hardening applications and keeping software updated—to further secure systems from attack. Auditing sever activities helps IT teams quickly identify when a potential security issue has occurred so that it can be resolved immediately.

So that users can implement applications quickly and easily, they rarely ship in a hardened state. However, vendors typically offer guidance on how to harden their applications. The number of browser versions used in the organization should be limited, and those that are used need to be hardened.

Most updates released by vendors include code fixes and changes that close security holes or improve the overall security of the system. Automated processes ensure OSes, firmware, and applications are updated with the latest versions as soon as possible.

Auditing activity that occurs on the servers can help businesses identify security problems quickly. Orin Thomas recommends forwarding events to a centralized server. That way, if there is an attack, the attacker can't change the logs to hide their existence and what they've done.

Free tools, such as Windows Event Logging Forensic Logging Enhancement Services (WEFFLES), can analyze event logs and help detect suspicious activity.

Monitoring tools should also be used for endpoints to ensure the environments are up to date, and that no configuration drift has occurred that might impact security.

Recommended Hardening Guides

- Hardening Windows 10 Workstations; Australian Cyber Security Centre (ACSC)
- Security Technical Implementation Guides; U.S. Department of Defense (DOD) Information Assurance Support Environment

Adaptiva Client Health is the fastest, most automated way to manage endpoints.

With a growing global shortage of cybersecurity experts—an estimated 3.5 million by 2021—businesses need the right tools to help them tackle these security challenges.

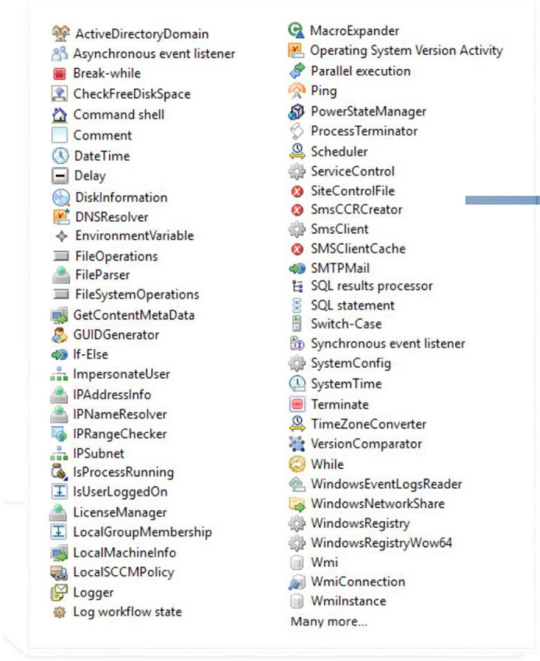
Adaptiva Client Health is an endpoint health and security engine that automatically checks an endpoint's health, diagnoses any problems, and instantly fixes security configuration management issues.

> Systems need to be healthy in order to remain secure, and systems [need] to be secure against outside threats in order to remain healthy.
>
> *Dan Richings*

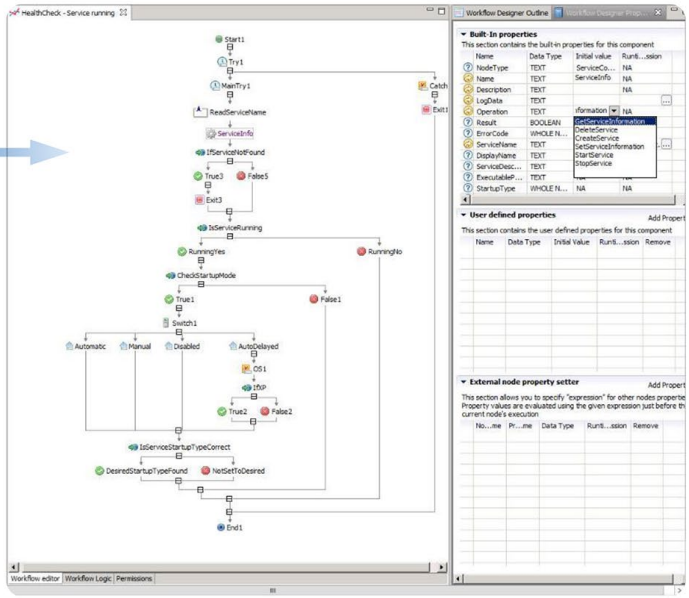
Client Health enables IT teams to respond rapidly to security breaches and vulnerabilities, patrol and enforce security policy, and keep all endpoints running and healthy. The solution also reduces help desk calls and speeds resolution, as well as automates complex custom needs.

Using an intuitive drag-and-drop workflow interface, Client Health users can simply create health checks that use even the most complex logic without writing any code. More than 190 workflow activities are included with the Adaptiva Client Health system, and others can be quickly assembled without code.

Sec Ops Strategies for the Windows Endpoint



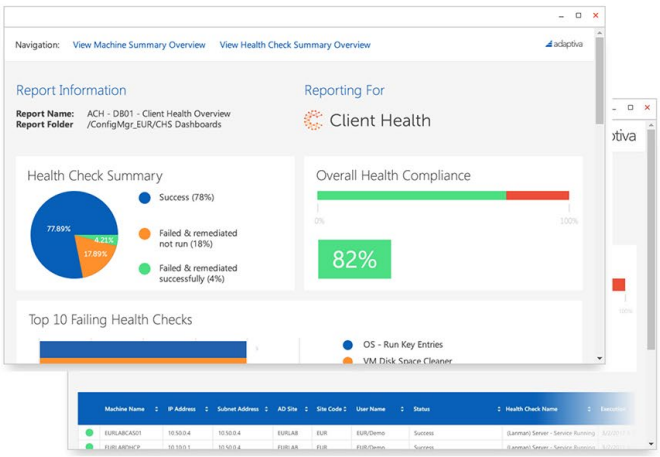
Drag and drop workflow creation



Adaptiva Client Health has dashboards and reports that allow users to quickly view the health status for endpoints across the organization. These tools also enable users to know when remediation occurred.

ADDITIONAL INFORMATION

For more information on Adaptiva Client Health visit https://adaptiva.com/products/client-health/



Sec Ops Strategies for the Windows Endpoint

BIOGRAPHIES

Orin Thomas

Contributor, *IT Pro Today*

Orin Thomas is an MVP, an MCT and has a string of Microsoft MCSE and MCITP certifications. He has written more than 30 books for Microsoft Press IT Pro topics. He is an author at PluralSight and is a contributing editor at **Windows IT Pro** magazine. He has been working in IT since the early 1990's and regularly speaks at conferences in Australia and around the world.

Dan Richings

Vice President of Solutions and Support, Adaptiva

Based in the UK, Dan Richings drives Adaptiva's outstanding engineering and exceptional customer experience throughout EMEA. Dan has an extensive technical skill set, and has been working with SCCM since it was still "SMS." He has been performing operating system deployment since 2001. His diverse background includes technical and leadership roles in the retail automotive, multinational engineering, and international project development and construction industries. Dan holds a computer science degree, BSc (Hons) Computing, from Swansea University.

In his free time, Dan enjoys racquetball, airsoft, and karting.