Switching to Windows 10?

Let's Boost Your Endpoint Security With a Least Privilege Strategy

thycotic

INTRODUCTION

Leverage Your Windows 10 Migration to Implement a Least Privilege Strategy

All software is prone to security defects – bugs in code and flaws in architecture – that provide opportunities for hackers. Windows is a prime example. Security bulletins from Microsoft reveal a number of critical vulnerabilities discovered across new and old versions of Windows that allow malware to enter via user- controlled workstations. Managing to eliminate these vulnerabilities often requires Windows users to constantly play catch up.

Microsoft recommends that organizations take a proactive risk management approach to add much-needed layers of security. As the primary way to protect your endpoints, Microsoft recommends adopting a policy of least privilege: “All users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. Doing so provides protection against malicious code, among other attacks. This principle applies to computers and the users of those computers.”[2]

All users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more.

- Microsoft Recommendation

In this whitepaper we’ll demonstrate how adopting a policy of endpoint least privilege can neutralize threats. We’ll outline the options for least privilege, including using Microsoft’s built-in least privilege tools, and give you the information you need to create the most effective and enforceable endpoint security strategy.

If you are considering a switch to Windows 10—or have already begun to plan—this whitepaper is for you.

Moving To Windows 10 Can Make You Safer — But Windows Alone Could Require A Lot More Work

The security vulnerabilities in Windows 7 have made many organizations anxious about malware, especially after Kaspersky revealed that 98% of the victims infected by the WannaCry/ WannaCrypt virus were running Windows 7.3 Microsoft says that Windows 7 "does not meet the requirements of users of modern technology, nor the higher security needs of IT departments," admitting the older OS "is based on long-outdated security architectures."[4]

Not surprisingly Microsoft is encouraging its customers to transition to Windows 10, indicating that Windows 10 devices are "58% less likely to encounter ransomware than when running Windows 7."[5] With Windows 10 Microsoft has enhanced and built many free tools to give IT and security teams the opportunity to close some of the security gaps exposed in previous versions of Windows. While this sounds promising, fully implementing them typically requires additional time and administrative resources.

Microsoft takes a componentized approach to endpoint security in Windows 10, from anti-virus protection to privilege management. This involves several individual products, which must be installed, configured and maintained independently via separate interfaces. Each of these security tools has its own limitations compared with best-in-class third-party solutions. Taken together, they can add up to a lot of work for admins, requiring admins to piece together and manage multiple systems. Most IT and security professionals probably don't have the time or resources to manage endpoint security in this way.

98%

of the victims infected by the WannaCry / WannaCrypt virus were running Windows 7

- Kaspersky

The Limits Of Windows' Approach To Endpoint Security

Anti-Virus Protection

Windows Defender Advanced Threat Protection (ATP), baseline anti-virus protection, is now built in for all Windows 10 devices. With ATP, Microsoft is entering the Endpoint Detection and Response (EDR) market, taking on "next-generation" Endpoint Protection Platforms (EPPs) and EDR solutions with a free tool.

According to independent tests, Windows Defender addresses the most common attacks, but in many cases generates false positives and negatives that affect its performance.[6]

In fact, Windows Defender itself is not immune from security defects. At the end of 2017, Microsoft released a patch to plug a vulnerability that can be exploited when a user downloads a specially crafted file that is scanned by Windows Defender and causes remote code execution.

Even when supplementing Windows Defender with additional anti-virus products, this approach to endpoint security has limitations. Almost three quarters of hackers report that traditional anti-virus tools are irrelevant or obsolete, and don't adapt quickly enough to block emerging threats.[7] Relying on anti-virus solutions that scan and identify malware only AFTER it has already infiltrated your organization increases your risks. By the time post-incident solutions flag issues and you act to fix them, hackers may be long gone, taking your sensitive data with them.

Reactive virus protection alone is not enough to keep you safe.

73%

of hackers report that traditional anti-virus tools are irrelevant or obsolete, and don't adapt quickly enough to block emerging threats

- Thycotic 2017 BlackHat Report

Preventing Windows Breaches With Least Privilege *AND* Application Control

The most effective way to prevent your Windows devices from becoming an entry point for threat agents is by implementing a foundational security policy based on the principle of least privilege. You can prevent unknown code, including malware, from executing malicious processes and penetrating your network by removing credentials that allow them to run as an administrator. **It's been widely reported that removing administrative rights from endpoints will mitigate the vast majority of Windows security vulnerabilities.**

Without access to administrative credentials, even if malware successfully downloads onto an endpoint, any damage is contained. Threat agents won't be able to make system changes, log keystrokes, or run other harmful processes. Most importantly, they won't be able to leverage those credentials to circumvent security controls, progress through your network or cause further damage.

Application control must be part of your least privilege strategy.

Microsoft offers a number of free tools to help organizations adopt a least privilege strategy. However, Microsoft's approach still leaves several important aspects of least privilege unaddressed that can limit its utility and adoption.

Organizations that have successfully implemented least privilege understand that application control is essential to making this type of restrictive policy a reality. Without application control, removing administrative rights from endpoints means users are not able to run programs and processes that are essential to doing their jobs. They can't install printers, can't update software, can't run common conferencing applications and can't change system preferences. Legacy applications often won't run. ActiveX controls and scripts can break. The IT desktop support team is flooded with requests to assist and productivity grinds to a halt.

Windows 10 may replace endpoint detection and response tools but it doesn't replace application control.

Gartner has said that security protections within Windows 10 make it a more viable solution for organizations looking to replace dedicated Endpoint Protection Platforms (EPPs) and Endpoint Detection and Response (EDR) solutions. However, Gartner points out that even in Windows 10 Microsoft does NOT have the capabilities to support the application control requirements to make least privilege work and prevent risks associated with local user accounts.[8]

Applocker Offered a Good Place *to Start*

Microsoft began offering application control in Windows 7 Ultimate and Enterprise Editions with the first introduction of Applocker. It provides basic whitelisting, allowing only a shortlist of known-good applications to run on workstations.

Applocker relies on the security team to maintain and update whitelisting policies as the primary method of preventing malware. However, it lacks the capability to maintain a constantly updated list of known-bad applications to blacklist and it doesn't allow users to greylist or sandbox application that are new or unknown.

Lack of self-service workflow for application elevation requests can also lead to spikes in desktop support calls.

In addition, Applocker lacks audit trail capabilities. This limits the security team's ability to demonstrate compliance with least privilege mandates, application usage policies, or malware protection requirements, essential in regulated industries.

Despite advocating least privilege, Microsoft makes it difficult to implement.

Device Guard Requires an Additional Commitment of Administrative Resources

With Windows 10, Microsoft introduced Device Guard, which has similar functions to Applocker. On the positive side, Device Guard is hardware-enforced and therefore is more tamper resistant than Applocker. However, Device Guard offers less flexible control and requires more effort to use.

Device Guard has an allowed list of applications only – no blacklist and no greylist options. In addition, it is managed with PowerShell scripts rather than a user interface. Gartner calls it "difficult to configure, manage, and report." The heavy requirements include I/O memory management unit (IOMMU), virtualization extensions, and Unified Extensible Firmware Interface (UEFI) 2.3.1 secure boot, as Gartner says, "relatively new hardware and specific configuration options to function, which may complicate and add time to your rollout process."

"Those planning to move to a default deny environment with their Windows 10 migration should exploit Device Guard only if they can also invest in the administration resources to manage it," Gartner recommends. "Use third-party application control solutions until Microsoft improves Device Guard management."[9]

Use third-party application control solutions until Microsoft improves Device Guard management.

- Gartner Reccomendation

Least Privilege Needs A Holistic Approach To Privilege Management

Besides the limitations of Microsoft's virus protection and application control tools, endpoint protection also requires a holistic privilege management strategy that covers your privilege security needs from endpoints to credentials.

This multi-layered approach ensures you have protection at every step of an attacker's chain. Let's say a hacker has been able to bypass virus scans, avoid blacklists, and circumvent your application control policies to gain access to an endpoint that has hidden admin privileges. You can't allow the threat to progress and reach deeper inside your organization. You need to raise the fences to prevent a full-scale data breach.

If this were to happen, you could immediately block continued progress of the attack by changing all passwords throughout your organization at once. Stolen credentials will fail, and the attacker won't be able to manipulate additional systems or access confidential information.

You can't allow a threat to progress and reach deeper inside your organization. You need to raise the fences to prevent a full-scale data breach.

Microsoft privileged credential protection is limited to managed Windows machines.

Microsoft's Local Administrator Password Solution (LAPS) and Group Policy Client-Side Extension (GPO) provide a centralized storage of secrets/passwords in Active Directory and allow you to manage, randomize, and rotate local administrator passwords. However, the Microsoft approach only works for managed Windows machines. What about third parties, consultants, contractors, and Mac users who need privileged credentials to access accounts? Even if third-party machines are not joined to your domain, their accounts ARE connected and can be an entry point for threats.

In addition, Microsoft's privilege solution requires updates to the Active Directory schema. GPO delivery is not always timely or reliable. It only defines group members at a single point in time, which means you have to consistently check groups to manage policies.

In Windows 10, Credential Guard uses virtualization-based security to isolate and protect domain credentials. Malware running with administrative privileges in the Operating System is not able to extract secrets protected by the virtualization layer.

This tool is powerful, but it can be time consuming to configure and manage, with no central user interface.

TAKE ACTION

For A Windows 10 Upgrade that Improves Endpoint Security

Windows 10 is the perfect opportunity to improve your endpoint security by moving to a least privilege model. However, the limitations of Microsoft tools may require more time and resources than you have available. Instead, you should explore options as part of your Windows 10 planning that offer a more efficient and effective least privilege implementation.

Prepare By “Rightsizing” Your Applications And Usage Policies

The move to Windows 10 is a chance to reset and do some housecleaning that (it’s ok to admit) may be long past due. Unaccounted for systems running unknown and unmanaged applications are among the most common security vulnerabilities.

> **The move to Windows 10 is a chance to reset and do some housecleaning that (let’s face it) may be long past due.**

This is the time to take inventory of every application your teams are using and evaluate them in depth. Are they still being used or are you paying for software you that you don’t need or have overprovisioned? Are licenses up to date? Do they need patches? Which ones will require updates when you move to a new OS? Have users installed software which is not known or supported by IT?

Once you have an accurate list, you’ll be better able to create policies that account for approved and blocked applications. Also, you’ll know if you have any legacy applications or controls that require administrative rights, so you can maintain business continuity even as you move to a least privilege model.

Leverage The Migration Timing To Remove Credentials

Whether you choose in-place upgrades, wiping and reloading images, or buying new machines, you can remove local administrative credentials from endpoints at the same time you roll out Windows 10.

Take care that no hidden or hardcoded administrative credentials remain within endpoints.

For maximum efficiency, you can use agent-based least privilege solutions that can be packaged together with Windows 10 and implemented simultaneously

Prioritize Application Control for Least Privilege Success, Even As Your Organization Changes

Understanding the limitations of Microsoft's tools, you'll want to make sure the privilege management solution you choose includes application control that is easy for security teams, desktop support, and users to adopt and maintain.

You want a tool that will support your least privilege strategy over the long term, not just for a single point in time.

PRIVILEGE MANAGEMENT SOLUTION CHECKLIST

✓ **Look for a tool with an integrated, intuitive user interface that lets you create and adapt application elevation policies as you need.**

✓ **Insist on greylisting and sandboxing capabilities that allow you to manage new and unknown applications.**

✓ **Avoid solutions that are dependent on Active Directory and Group Policies. For maximum flexibility and scale, find a tool that is always looking for changes and will adjust to make sure users and endpoints always meet your least privilege policies.**

✓ **Make sure you can manage non-domain devices as well as non-Windows endpoints, without the need to bolt on additional tools.**

✓ **Test out reporting capabilities so you can demonstrate compliance with least privilege best practices, show which applications were requested, elevated and executed, and which types of malware have been prevented.**

✓ **Review smart phone applications to make reviewing greylist requests as quick and easy as possible while still getting rigorous reputation guidance.**

ABOUT THYCOTIC

Thycotic, a global leader in cybersecurity, is the fastest growing provider of Privileged Access Management (PAM) solutions. Thycotic enables you to minimize privileged credential risk, limit user privileges, and control applications on endpoints and servers. Thycotic's award-winning PAM solutions improve cybersecurity, increase productivity, and help demonstrate compliance for more than 7500 organizations worldwide, including Fortune 500 companies.

Thycotic Privilege Manager automatically removes administrative rights from domain and non-domain managed endpoints, including privileged credentials that are hidden or hard-coded. It uses policy-based controls to elevate applications users need to do their jobs, without requiring administrative credentials or requesting IT support. Because Privilege Manager elevates applications and not the user, it never leaves a window open for hackers, even for a moment. As your organization grows and users continually explore applications, Privilege Manager adjusts.

Automate Virtually All Application Elevation

With Thycotic Privilege Manager, the vast majority of application elevation requests are managed automatically, based on granular, contextual policies. As a result, most applications are either approved or denied without any extra work from IT, leaving only specialized or custom applications for hands-on review and approval. Your support queue is smaller and you have more time for other IT and security priorities.

Endnotes

1. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models
2. https://www.techrepublic.com/article/98-of-wannacry-victims-were-running-windows-7-not-xp/
3. https://www.techrepublic.com/article/98-of-wannacry-victims-were-running-windows-7-not-xp/
4. https://www.techrepublic.com/article/despite-privacy-concerns-microsoft-calls-windows-10-the-most-secure-version-of-windows/ 6. http://www.av-comparatives.org/wp-content/uploads/2016/01/avc_sum_201512_en.pdf
7. https://thycotic.com/resources/black-hat-2017-survey/
8. Gartner, Windows 10 Enhances Security, April 2017
9. Ibid