Analyst Program

Product Review

How SMBs Can Benefit from the Security Protections of Windows 11

Written by Jake Williams

January 2022

Introduction

This paper highlights some of the security features in Windows 11 and how they prove useful specifically to small and medium businesses (SMBs). While all organizations should find the security features in Windows 11 of interest, SMBs in particular have extremely limited security budgets. With Windows 11, Microsoft has integrated more core security features into the operating system, providing an ecosystem for security from the chip to the cloud, increasing the value proposition for SMBs to upgrade to Windows 11. Those charged with implementing IT and security in SMBs should review the security features highlighted in this paper and consider the additional value of upgrading to Windows 11 immediately.

Note: To remain focused on SMBs, this paper intentionally avoids discussion of some enterprise security features of Windows 11 that offer substantial protection. For those SMBs with enterprise licensing (either Windows E3[1] *or Windows E5, which includes Microsoft Defender for Endpoint*[2]*), the security value proposition is substantially higher.*

Built on Zero-Trust Principles

The core principle of zero trust is that everything, including users, devices, and applications, must be explicitly verified before any resources are accessed. This approach stands in stark contrast to the traditional operating mode of "permit all, deny by exception," which has obviously failed to scale to the number and diversity of threats targeting organizations today. The only viable plan to turn the tables on threat actors is to build a framework that allows only verified activities. As we discuss in this paper, Microsoft built Windows 11 on a foundation of zero-trust principles.

Data points used for verification can include user identity, device status (such as patch level), and location, among others. Any verification is only as good as the data used in the verification consideration. That's why it's important that any operating system used for zero-trust deployments be built on top of a zero-trust foundation.

Least privilege is another important caveat to any zero-trust framework. Application isolation ensures that even if an application runs untrusted code, it can be isolated from the operating system, limiting the blast radius of a successful attack. Whereas legacy operating system frameworks often required service (and user) accounts with substantial permissions, Microsoft engineered Windows 11 from the ground up to allow systems administrators to provision accounts with the principles of least privilege applied.

[1] For more information, see "Windows 10/11 Enterprise E3 in CSP," Microsoft, https://docs.microsoft.com/en-us/windows/deployment/windows-10-enterprise-e3-overview

[2] For more information, see "Microsoft Defender for Endpoint," Microsoft, https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide

Legacy security models rely on keeping a threat actor out of the network in the first place. Many security professionals analogize this model to a piece of candy: a hard, crunchy outside and a soft, gooey inside. Zero trust, in contrast, follows a principle of "assume breach." Because Microsoft designed the security model of Windows 11 from the ground up to assume that some component has already been compromised, threat actors will find it orders of magnitude more difficult to remain undetected in the environment than in traditional architectures. And although remaining undetected in a zero-trust environment is difficult, persisting is orders of magnitude more difficult.

The zero-trust principles integrated into Windows 11 don't stop at the PC; they continue into the cloud. This proves especially important for SMBs, which are much more likely to have cloud-first deployment models because they lack traditional data centers.

Hardware Security Root of Trust

Without a hardware root of trust, nothing stops a threat actor from subverting the boot process and the operation of the system. Most IT professionals have heard the term Trusted Platform Module (TPM), but few understand what it really means. Even fewer understand the value it provides. A TPM provides a hardware root of trust that ensures only software (and firmware) signed with trusted keys is allowed to execute. Prior to TPM adoption, any threat actor that gained system-level permissions could modify the bootloader, remain undetected throughout the boot sequence, and embed itself into the kernel throughout the lifetime of the operating OS.

> **If every component (users, devices, applications, etc.) could be implicitly trusted, we would have no need for zero trust. But zero trust isn't something that we can just bolt on; we must build it in to the architecture. Because Microsoft designed the security model of Windows 11 from the ground up to assume that some component has already been compromised, threat actors will find it orders of magnitude more difficult to remain undetected in the environment than in traditional architectures.**

This isn't just a theoretical attack. Threat actors bypassing boot-time protections have a long history. And it's not just nation-state threat actors who have bypassed boot-time protections. In 2020, a modified version of the TrickBot malware was discovered compromising firmware.[3] Unified Extensive Firmware Interface (UEFI) compromises offer advanced persistence, and also afford the threat actor the possibility of rendering compromised hardware unusable. SMBs that have especially limited budgets for bulk hardware replacement find both situations particularly untenable. When an SMB devotes limited IT resources to rebuild a malware-infected machine, it can't afford to repeat the process because a hidden threat has persisted in the firmware. Compounding this issue is the fact that these same SMBs are much less likely to identify the threat persisting in the first place than those with large enterprise security teams. Replacing hardware that has been rendered inoperable by a malicious firmware update also disproportionately impacts SMBs.

[3] "The Internet's Most Notorious Botnet Has an Alarming New Trick," Wired, www.wired.com/story/trickbot-botnet-uefi-firmware/

Trusted Boot

Trusted boot ensures that every instruction that executes on the CPU is part of a digitally signed software package. We've known for years that digitally signing applications is an excellent mechanism for ensuring software security. But when the application begins execution, what checks the integrity of the application's code? The short answer is that system processes (underpinned by the Windows kernel) perform the application signature checking. Any compromise to the kernel would allow a threat actor to bypass application signature checking and access or modify all data processed in software.

Trusted boot changes the game for threat actors. In the past several releases, Microsoft has continually upped the stakes for threat actors trying to persist in kernel space. The TPM verifies that the firmware is digitally signed before loading it. The firmware ensures the OS bootloader is signed and also ensures that no one has tampered with Secure Boot policies. Next, execution is transferred to the bootloader, which ensures that the OS kernel has an appropriate digital signature. Once loaded, the Windows kernel ensures that every kernel-mode component (including device drivers) possess a valid digital signature. One such driver is an Early Launch Anti-Malware (ELAM) driver, often used by security products to load into memory and begin offering protection before any user processes are permitted to run. This process, while complex, is necessary to prevent the compromise of workloads run by the SMB after boot.

Advances in network security features for Windows 11 mean that SMB administrators can spend less time thinking about network security and more time attending to their software workloads.

Network Security

Advances in network security features for Windows 11 mean that SMB administrators can spend less time thinking about network security and more time attending to their software workloads. In this section, we discuss network security features that make Windows 11 a more robust offering for SMBs, all either enabled by default or provisioned with minimal administration.

DNS Security

With DNS security, Windows 11 protects by default all DNS requests from eavesdropping and modification. DNS is a prime attack vector for threat actors who want to create interception attacks (sometimes referred to as *person-in-the-middle*) by redirecting network traffic. These attacks also prove inherently difficult for organizations of any size to detect and block. Recognizing this threat, many major web browsers encrypt their DNS traffic by sending it over HTTPS. Windows 11 offers exactly the same security for all DNS requests, eliminating this key attack vector.

Windows 11 gives organizations the flexibility to implement DNS over HTTPS by default, or instead of using the feature they can inspect traffic with an on-premises solution such as a DNS firewall. The flexibility is present because some worry that DNS over HTTPS removes the ability of organizations to monitor their own DNS traffic for indicators of compromise. Although this scenario is more likely to concern enterprises than SMBs, Windows 11 enables administrators to disable this feature so that traffic inspection happens in an on-premises environment where perhaps the organization has a DNS firewall.

Windows Defender Firewall

The Windows Defender Firewall has also been updated for Windows 11 with new features to keep threat actors out of the network and to provide easier management. With ubiquitous encryption becoming an impediment to network analysis, IPSec inspection is now integrated into the firewall's packet monitor service (something not easily obtained with out-of-band monitoring). Additionally, the verbosity of the logs for Windows Defender Firewall has been substantially enhanced, ensuring that analysts can more easily tie observed behaviors to alerts (and vice versa). Windows Defender Firewall, a robust host-based firewall, offers excellent performance and ease of management and analysis without the need to purchase and manage third-party tools.

SMB 3.1.1 File Services

Server Message Block (SMB, the core file-sharing technology in Windows) file services benefit from numerous enhancements in Windows 11. These include more advanced (and faster) encryption and SMB signing, enhanced performance with Remote Direct Memory Access (RDMA), and SMB over QUIC.

Perhaps the most exciting change to SMB 3.1.1 file services is SMB over QUIC. For those not familiar with QUIC (pronounced "quick"), this transport layer protocol offers speed on par with UDP with the reliability of TCP. QUIC is a protocol that has been formally standardized by the IETF and offers several benefits, not the least of which is that packets are always encrypted (including the handshake). Additionally, it offers the capability to recover from an IP address change (something TCP cannot). This feature proves extremely important in environments where IT doesn't control the entire network infrastructure from end to end (for example, when users tether from a mobile device).

SMB over QUIC is a strong reason to upgrade immediately. Many SMBs maintain VPN services only to provide access to their on-premises Windows file shares. With SMB over QUIC, we can expose these services directly over TCP port 443. QUIC provides a tunnel for SMB 3.1.1 secured with TLS 1.3 (integrated into the core of Windows 11[4]), the same encryption technology employed by today's leading VPN appliances. This feature ties in well with the least-privilege discussion earlier. In SMB environments where the VPN is only present to provide SMB 3.1.1 file services, removing the VPN ensures that a compromised endpoint can't access the rest of the network. Further, in recent years threat actors have exploited unpatched VPN appliances as a common initial entry vector. Due to licensing challenges (patches are often only available for an additional licensing fee) and vulnerability management difficulties, SMBs find themselves disproportionately affected by these threats. We cannot overstate the value that SMB over QUIC brings to SMBs.

[4] "Taking Transport Layer Security (TLS) to the Next Level with TLS 1.3," Microsoft, www.microsoft.com/security/blog/2020/08/20/taking-transport-layer-security-tls-to-the-next-level-with-tls-1-3/

BitLocker

BitLocker encryption isn't new in Windows 11, but it integrates with modern hardware controllers more tightly than in previous OS versions. The Windows Encrypted Hard Drive feature is built on top of BitLocker and ensures that encryption remains always on and that encryption keys are secured on the hard drive.

Due to budgetary constraints, many SMBs operate on shoestring IT budgets. Many IT professionals in SMBs have resisted implementing drive encryption because they believe it degrades performance on the machine and negatively affects the user experience. BitLocker encryption is offloaded to processors on the drive controller; no CPU cycles are needed. Additionally, because BitLocker is a core Windows component, recovery keys needed by IT are stored in the existing Windows infrastructure with Active Directory and Azure AD.

It is difficult to overstate the importance of drive encryption for SMBs. SMBs typically find themselves less able to recover from a data breach that results from the theft of a user's laptop. Given the remote workforce model, employees more often travel with their devices (thus increasing the chances of lost or stolen devices).

Deploying BitLocker encryption with Windows 11 on all office PCs can be the difference between filing a police report for stolen property and filing a data breach notification with attorneys general from multiple states.

Disk encryption doesn't just provide value adds for mobile devices such as laptops. With the advances in BitLocker performance in Windows 11, it's easy to implement BitLocker on desktop machines too. SMBs that often have relatively poor physical security when compared with larger enterprises will find this especially important. Many SMBs operate in shared office buildings where thieves can steal computers by simply crawling through drop ceilings or punching through a sheet of drywall. Given the increasingly onerous data breach notification landscape, a stolen PC at an SMB is more likely than ever to trigger breach notification requirements. Deploying BitLocker encryption with Windows 11 on all office PCs can be the difference between filing a police report for stolen property and filing a data breach notification with attorneys general from multiple states.

If a device does go missing, Windows 11 location services offer the possibility of recovery in a way not available in legacy versions of Windows. We must enable location services to permit recovery. When MDM is employed, remote wipe of the device is also supported.

Cloud Integration

Windows 11 has unparalleled cloud integration, which should spark the immediate interest of SMBs. The use of cloud technology allows SMBs to scale quickly (without burning significant operational expenditure funds), and Windows 11 is ready to integrate.

OneDrive for Business

We can configure OneDrive for Business with Windows 11 to automatically back up files to the cloud. In addition to the obvious convenience of data mobility, OneDrive for Business offers significant security benefits. SMBs tend not to have robust backup and recovery programs. They also typically operate with hardware that is less fault tolerant (for example, servers without redundant power supplies or RAID 1 arrays). IT professionals at SMBs know they're operating without the sort of disaster recovery redundancy and fault tolerance employed by bigger enterprise players, but they lack the resources to replicate it. When properly implemented, OneDrive for Business with Windows 11 bridges that gap and provides secure offsite backups that already integrate with Active Directory authentication.

OneDrive for Business also offers an effective control against ransomware attacks. SMBs are disproportionately affected by modern ransomware attacks because, lacking an enterprise security team, they often miss the lateral-movement operations that occur before the ransomware deployment. OneDrive for Business backups can make the difference between the SMB paying a ransom and trivially recovering their data.

Endpoint Management

Windows 11 supports endpoint management without the need for additional agents installed on the endpoint. While enterprises typically administer devices using Microsoft Intune, many SMBs use third-party managed service providers (MSPs) for their IT needs. In these cases, the SMB will use whatever endpoint management solution the MSP uses, though certainly Intune is optimized for use with Windows 11. The capability of Windows 11 to support endpoint management without the need for additional agents straining CPU resources is a key feature for SMBs.

Endpoint management also ensures that configurations remain consistent, even offering the capability to reapply settings that someone has changed. In a perfect world, end users wouldn't have the ability to change settings, particularly those impacting security, but in reality, this is often not the case. SMBs are particularly prone to provisioning accounts with too many permissions, usually to allow users to self-service in the face of limited IT staff, increasing this risk. Traditionally, endpoint management would synchronize changed settings on the next settings sync (often hours for remote devices). Endpoints running Windows 11 can implement Config Lock, however, thus effectively preventing even users with local administrator permissions from changing key configuration values. The value of Config Lock, especially for organizations like SMBs that have small IT and security teams, is substantial.

Authentication Controls

Windows 11 provides numerous authentication enhancements. SMBs will find great value in many of these authentication controls. All organizations can benefit from these authentication control enhancements, but SMBs and those with limited security staff will see the largest gains.

Passwordless Authentication

Like organizations of every size, SMBs face increasing risk of password theft and replay attacks. Windows Hello provides a passwordless authentication model that limits the impact of any password-theft attack. Windows Hello allows users to log in to their devices with a chosen PIN. If the device supports biometric collection (such as a fingerprint reader), we can use that in lieu of a PIN. The TPM on the device stores the actual user credentials that are used for authenticating to remote services. When a user enters his or her PIN, it unlocks the credentials on the TPM, which are loaded into memory and used to authenticate to other services, such as Azure Active Directory.

Windows Hello removes many of the traditional problems with password complexity, creating a scenario where password complexity matters substantially less. We know that even when provided with extremely strict password requirements, many users still choose easily hackable passwords. This problem disproportionately affects those that have fewer resources for security awareness training, such as SMBs.

Using passwordless authentication from Windows Hello limits phishing attacks in two important ways. First, if the user doesn't know their password in the first place, it's difficult for them give it to attackers. Second, the PIN matters on only a single device. Sure, users can be tricked into giving away their PINs, but in most scenarios, this doesn't do anything for the attacker. The PIN decrypts a user's credentials on the TPM of his or her device only. Taking a user's PIN to another device doesn't get the threat actor anything.

TAKEAWAY

SMBs should consider implementing Windows Hello for Business and integrating with Azure Active Directory. Additionally, they should consider using the Microsoft Mobile Authenticator as a second factor of authentication (multi-factor authentication, or MFA). Microsoft Mobile Authenticator integrates seamlessly with Windows authentication. Unlike SMS-based MFA, Microsoft Mobile Authenticator is not subject to SIM swapping attacks.

Credential Guard

Windows 11 implements Credential Guard and Remote Credential Guard. Credential Guard prevents threat actors who gain administrative permissions on a machine from dumping the memory of the authentication process (lsass.exe) to gain credentials from memory. This process is implemented using virtualization-based security, effectively storing the credentials in a separate virtual machine.

Remote Credential Guard goes even further, supporting authentication while ensuring that your credentials never pass to the remote system. This feature is significant because threat actors routinely use techniques such as NT LAN Manager (NTLM) relay to steal credentials as systems administrators connect to a compromised system under their control. By implementing Remote Credential Guard, we can safeguard credentials even when users connect to an attacker-controlled system.

Access Controls and Least Privilege

This section covers some of the most important access control features for SMBs as related to Windows 11.

Non-Administrative Users

Users with excessive privileges undermine a good security architecture. SMBs, like all organizations, suffer when users log in with administrative accounts to perform everyday tasks. Windows 11 provides easy user management, and when combined with integrated device management policies and Azure Active Directory, it's easy to provision non-administrative accounts for the majority of SMB workloads. While the standard of not using administrative accounts for everyday use hasn't changed, thanks to Microsoft the ease with which it can be done has.

User Account Control

Everyday tasks should not require administrative permissions on a system. SMBs should create user accounts without administrator permissions for daily tasks. Windows 11 also supports User Account Control (UAC) to ensure that even when the logon account has administrative permissions, the applications running do not automatically inherit those privileges.

For the sake of convenience, many SMBs disable UAC for their administrative users. They absolutely should not. UAC ensures that applications always run in the context of a non-administrator account but can request elevation for any changes that require administrative permissions.

UAC provides two important benefits for SMBs:

1. In environments where SMBs use administrative logons for daily work, UAC limits the blast radius for any malicious code that they might otherwise execute.
2. The second key benefit is a bit subtler. SMBs regularly use custom-developed applications and lack the budget for significant security testing of those applications. While those same applications traditionally would fail without admin permissions or function adequately with admin permissions, with UAC, SMBs can determine the specific functions requiring elevation. After testing these applications with UAC, it is often determined that only some specific functions (and as such only limited numbers of users) even need elevated access. This approach allows the SMB to provision only the users who actually perform functions requiring administrative permissions with those elevated privileges.

Application Control

Windows Defender Application Control (WDAC) is another key Windows 11 security feature for SMBs. Organizations determine specific applications that should never be allowed to run and enforce this with WDAC configurations. In more secure configurations, WDAC can include the full list of applications that a given user should execute. This configuration takes a bit more upfront work to determine the full list of applications that should be allowed but provides a far superior level of security.

A WDAC configuration where only certain pre-approved applications can be executed by a user is another component of a zero-trust architecture. Admittedly, some users have unpredictable workloads and may find this type of configuration onerous. However, many SMBs employ task workers with entirely predictable workloads. In these cases, WDAC can provide two benefits: security and oversight. When a user attempts to execute an application not in the WDAC allow list, it is blocked and an alert is generated. Supervisors can examine alerts to identify employees with changing job requirements that they might otherwise miss. Of course, an alert might also result from an employee engaging in non-work activity.

Even in environments without task workers, SMBs can still trivially deploy WDAC on their servers. Server workloads rarely change, making keeping up with a strict “allow listed only” policy a breeze. In most cases, we need to retrain the WDAC profile only with monthly Windows updates.

Conclusion

In this paper, we highlighted security features of Windows 11 that should demonstrate a high value proposition for SMBs. However, we’ve barely scratched the surface. Windows 11 offers additional productivity features that we didn’t even attempt to cover in this paper purely due to scope. Windows 11 has numerous other security features that SMBs will likely find interesting that also didn’t make the cut. Finally, those SMBs with enterprise licensing (see information in introductory section of this paper) will find the security value proposition substantially higher. Security-conscious system administrators should consider upgrading to Windows 11 sooner rather than later.

Sponsor

SANS would like to thank this paper’s sponsor:

Microsoft