Secure the Windows boot process

By officedocspr5

Archived: 2026-04-05 16:19:36 UTC

Windows has many features to help protect you from malware, and it does an amazingly good job. Except for apps that businesses develop and use internally, all Microsoft Store apps must meet a series of requirements to be certified and included in the Microsoft Store. This certification process examines several criteria, including security, and is an effective means of preventing malware from entering the Microsoft Store. Even if a malicious app does get through, Windows includes a series of security features that can mitigate the effect. For instance, Microsoft Store apps are sandboxed and lack the privileges necessary to access user data or change system settings.

Windows has multiple levels of protection for desktop apps and data, too. Windows Defender Antivirus uses cloud-powered real-time detection to identify and quarantine apps that are known to be malicious. Windows Defender SmartScreen warns users before allowing them to run an untrustworthy app, even if it's recognized as malware. Before an app can change system settings, the user would have to grant the app administrative privileges by using User Account Control.

Those components are just some of the ways that Windows protects you from malware. However, those security features protect you only after Windows starts. Modern malware, and bootkits specifically, are capable of starting before Windows, completely bypassing OS security, and remaining hidden.

Running Windows 10 or Windows 11 on a PC with Unified Extensible Firmware Interface (UEFI) support ensures that Trusted Boot safeguards your PC against malware right from the moment you power it on. This protection continues until your anti-malware software takes over. If, by any chance, malware manages to infect your PC, it won't be able to stay hidden. Trusted Boot can verify the system's integrity to your infrastructure in a manner that malware can't mask. Even for PCs without UEFI, Windows offers enhanced startup security compared to earlier Windows versions.

To begin, let's take a closer look at rootkits and their functioning. Following that, we'll illustrate how Windows can ensure your protection.

The threat: rootkits

Rootkits are a sophisticated and dangerous type of malware. They run in kernel mode, using the same privileges as the OS. Because rootkits have the same rights as the OS and start before it, they can completely hide themselves and other applications. Often, rootkits are part of an entire suite of malware that can bypass local logins, record passwords and keystrokes, transfer private files, and capture cryptographic data.

Different types of rootkits load during different phases of the startup process:

- **Firmware rootkits.** These kits overwrite the firmware of the PC's basic input/output system or other hardware so the rootkit can start before Windows.
- **Bootkits.** These kits replace the OS's bootloader (the small piece of software that starts the OS) so that the PC loads the bootkit before the OS.
- **Kernel rootkits.** These kits replace a portion of the OS kernel so the rootkit can start automatically when the OS loads.
- **Driver rootkits.** These kits pretend to be one of the trusted drivers that Windows uses to communicate with the PC hardware.

The countermeasures

Windows supports four features to help prevent rootkits and bootkits from loading during the startup process:

- **Secure Boot.** PCs with UEFI firmware and a Trusted Platform Module (TPM) can be configured to load only trusted OS bootloaders.
- **Trusted Boot.** Windows checks the integrity of every component of the startup process before loading it.
- **Early Launch Anti-Malware (ELAM).** ELAM tests all drivers before they load and prevents unapproved drivers from loading.
- **Measured Boot.** The PC's firmware logs the boot process, and Windows can send it to a trusted server that can objectively assess the PC's health.

Figure 1 shows the Windows startup process.


Screenshot that shows the Windows startup process.

Figure 1. Secure Boot, Trusted Boot, and Measured Boot block malware at every stage:

Secure Boot and Measured Boot are only possible on PCs with UEFI 2.3.1 and a TPM chip. Fortunately, all Windows 10 and Windows 11 PCs that meet Windows Hardware Compatibility Program requirements have these components, and many PCs designed for earlier versions of Windows have them as well.

The sections that follow describe Secure Boot, Trusted Boot, ELAM, and Measured Boot.

Secure Boot

When a PC starts, it first finds the OS bootloader. PCs without Secure Boot run whatever bootloader is on the PC's hard drive. There's no way for the PC to tell whether it's a trusted OS or a rootkit.

When a PC equipped with UEFI starts, the PC first verifies that the firmware is digitally signed, reducing the risk of firmware rootkits. If Secure Boot is enabled, the firmware examines the bootloader's digital signature to verify that it hasn't been modified. If the bootloader is intact, the firmware starts the bootloader only if one of the following conditions is true:

- **The bootloader was signed using a trusted certificate.** For PCs certified for Windows, the Microsoft certificate is trusted.

- **The user has manually approved the bootloader's digital signature.** This action allows the user to load non-Microsoft operating systems.

All x86-based Certified For Windows PCs must meet several requirements related to Secure Boot:

- They must have Secure Boot enabled by default.
- They must trust Microsoft's certificate (and thus any bootloader Microsoft has signed).
- They must allow the user to configure Secure Boot to trust other bootloaders.
- They must allow the user to completely disable Secure Boot.

These requirements help protect you from rootkits while allowing you to run any OS you want. You have three options for running non-Microsoft operating systems:

- **Use an OS with a certified bootloader.** Because all Certified For Windows PCs must trust Microsoft's certificate, Microsoft offers a service to analyze and sign any non-Microsoft bootloader so that it will be trusted by all Certified For Windows PCs. In fact, an open source bootloader capable of loading Linux is already available. To begin the process of obtaining a certificate, go to https://partner.microsoft.com/dashboard.
- **Configure UEFI to trust your custom bootloader.** All Certified For Windows PCs allow you to trust a non-certified bootloader by adding a signature to the UEFI database, allowing you to run any OS, including homemade operating systems.
- **Turn off Secure Boot.** All *Certified For Windows* PCs allow you to turn off Secure Boot so that you can run any software. This action doesn't help protect you from bootkits, however.

To prevent malware from abusing these options, the user must manually configure the UEFI firmware to trust a non-certified bootloader or to turn off Secure Boot. Software can't change the Secure Boot settings.

The default state of Secure Boot has a wide circle of trust, which can result in customers trusting boot components they may not need. Since the Microsoft 3rd Party UEFI CA certificate signs the bootloaders for all Linux distributions, trusting the Microsoft 3rd Party UEFI CA signature in the UEFI database increase s the attack surface of systems. A customer who intended to only trust and boot a single Linux distribution will trust all distributions - more than their desired configuration. A vulnerability in any of the bootloaders exposes the system and places the customer at risk of exploit for a bootloader they never intended to use, as seen in recent vulnerabilities, for example with the GRUB bootloader or firmware-level rootkit affecting boot components. Secured-core PCs require Secure Boot to be enabled and configured to distrust the Microsoft 3rd Party UEFI CA signature, by default, to provide customers with the most secure configuration of their PCs possible.

To trust and boot operating systems, like Linux, and components signed by the UEFI signature, Secured-core PCs can be configured in the BIOS menu to add the signature in the UEFI database by following these steps:

1. Open the firmware menu, either:
    - Boot the PC, and press the manufacturer's key to open the menus. Common keys used: Esc, Delete, F1, F2, F10, F11, or F12. On tablets, common buttons are Volume up or Volume down. During startup, there's often a screen that mentions the key. If there's not one, or if the screen goes by too fast to see it, check your manufacturer's site.

    - Or, if Windows is already installed, from either the Sign on screen or the Start menu, select Power ( ) > hold Shift while selecting Restart. Select Troubleshoot > Advanced options > UEFI Firmware settings.
2. From the firmware menu, navigate to Security > Secure Boot and select the option to trust the "3rd Party CA".
3. Save changes and exit.

Microsoft continues to collaborate with Linux and IHV ecosystem partners to design least privileged features to help you stay secure and opt-in trust for only the publishers and components you trust.

Like most mobile devices, Arm-based devices, such as the Microsoft Surface RT device, are designed to run only Windows 8.1. Therefore, Secure Boot can't be turned off, and you can't load a different OS. Fortunately, there's a large market of ARM processor devices designed to run other operating systems.

Trusted Boot

Trusted Boot takes over where Secure Boot ends. The bootloader verifies the digital signature of the Windows kernel before loading it. The Windows kernel, in turn, verifies every other component of the Windows startup process, including the boot drivers, startup files, and ELAM. If a file has been modified, the bootloader detects the problem and refuses to load the corrupted component. Often, Windows can automatically repair the corrupted component, restoring the integrity of Windows and allowing the PC to start normally.

Early Launch anti-malware

Because Secure Boot has protected the bootloader and Trusted Boot has protected the Windows kernel, the next opportunity for malware to start is by infecting a non-Microsoft boot driver. Traditional anti-malware apps don't start until after the boot drivers have been loaded, giving a rootkit disguised as a driver the opportunity to work.

Early Launch anti-malware (ELAM) can load a Microsoft or non-Microsoft anti-malware driver before all non-Microsoft boot drivers and applications, thus continuing the chain of trust established by Secure Boot and Trusted Boot. Because the OS hasn't started yet, and because Windows needs to boot as quickly as possible, ELAM has a simple task: examine every boot driver and determine whether it is on the list of trusted drivers. If it's not trusted, Windows doesn't load it.

An ELAM driver isn't a full-featured anti-malware solution; that loads later in the boot process. Windows Defender (included with Windows) supports ELAM, as does several non-Microsoft anti-malware apps.

Measured Boot

If a PC in your organization does become infected with a rootkit, you need to know about it. Enterprise anti-malware apps can report malware infections to the IT department, but that doesn't work with rootkits that hide their presence. In other words, you can't trust the client to tell you whether it's healthy.

As a result, PCs infected with rootkits appear to be healthy, even with anti-malware running. Infected PCs continue to connect to the enterprise network, giving the rootkit access to vast amounts of confidential data and

potentially allowing the rootkit to spread across the internal network.

Measured Boot works with the TPM and non-Microsoft software in Windows. It allows a trusted server on the network to verify the integrity of the Windows startup process. Measured Boot uses the following process:

1. The PC's UEFI firmware stores in the TPM a hash of the firmware, bootloader, boot drivers, and everything that is loaded before the anti-malware app.
2. At the end of the startup process, Windows starts the non-Microsoft remote attestation client. The trusted attestation server sends the client a unique key.
3. The TPM uses the unique key to digitally sign the log recorded by the UEFI.
4. The client sends the log to the server, possibly with other security information.

Depending on the implementation and configuration, the server can now determine whether the client is healthy. It can grant the client access to either a limited quarantine network or to the full network.

Figure 2 illustrates the Measured Boot and remote attestation process.

 Screenshot that shows the Measured Boot and remote attestation process.

Figure 2. Measured Boot proves the PC's health to a remote server:

Windows includes the application programming interfaces to support Measured Boot. However, to take advantage of it, you need non-Microsoft tools to implement a remote attestation client and trusted attestation server. For example, see the following tools from Microsoft Research:

- TPM Platform Crypto-Provider Toolkit
- TSS.MSR

Measured Boot uses the power of UEFI, TPM, and Windows to give you a way to confidently assess the trustworthiness of a client PC across the network.

Summary

Secure Boot, Trusted Boot, and Measured Boot create an architecture that is fundamentally resistant to bootkits and rootkits. In Windows, these features have the potential to eliminate kernel-level malware from your network. With Windows, you can trust the integrity of your OS.
