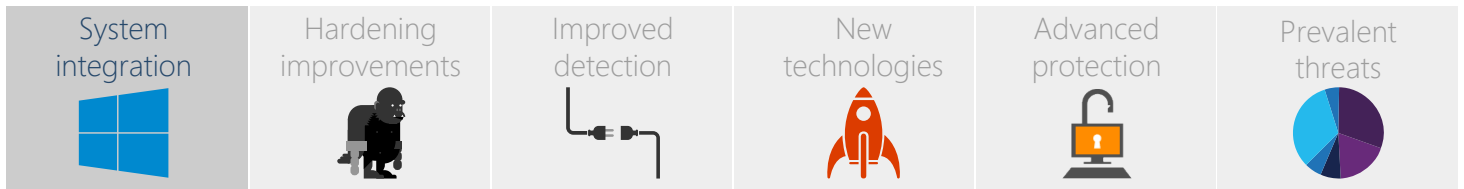


Malware Protection Center



Windows Defender in Windows 10: System integration

Windows 10 brings a number of advances and features over previous Windows operating systems.

This report details the new technologies and features that are included in Windows Defender in Windows 10.

Windows 10 integration

In Windows 10 we've changed how Windows Defender integrates with the operating system, and how users can interact with it. Windows Defender is now integrated into the standard settings system, and helps protect the device from its very first boot up.

End users will now always see the Windows Defender name, regardless of whether it is an enterprise-level managed device (for example, via the System Center Configuration Manager or Intune) or a consumer device.

However, there are no changes in the management experience for Windows Defender in Windows 10 from other supported versions of Windows.

Better protection

As malware becomes more aggressive and destructive, the need to be protected at all times also becomes more important.

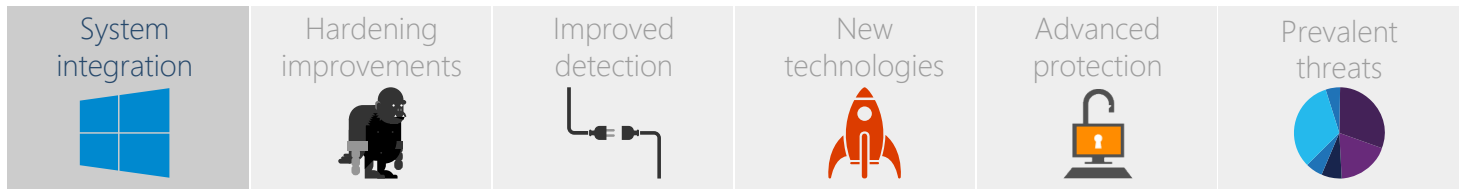
In order to help protect users, Windows Defender in Windows 10 will turn on malware protection if other protection is not installed or has expired through stronger logic and decision making.

For example, Windows Defender is enabled by default, but if a user installs a different antimalware product with real-time protection, Windows Defender is silently disabled. If the installed product is determined to be inactive or outdated, Windows Defender is enabled and the user is notified about the change.

In all cases, users are informed of the changes and given information to help them choose how they want to manage their protection – either by updating their existing antimalware product, or continuing with Windows Defender.

Administrators can configure how this process plays out in managed situations, and it can be controlled either via Group Policies, with System Center Endpoint Protection (SCEP) or Microsoft Intune.

Malware Protection Center



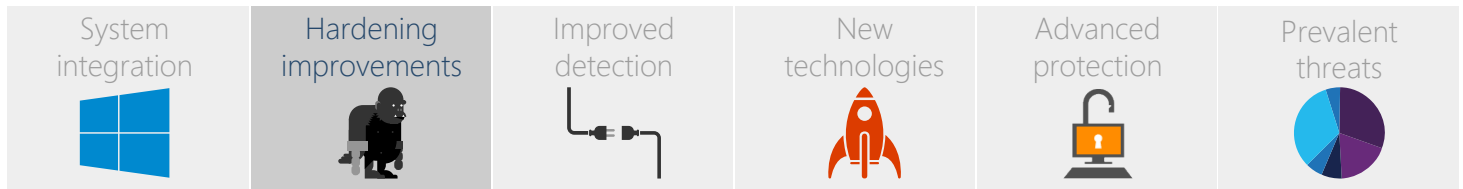
Operating system, enterprise-level management, and BYOD integration

Windows 10 introduces a mobile device management (MDM) interface for devices running Windows 10. The introduction of this management infrastructure makes it possible for IT administrators to use MDM-capable products, such as Microsoft Intune, to manage Windows Defender on Windows 10 devices, including BYODs that aren't domain-joined.

Many of the settings and actions are similar between MDM and domain-joined machines.

For more information on how Windows 10 includes MDM and multi-user capabilities, see the "In the Cloud" blog [Integrating Windows 10 identity innovations with EMS and SCCM](#).

Malware Protection Center



Hardening improvements

Windows Defender in Windows 10 has improved tamper protection, registry and folder modification tampering, and real-time protection service hardening.

As malware evolves, it often enters a stage where the authors attempt to override basic protection processes and services. There are a number of methods malware use, including tampering with the protection service's registry entries, folder structures, or even direct modification of the service.

Windows Defender in Windows 10 hardens itself against these attempts with features that isolate, identify, and work to prevent this tampering.

Protected services

In Windows 10, Windows Defender runs as a [protected service, which isolates it from tampering](#) by standard-user-privileged and most administrator-privileged malware attacks.

Antimalware registry and folder hardening

Windows 10 has an extensible registry blocking mechanism that prevents changes from any administrator and user-mode process, and Windows Defender also prevents changes to selected folders. For example, Windows Defender prevents changes to its Definition Update folder and certain registry keys used by Windows Defender for debugging.

The list of processes that are permitted to make changes and the registry keys and folders that are protected are updated along with definition updates.

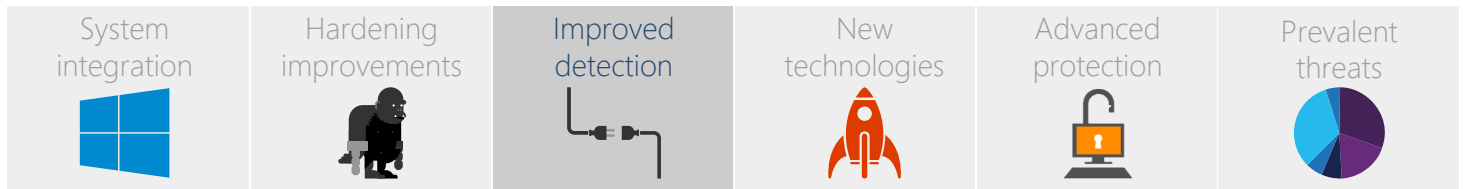
Quick restoration

In some cases, tampering can only be resolved through restoration.

For example, in Windows 10, Windows Defender uses its [Early Launch Antimalware \(ELAM\) driver](#) to remove any malicious changes at the next reboot. This limits kernel-mode malware from making lasting changes to Windows Defender's mini-filter driver.

Additionally, as malware may also tamper with Windows security settings, Windows Defender will restore tampered components when it finds malware. In particular, it restores User Account Control (UAC) and Windows Update settings to their defaults when it remediates malware known to tamper these features. This helps ensure that critical updates (and antimalware signatures) are delivered even if malware attempts to block or prevent them.

Malware Protection Center



Improved malware detection

Contextual clues for Windows Defender

Windows Defender in Windows 10 has improved remediation, reporting, and malware detection capabilities. The context can be divided into three areas:

- Local context
- Securely persisted context
- Shared global context

Local context

Entry point context

Windows Defender detects particular methods of malware infiltration in a system. This means it can target advanced scanning at these higher risk “entry points”, and more reliably prevent specific threats from infecting a system.

Windows Defender uses the [mark of the web \(MOTW\)](#) to both determine whether the file was originally from an external location and the level of scanning that is required.

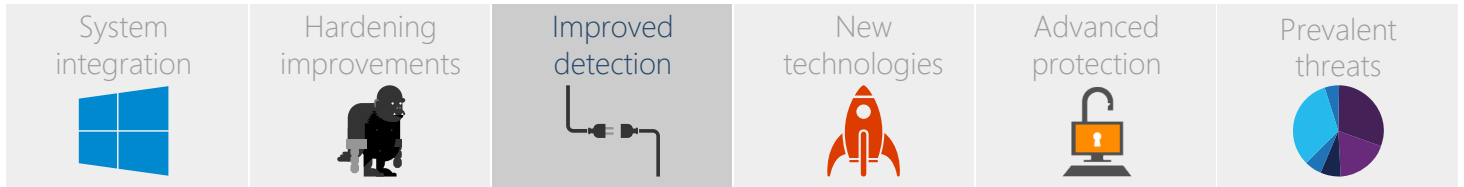
In addition to the MOTW, Windows Defender tracks the entry point context of each file. This context is made available during file use, even if the file is used or executed at a later point in time.

Elevation change context

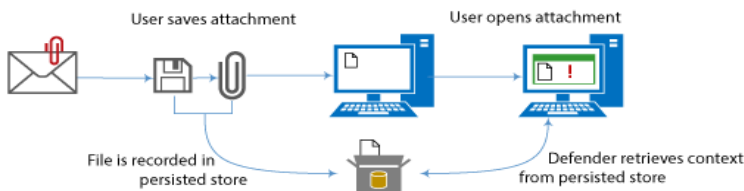
Windows Defender has a new synchronous scan hook at the User Account Control (UAC) elevation point to perform an in-depth scan of the process or file requesting additional privileges. See the [Antimalware Scanning Interface \(AMSI\) section on the New technologies tab](#) for more details.

Process [integrity levels](#) are also tracked as another indicator of elevation point context and the Secure Event Tracing for Windows channel also provides this type of context. See the [Secure events section on the New technologies tab](#) for more details.

Malware Protection Center



Securely persisted context



Windows Defender tracks and stores these contexts in a secure manner in its Persisted Store, which it then uses for its behavior (or “heuristic”) monitoring engine.

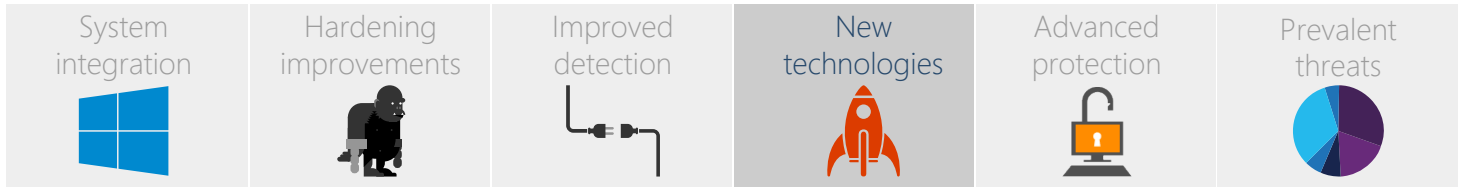
The Persisted Store allows Windows Defender to maintain the state for files and processes that its scanning engines can use at a later time. This allows for a workflow such as the following, and illustrated above:

- Email arrives via Outlook or other mail client, and the user saves the attachment
- Several days later, the user decides to run the attachment
- When run, the file requires administrator privileges (through a UAC prompt)
- Windows Defender is able to maintain that state and determine the level of scanning that needs to be done, as it knows the file came from Outlook due to its records in the Persisted Store

Shared global context

In Windows 10, Windows Defender takes advantage of technologies such as [UAC and AMSI scanning](#), [cloud protection](#), and [offline cleaning outside of the main operating system shell](#) form part of a shared, “global” level of protection.

Malware Protection Center



New technologies

Smart UAC

In Windows 10, Microsoft implemented a new technology that allows Windows Defender to work closely with User Account Control (UAC) requests.

When the UAC system is triggered, it requests a scan from Windows Defender before prompting for elevation.

When Windows Defender scans the file or process it determines if it's malicious or not. If it's malicious, the user will see a message explaining that Windows Defender blocked the file or process from executing; if it's not malicious, then UAC will run and display the usual elevation request prompt.

Secure events

Windows 10 introduces new Secure Event Tracing for Windows (Secure ETW channel). [Normal ETW events](#) can be consumed by any user-mode process, but the new secure channel has been designed such that only a security application that is running as a [Protected Process](#) (such as Windows Defender)) can consume these security-related or protection-impacting events.

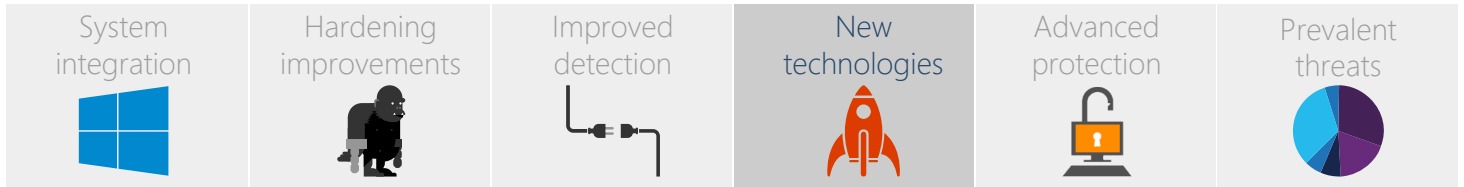
As malware cannot listen to these events, the new Secure ETW channel provides security applications with an extra advantage in avoiding tampering and being aware of possible malware.

Antimalware Scanning Interface (AMSI)

The [Antimalware Scan Interface \(AMSI\)](#) is a generic public interface standard that allows applications and services to integrate with any antimalware product present on a device.

AMSI allows security applications or services to scan in-memory scripting content (such as PowerShell, the Windows Scripting Host, JavaScript, and JScript) and obfuscated dynamic content for malicious activity. The scan results can be then be returned to the calling application or service.

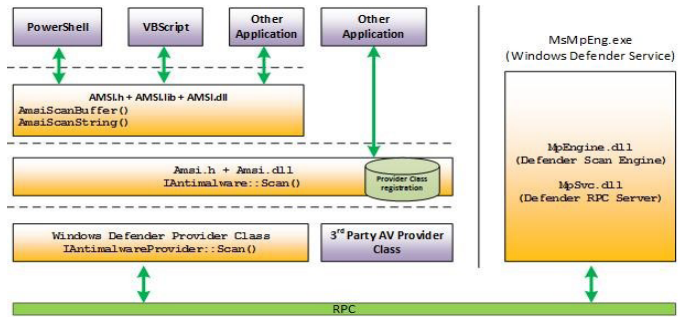
Malware Protection Center



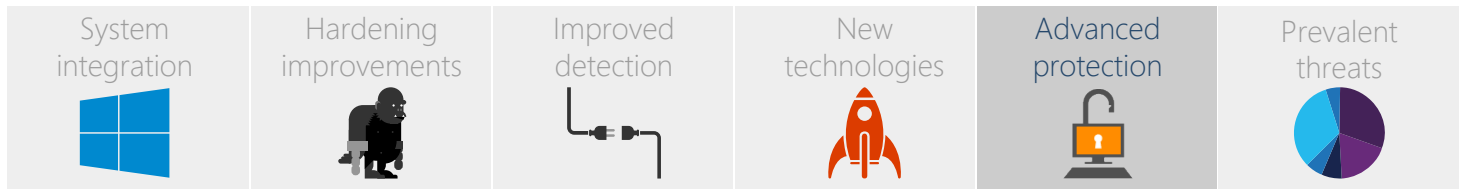
The interface supports a calling structure allowing for file and memory or stream scanning, content source URL/IP reputation checks, among other techniques. It also enables visibility for antimalware products into code that is often dynamically generated or retrieved at runtime.

AMSI also supports the notion of a session so that security products, such as Windows Defender, can correlate different scan requests. For instance, the different fragments of a malicious payload can be associated to reach a more informed decision, which would be much harder to reach just by looking at those fragments in isolation.

For more information on AMSI, see our blog [Windows 10 to offer application developers new malware defenses](#).



Malware Protection Center



Advanced protection

Cloud protection

Windows Defender began building a cloud protection capability with the release of Windows 8. In Windows 8, Microsoft introduced Windows Defender Cloud Protection for the first time (as the Microsoft Active Protection Service), a solution to better protect and react in the fast-evolving malware landscape.

Our goal with Windows Defender Cloud Protection is to block malware the “first time it’s seen” in the first critical hours of a malware attack.

Using a signature-driven approach, the device can query the Windows Defender Cloud (cloud protection is an optional feature, and can be toggled on or off in Windows 10 by going to (Settings > Update & security > Windows Defender > Cloud-based Protection) and see if it has a threat determination on suspicious resources. If it does not, a report and optional sample can also be sent to allow Microsoft researchers to analyze the sample to determine whether or not it should be blocked.

Windows Defender takes several steps to maintain your privacy when sending the report and you can see the privacy statement by going to (Settings > Update & security > Windows Defender > Cloud-based Protection).

In most cases, the execution of the resource will be held while the evaluation is undertaken. On average, the cloud query takes less than 0.5 seconds anywhere in the world. These checks can also be done asynchronously in lower risk circumstances.







Antimalware cleaning in the Windows Recovery Environment

Some threats are so pervasive and damaging that normal-level Windows GUI shell-based remediation can encounter problems.

In Windows 10, the Windows Recover Environment functions as a separate operating system from the main shell, and supports an integrated, updated offline cleaning tool called Window Defender Offline.

In the event that offline cleaning is required, after user consent is obtained, the machine automatically reboots into the Windows Recovery Environment, executes the offline tool, cleans the advanced malware and reboots the machine back to Windows 10. There is no other effort required by the user other than initiating the reboot.

Malware Protection Center

System integration 	Hardening improvements 	Improved detection 	New technologies 	Advanced protection 	Prevalent threats 
---	---	---	---	--	--

Top detections for the past 30 days

The tables in this section show top detections for all malware categories for the past 30 days.

“Distribution” is the percentage share of each detection amongst the top 10 detections in that category.







Enterprise detections	
Threat name	Distribution
BrowserModifier:Win32/CouponRuc	44%
BrowserModifier:Win32/KipodtoolsCby	11%
Win32/Gamarue	10%
SoftwareBundler:Win32/InstalleRex	8%
Win32/Jenxcus	7%
Trojan:Win32/Skeeyah.A!plock	7%
JS/Axpergle	5%
Trojan:Win32/Peals	5%
Win32/Conficker	2%
TrojanDownloader:W97M/Donoff	1%

Top detections (all types)	
Threat name	Distribution
BrowserModifier:Win32/CouponRuc	31%
HackTool:Win32/Keygen	15%
BrowserModifier:Win32/AlterbookSP	14%
HackTool:Win32/AutoKMS	8%
BrowserModifier:Win32/KipodToolsCby	8%
Adware:Win32/EoRezo	6%
BrowserModifier:Win32/EonarchSP	6%
SoftwareBundler:Win32/InstalleRex	5%
Worm:VBS/Jenxcus!lnk	4%
VirTool:Win32/Obfuscator.XZ	3%

Families	
Threat name	Distribution
BrowserModifier:Win32/CouponRuc	36%
HackTool:Win32/Keygen	18%
HackTool:Win32/AutoKMS	9%
BrowserModifier:Win32/KipodtoolsCby	9%
Win32/Gamarue	8%
Adware:Win32/EoRezo	7%
Win32/Obfuscator	7%
SoftwareBundler:Win32/InstalleRex	6%
Win32/Jenxcus	6%
Trojan:Win32/Skeeyah.A!plock	6%

Top rogue detections	
Threat name	Distribution
Rogue:JS/FakeCall.B	56%
Rogue:HTML/Phish.A	8%
Rogue:Win32/Winwebsec	8%
Rogue:Win32/FakeRean	7%
Rogue:VBS/Trapwot	7%
Rogue:Win32/FakePAV	5%
Rogue:VBS/FakePAV	3%
Rogue:Win32/Trapwot	3%
Rogue:Win32/FakeVimes	2%
Rogue:Win32/FakeCog	2%

Malware Protection Center

System integration 	Hardening improvements 	Improved detection 	New technologies 	Advanced protection 	Prevalent threats 
---	---	---	---	--	--






Top ransomware detections	
Threat name	Distribution
Ransom:HTML/Crowti.A	36%
Ransom:Win32/Crowti.A	19%
Ransom:Win32/Crowti	17%
Ransom:JS/Krypterade.A	8%
Ransom:Win32/Troldesh.A	5%
Ransom:Win32/Critroni.B	4%
Ransom:Win32/Critroni	4%
Ransom:HTML/Tescrypt.A	3%
Ransom:Win32/Nymaim.F	2%
Ransom:Win32/Reveton.V	2%

Top unwanted software detections	
Threat name	Distribution
BrowserModifier:Win32/CouponRuc	40%
BrowserModifier:Win32/AlterbookSP	18%
BrowserModifier:Win32/KipodToolsCby	10%
Adware:Win32/EoRezo	8%
BrowserModifier:Win32/EonarchSP	8%
SoftwareBundler:Win32/Install-eRex	7%
Adware:Win32/ZoomyLib	4%
BrowserModifier:Win32/MeninchSP	2%
BrowserModifier:Win32/TogiraSP	1%
BrowserModifier:Win32/Default-Tab	1%

Top exploit detections	
Threat name	Distribution
Exploit:HTML/Axpergle.O	29%
Exploit:Win32/CplLnk.A	15%
Exploit:JS/Neclu.AH	8%
Exploit:HTML/Axpergle.AB	7%
Exploit:HTML/Neclu.O	6%
Exploit:VBS/CVE-2014-6332	6%
Exploit:JS/Meadgive.S	6%
Exploit:Win32/Sdbby	5%
Exploit:HTML/IframeRef.gen	5%
Exploit:Win32/ShellCode.A	5%

Top password stealer detections	
Threat name	Distribution
PWS:Win32/Fareit	21%
PWS:Win32/Lmir.AAA	16%
PWS:Win32/Zbot	13%
PWS:Win32/Prast!rts	11%
PWS:Win32/VB.CU	10%
PWS:Win32/Zbot!rfn	8%
PWS:Win32/QQpass.CI	6%
PWS:Win32/Dyzap	6%
PWS:Win32/Dyzap.Q	5%
PWS:Win32/Mujormel.D	4%

Malware Protection Center

System integration 	Hardening improvements 	Improved detection 	New technologies 	Advanced protection 	Prevalent threats 
---	---	---	---	--	--

Top spyware detections	
Threat name	Distribution
TrojanSpy:Win32/Banker	38%
TrojanSpy:JS/Phish.D	11%
TrojanSpy:Win32/Bancos.AMM	10%
TrojanSpy:MSIL/Hakey.A	7%
TrojanSpy:Win32/Banker.AOE	7%
TrojanSpy:Win32/Ursnif	6%
TrojanSpy:Win32/Bancos	6%
TrojanSpy:MSIL/Omaneat.A	5%
TrojanSpy:MSIL/Golroted.B	5%
TrojanSpy:Win32/Mafod!rts	4%

Copyright

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2015 Microsoft. All rights reserved.

Please refer to [Microsoft Trademarks](#) for a list of trademarked products.

All other trademarks are property of their respective owners.