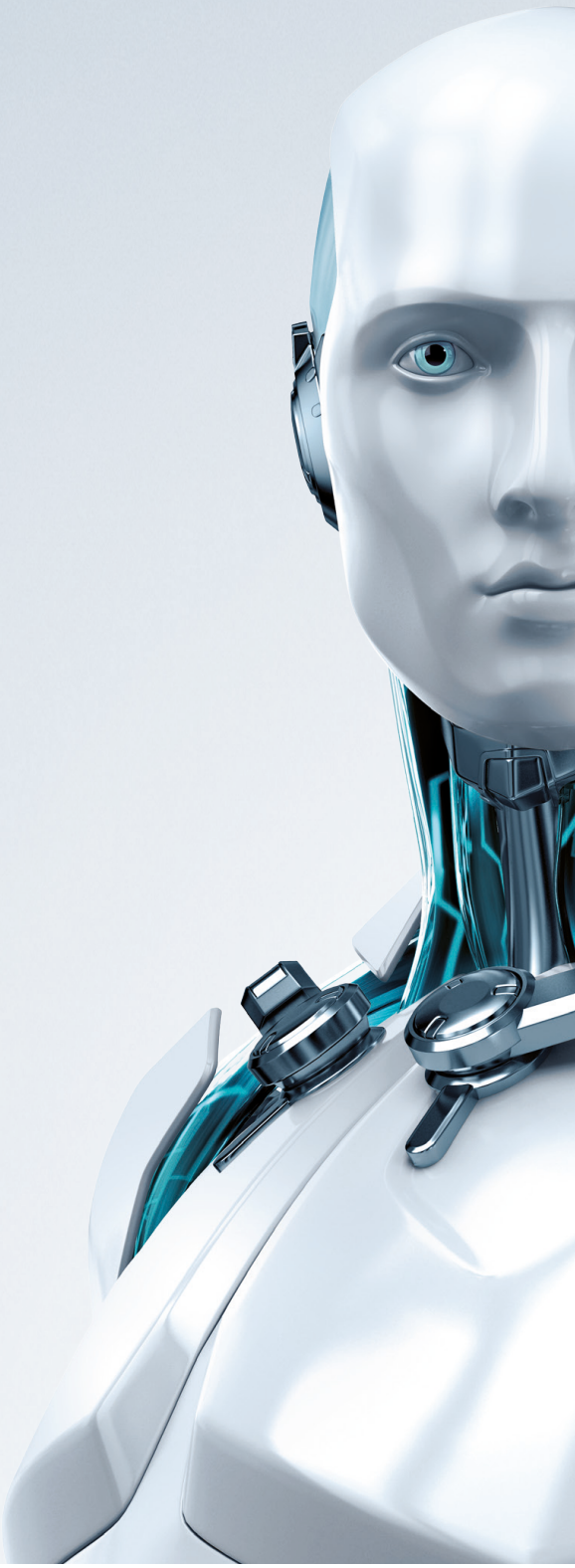
Microsoft Windows® 10 Security and Privacy

An ESET White Paper



ENJOY SAFER TECHNOLOGY™

Microsoft Windows® 10 Security and Privacy

An ESET White Paper

Version 1.0 - June, 2016

NOTE: Microsoft is continuously changing Windows 10 in order to improve its reliability, quality and security. As a result, the behavior of the operating system may, over time, diverge from that described in the original version of the white paper. While every attempt has been made to provide accurate descriptions of Windows 10 features (including screenshots), future changes made by Microsoft may make parts of this white paper out of date. Please check with ESET for the latest version of this white paper for the most accurate and up-to-date information on Windows 10.

Contents

Introduction

On July 29th, 2015, Microsoft released Microsoft Windows 10, a version of Windows that has been widely discussed and promoted as everything from "what Windows 8 should have been" to "the last version of Windows." It will certainly be the most secure version of Windows, ever. Windows 10 is the closest Microsoft has come to a virus-proof operating system so far, but the cost and complexity of implementing that level of security may be something that most of Microsoft's customers cannot afford.

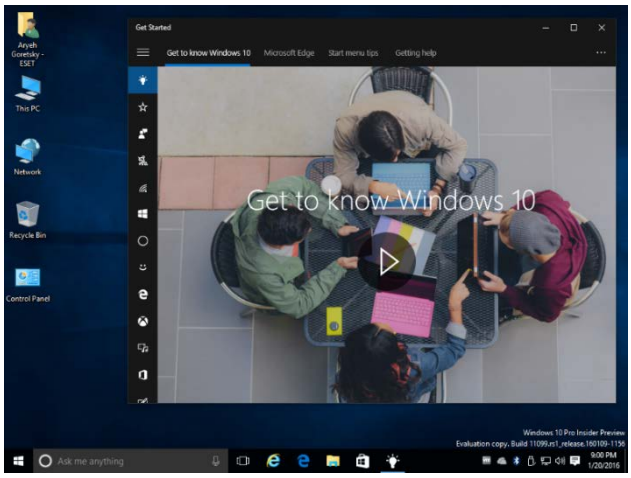


Figure 1: Getting started with a short introductory video.

Windows 10 incorporates the most ambitious changes seen between two versions of Windows since XP and Vista. Microsoft has found itself in an interesting position: Windows 8 was met with lukewarm adoption, taking three years to surpass Windows XP usage since its release in 2012. In businesses, Windows 7 continues to reign on the desktop. With Windows 10, Microsoft has to deliver a version of Windows that is not seen merely as a more-than-capable upgrade to Windows 7, but also a version of Windows that pleases those who have embraced Windows 8.

Windows 10 is the closest Microsoft has come to a virus-proof operating system so far, but the cost and complexity of implementing that level of security may be something that most of Microsoft's customers cannot afford.

Windows 10 is the first release of desktop Windows to introduce consumers to Microsoft's *Windows as a Service* (WaaS) licensing model.[1] Such arrangements have been common in the corporate world for years, where licensing allows enterprises automatic access to the latest versions of software. It is a new arrangement to consumers who are used to purchasing a computer with a license for one version of Windows and using it through, and sometimes well beyond, its support lifecycle.

With Windows 10, Microsoft plans to release new features and functionality throughout the 10-year lifecycle of the operating system, instead of releasing new versions to provide them. While this may not sound as ambitious as Windows 8's Start Screen, it is actually a far bigger and more fundamental change in how Windows is maintained by Microsoft.[2] The company's goal is to have one billion devices running Windows 10 by 2018, which requires a very different strategy than was previously used to get to that 10 digit number, but even that is something of a guesstimate, notes Ziff-Davis journalist Ed Bott:[3]

---

[1] Myerson, Terry. "The next generation of Windows: Windows 10." Published Jan. 21, 2015. Microsoft Blogging Windows. http://blogs.windows.com/bloggingwindows/2015/01/21/the-next-generation-of-windows-windows-10/.

[2] Microsoft. "Designed to be the most secure Windows yet." Windows for Business. https://www.microsoft.com/en-us/WindowsForBusiness/Windows-security.

[3] Bott, Ed. "Microsoft's big Windows 10 goal: one billion or bust." Published May 8, 2015. Ziff-Davis. http://www.zdnet.com/article/microsofts-big-windows-10-goal-one-billion-or-bust.

Execution is everything, of course, and putting that 10-digit number out there as a goal is actually defining the minimum acceptable standard of success. Let's check back in two years and see how it all worked out.

All for one, one for all?

Microsoft is consolidating its disparate operating system strategy, with Windows 10 coalescing its separate computer and smartphone operating systems into Windows 10 for PCs, Windows 10 Mobile for smartphones *and* tablets (those with screens under 7 inches in size, that is) and even an experimental version of Windows 10 for the Internet of Things scaled down to run on devices such as Raspberry Pi. [4, 5]

Having one operating system for several very different devices can make explaining security features a bit confusing, so in this paper I am using the term "PC" to denote a broad category which includes not just traditional desktop and notebook computers, but tablets like Microsoft's *Surface Pro* and Lenovo's *Helix* lines, all-in-one (AIO) computers, and similar devices that run desktop versions of Windows 10. Regardless of form-factor, all of these PCs have a 32-bit (x86) or a 64-bit (aka AMD64, EMT64T, x86-64 or simply x64) Intel- or AMD-compatible processor, running what we call the IA-32 instruction set.[6]

Here is a quick run-down on various editions of Windows 10 and their intended audiences:

Edition	Target Audience	Comment
Windows 10 Education	Education	Windows 10 Enterprise edition sold under Microsoft Academic Volume Licensing.
Windows 10 Enterprise	Business	Version of Windows 10 with management features. Replaces Windows 8.1 Enterprise.
Windows 10 Enterprise LTSB *(Long Term Servicing Branch)*	Business	Version of Windows 10 Enterprise that will not receive any new features, just security updates and bug fixes.
Windows 10 Home	Consumer	Version of Windows 10 for consumers. Replaces Core and Home editions from previous versions of Windows.
Windows 10 IoT Core	Developers	Version of Windows 10 for embedded systems.
Windows 10 Mobile	Consumer	Version of Windows 10 for smartphones and tablets with 7" or smaller screens. Replaces Windows Phone 8.1.
Windows 10 Mobile Enterprise	Business	Version of Windows 10 Mobile with management features.
Windows 10 Pro	Consumer	Version of Windows 10 for small businesses and power users. Replaces Pro, Business and Ultimate editions from previous versions of Windows.

[4] Dallas, Kevin. "Windows 10 IoT: Powering the Internet of Things." Published Mar. 18, 2015. Microsoft Blogging Windows. http://blogs.windows.com/bloggingwindows/2015/03/18/windows-10-iot-powering-the-internet-of-things/.

[5] Upton, Liz. "Windows 10 for IOT." Published Apr. 30, 2015. Raspberry Pi Foundation. https://www.raspberrypi.org/windows-10-for-iot/.

[6] Wikipedia. "IA-32." Published June 29, 2015. Wikimedia Foundation. https://en.wikipedia.org/wiki/IA-32.

In this white paper, we will be focusing primarily on the security features of Windows 10 for PCs that are impactful to home and business users. Windows 10 Mobile and Windows 10 IoT (Internet of Things) will be discussed where and when they are applicable. Windows Server 2016, the next server version of Microsoft Windows and still in beta, will be briefly mentioned as well. However, the focus of this white paper is on desktop/laptop versions of Microsoft Windows, not the smartphone, tablet or server versions.

Any new version of Windows is going to contain thousands of security improvements, and it is beyond the scope of this white paper to look into all of them.[7] We can, however, look at those features that are going to have the most impact on the security landscape.

Some security features of Windows 10, such as *Virtualization-Based Security* (VBS, formerly called *Virtual Secure Mode* during beta-testing), vary by which edition of Windows 10 is installed on the desktop, and these differences will be noted in this paper. Unless they are specifically mentioned, we will not be discussing the security of Windows 10 Mobile or Windows 10 IoT, as these non-desktop devices differ substantially in capabilities and use cases from Windows on the desktop.

For home users, Windows 10 Home and Windows 10 Pro will be the versions they typically use, while businesses will gravitate towards Windows 10 Pro or Windows 10 Enterprise. There are additional versions available with specific features for enterprises in regulated markets where change control must be managed, as well as for educational markets.

The fact that there were no major changes to hardware requirements for security between Windows 8/8.1 and Windows 10 is likely a boon to enterprise computer users, although perhaps not to computer manufacturers who used to rely on Windows upgrades to drive hardware sales.

The requirements for managing device integrity remain largely unchanged as far as Secure Boot goes: UEFI Version 2.3.1 Annex B (or newer), and TPM Version 1.2 (or newer) are required. Provable PC Health has been enhanced to work with Conditional Access, which functions similarly to NAP or NAQ.

For anti-malware developers, there are no major changes to Microsoft Early Launch Anti Malware (ELAM), just incremental updates. This should help speed development and interoperability of security software with Windows 10.[8, 9]

Since no discussion of the latest version of Microsoft Windows would be complete without mentioning previous versions of Windows, we'll start with a *very* brief recapitulation of which versions of Windows are still in use.

Windows Adoption by the Numbers

First, I want to share a look at which versions of Microsoft Windows were used by ESET's customers just prior to Windows 10's release. Here's what that looked like in July 2015, at the end of that month:

---

[7] Microsoft. "Platform Security." Developer Network. Published June 25, 2015. https://msdn.microsoft.com/en-us/library/dn756283.aspx.

[8] Microsoft. "Early Launch AntiMalware." Hardware Dev Center. https://msdn.microsoft.com/en-us/library/windows/hardware/dn265157%28v=vs.85%29.aspx.

[9] Microsoft. "Early launch antimalware." Windows Dev Center. https://msdn.microsoft.com/en-us/library/windows/desktop/hh848061%28v=vs.85%29.aspx.

As we can see, over 60% of computers were running Windows 7 as their desktop operating system, with about 18% running Windows 8.*x* or Windows XP, respectively. About 2% were still on Windows Vista. Just under 0.2% were running a preview build of Windows 10 (and likely testing version 9 of ESET's software, which was then in public beta test).

Curiously, a small fraction of a single percent were running Windows 2000 or NT 4.0 SP6a. While it is easy to think of these as belonging to the ultimate Windows die-hards, they are most likely to be servers managing automated systems, equipment or infrastructure that have not been replaced for economic reasons.

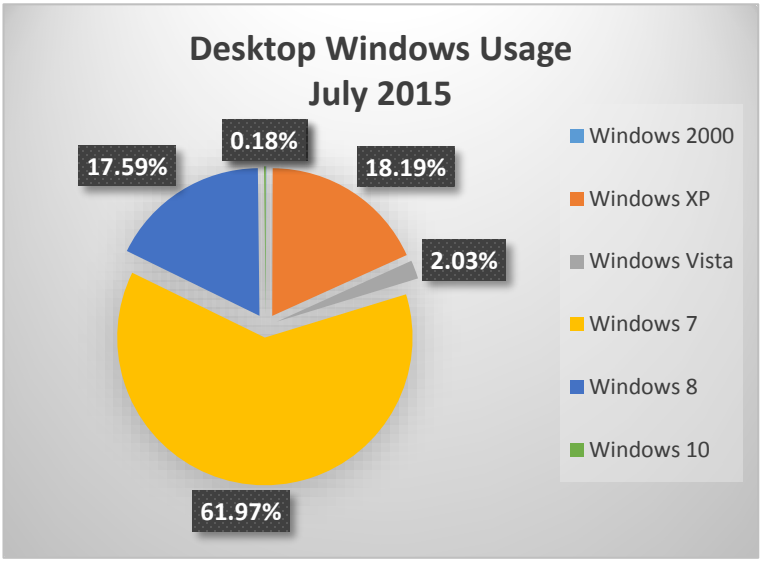


Figure 2: Source: ESET LiveGrid® data

Windows 8: The Security Story So Far

It has been over a year and a half since Microsoft released the last Windows 8.1 Update, the successor to 2014's Windows 8.1 and 2012's Windows 8. All of these versions of Windows have been treated largely with indifference or even scorn by the computing public, ignoring the addition of numerous security features and improvements.

We looked at these versions of Windows extensively when they arrived in ESET's blog, *We Live Security*:

Windows Version	Date	Blog Post	White Paper
Windows 8 RTM	August, 2012	*A white paper: Windows 8's Security Features*	Windows 8: FUD* for Thought [PDF, 356KB]
Windows 8 RTM (+ 6 months)	February, 2013	*Six Months with Windows 8 (white paper)*	Six Months with Windows 8 [PDF, 787KB]
Windows 8.1	August, 2013	*Windows 8.1 – Security Improvements (White Paper)*	Windows 8.1 Security: New and Improved [PDF, 456KB]

NOTE: *Windows 8.1 Update, released in April, 2014, contained no major differences in security over the 2013 release of Windows 8.1.*

Windows 8 was the first release of Microsoft's flagship desktop operating system to support Secure Boot and Early Launch Anti Malware (ELAM), while Windows 8.1 built on its predecessor's security by adding improvements to biometrics and Device Encryption as well as an updated version of Windows Defender.

Microsoft sought to bring Windows into the "modern era" with Windows 8, introducing the much-maligned Start Screen (replaced by a hybrid Start Menu in Windows 10); tighter integration with Microsoft OneDrive, Microsoft's Internet-based storage service; and a new application API for Windows Universal Apps (*née* Modern *née* Metro), which are similar to smartphone apps in terms of permissions and security.

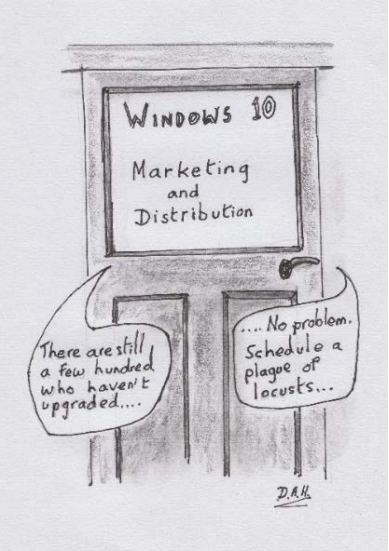
Microsoft's goal with Windows 10 has been not only to embrace and extend what worked well in Windows 8, but also to improve things so they work better in Windows 10, such as the new Windows Universal App platform. But Windows 10 is not just about changes and improvement: Windows 10 also adds new security features as well, such as Device Guard and Virtualization-Based Security mode.

With Windows 10, Microsoft seeks even greater integration with its Microsoft Azure-powered cloud, allowing users to move effortlessly between PCs, tablets and smartphones; a design choice that has enormous implications for the privacy and confidentiality of users' data.

What's Improved in Windows 10

Windows Update

Windows Update is certainly not a new feature of Microsoft Windows, having been introduced in 1995 with Windows 95. For the past two decades, Windows Update has served as the keystone of Microsoft's patching system for versions of Windows in order to keep them up to date. Windows Update provides a subset of offerings from Microsoft Update, which offers updates for Microsoft Office, .NET Framework, Windows Live, as well as occasionally offering programs to leverage adoption of Microsoft's other offerings, such as Skype and Bing.[10, 11]



Microsoft's aggressive pushing of Windows 10 has its critics. Credit: David Harley

Admittedly, some of these additions have been met by Microsoft's customers with varying degrees of interest. Still, Windows Update is primarily for delivering patches for the operating system—arguably the most important security feature in Windows—so it is important to take a look at how updates and upgrades have changed in Windows 10.

Updates to Windows 10 occur at each servicing point (formerly known as Patch Tuesdays) and do not contain any new features. Patches are cumulative in nature as well, so applying a patch to one file for an issue applies all the previous patches as well. This may also mean that the size of patches will increase over time (and then periodically decrease as upgrades containing the fully patched files are released).

Upgrades to Windows 10, on the other hand, will occur two to three times a year, depending on the branch. Upgrades may change the software development and device driver development models, meaning that software and device drivers may need to be recompiled to take advantage of these changes. Upgrades may also add new settings and features to the operating system, although given the youth of the operating system, it is difficult to speculate whether these will be more like the features added during Windows XP's lifetime (Windows Firewall, Bluetooth and USB 2.0 support, and

[10] Saberman. "Why Am I Being Offered An Update To Skype When I Don't Have It Installed?" Published Mar. 25, 2015. Microsoft Community. https://answers.microsoft.com/en-us/windows/forum/windows_7-windows_update/why-am-i-being-offered-an-update-to-skype-when-i/f12baa9d-8aa5-4398-8797-a43ef580ffd9.

[11] Jeltz. "Was Bing Desktop Mistakenly Put On Windows Update?" Published Apr. 26, 2012. Microsoft Community. https://answers.microsoft.com/en-us/windows/forum/windows_7-windows_update/was-bing-desktop-mistakenly-put-on-windows-update/da9717b1-4ead-4d75-b970-ca70c31689a9.

so forth) or more like Vista's Windows Ultimate Extras, which contained a couple of add-on utilities, but mostly consisted of games and multimedia add-ons.

For consumers running the Home and Pro editions, Windows 10 now obtains updates directly from Microsoft's `catalog.update.microsoft.com` servers in the cloud, bypassing the **Windows Update** application (filename: **WUAPP.EXE**) that had long been a staple of earlier versions of Windows. It is still possible to obtain Windows Updates via a command line, but the means to do so have changed considerably.[12, 13] Strangely, though, the front end for the Windows Update Catalog web site suggests users access it using Internet Explorer 6 from the Windows XP era circa 2001, and requires that an ActiveX control be installed, a feature deprecated in Microsoft's new Edge web browser.

For businesses, the Microsoft Update catalog also serves as the back-end repository for the Windows Server Update Service (WSUS), which allows central management of Microsoft patches to the computers on their domain.[14, 15] WSUS 4.0 is Microsoft's preferred tool for business customers to manage their Microsoft Updates, and will do so through Windows Update for Business (WUfB).

Windows Update for Business is not a discrete program like WSUS, but rather a set of Group Policy Objects (GPOs) to manage it. Using Windows Update for Business, system administrators can control how Windows Updates are deployed through the enterprise. For most branches of Windows 10, upgrades to new builds of Windows 10 can be deferred by system administrators for one to eight months, while updates to the existing installed builds can be deferred for one to four weeks. If there is a problem with the rollout of an upgrade or an update using Windows Update for Business, it can be paused, although the rollout will start again when the next set of updates or upgrades is released by Microsoft.[16, 17, 18, 19]

One of the reasons for all of these changes to how Windows is serviced is because updates to the existing build of Windows 10 and upgrades to new builds of Windows 10 will primarily be delivered through these mechanisms, although other Microsoft technologies such as System Center Configuration Manager (SCCM) and third-party mobile device management (MDM) solutions will

---

[12] Parker, Steven. "PSA: How to open specific Settings directly I Windows 10 from the Run command." Published Jun. 2, 2015. Neowin. http://www.neowin.net/news/psa-how-to-open-specific-settings-directly-in-windows-10-from-the-run-command.

[13] Wilson, Ed. "Use a PowerShell Module to Run Windows Update." Published Nov. 8, 2012. Microsoft Hey, Scripting Guy! Blog. http://blogs.technet.com/b/heyscriptingguy/archive/2012/11/08/use-a-powershell-module-to-run-windows-update.aspx.

[14] Microsoft. "Windows Server Update Services." Microsoft TechNet. https://technet.microsoft.com/en-us/windowsserver/bb332157.aspx.

[15] Wikipedia. "Windows Server Update Services." Published Jun. 16, 2015. Wikimedia Foundation. https://en.wikipedia.org/wiki/Windows_Server_Update_Services.

[16] Myerson, Terry. "Announcing Windows Update for Business." Published May 4, 2015. Microsoft Windows Experience Blog. https://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/.

[17] Microsoft. "Windows Update for Business." Published Nov. 19, 2015. Microsoft TechNet. https://technet.microsoft.com/en-us/library/mt622730%28v=vs.85%29.aspx.

[18] Samir, Hammoudi. "Windows Update for Business Explained." Published Nov. 15, 2015. Microsoft BeAnExpert blog. http://blogs.msdn.com/b/beanexpert/archive/2015/11/16/windows-update-for-business-explained.aspx.

[19] Trent, Rod. "GPS Settings for Windows Update for Business." Published Nov. 16, 2015. Windows IT Pro. http://windowsitpro.com/windows-10/gpo-settings-windows-update-business.

continue to be supported. Reducing the number of mechanisms through which Windows 10 is deployed should ultimately simplify maintenance for Microsoft customers. However, there may be incremental costs to businesses that need to change existing operating system deployment mechanisms, or implement one if they have never had any such mechanisms in place.

These incremental features provide granular controls for businesses to manage Windows 10 on their computers, which makes the changes that Microsoft has made to enforcing Windows 10 updates for home users a surprising form of "tough love."

Are updates Windows 10's new Achilles Heel?

In some editions of Windows 10, users will be able to defer non-security upgrades for a specific length of time, although security upgrades will continue to be installed without user intervention. Microsoft states the following about this deferment:

> *Some Windows 10 editions let you defer upgrades to your PC. When you defer upgrades, new Windows features won't be downloaded or installed for several months. Deferring upgrades doesn't affect security updates. Note that deferring upgrades will prevent you from getting the latest Windows features as soon as they're available*.[20]

Computers running the Home Edition of Windows 10 will receive and install updates from Microsoft as they are released. Computers running the Pro Edition of Windows 10 will have a limited ability to defer most updates by one week. Note that this does not block non-security updates from being installed; it only postpones their download and eventual installation.

Microsoft's decision to limit the ability of its home customers to block updates has been greeted with mixed responses. Some power users decry the lack of control and losing the choice to determine what updates are installed on their computers, while IT and security personnel welcome it.

The reason for this dramatic change in policy about Windows updates for home users is simple: Home PCs would sometimes have their Windows update functionality disabled or certain updates blocked because the user thought that the updates would cause crashes, problems with third-party programs, or slow the computer down. In some cases, users disabled updates because they had pirated Windows and were concerned that installing updates would disable their copies of Windows. Of course, sometimes this was not intentional user behavior: Sometimes it was malware that disabled updates on Windows, too, as a mechanism to protect itself from being detected and removed.

For a long time, Microsoft has been fighting the problem of compromised Windows computers being used as attack platforms. In Windows 8, Microsoft first made it a requirement that working anti-malware software be running on Windows at all times, because in many investigations, it turned out that affected computers either were not running anti-malware software, or were running anti-malware software that had expired and was no longer receiving updates.

By requiring anti-malware software to be active and keeping Windows 10 components up to date, Microsoft believes it can make Windows 10 less of a springboard for attacks on other computers than previous generations of Windows.

Even the ability to defer updates in Windows 10 has limits: Security-related updates, such as virus signature database updates for Windows Defender, can never be deferred. A small concession,

---

[20] Microsoft. "Defer upgrades in Windows 10." Microsoft Windows. http://windows.microsoft.com/en-us/windows-10/defer-upgrades-in-windows-10.

introduced after Windows 10 launched, is that Universal Windows Apps (the successor to Windows 8's Modern apps) will not be automatically updated when Windows 10 downloads operating system updates.

One criticism of the policy of forcing updates and upgrades onto consumers before businesses is that it gives the appearance that home users are now involuntary, non-compensated beta testers for Windows 10. Is this good or bad for Microsoft's customers running Windows 10? That is a question which is much harder to answer.

In an article in Forbes.Com's Tech column published about a month before Windows 10's release, contributor Gordon Kelly does not mince words concerning Microsoft's new practice of giving early, less well-tested code to consumers.[21] In the article, Kelly, states:

> *Windows 10 turns us all into guinea pigs…*

This is debatable, given that updates for Windows 10 will have gone through internal testing by Microsoft, but even Microsoft acknowledges a difference in the level of quality of its updates for this "consumer-first" approach, stating it will take several months before updates deployed to consumers have enough "increased assurance of validation" that they can be deployed to business customers.[22]

Conversely, by **not** releasing Windows Updates at the same time to business users, Microsoft may be exposing those customers to increased risk. While this may seem contrary to what one should expect from security patches, there are solid reasons behind this: As soon as Windows Updates are released, attackers begin reverse-engineering to see what changed in the operating system files. By comparing the differences between patched and unpatched Windows' operating system files, attackers can identify what vulnerabilities were fixed by the update. Using this information, attackers then create code that exploits these vulnerabilities. While the home users who first received the security updates might be protected against these attacks, business users may have to wait weeks or months before the security updates are provided to them, meaning their Windows 10 computers will have a larger window of vulnerability than consumer computers.

The size of that window of vulnerability is hard to determine, since Windows 10 is just being introduced to the enterprise. It will be some time before we can quantify the exact impact that delaying updates will have on business users. Readers who want to know more about this issue should read the white paper *Windows 10 patching process may leave enterprises vulnerable to zero-day attacks*, published in Virus Bulletin.[23]

There is only one edition of Windows 10 whose update branch allows updates to be postponed indefinitely and even prevents new features from being added: Windows 10 Enterprise LTSB (Long Term Servicing Branch). This edition of Windows 10 is available only to enterprises that have signed up for Microsoft's volume licensing program or have other custom licensing agreements in place, and will not be sold to consumers as a boxed product or preloaded on computers purchased from resellers.

---

[21] Kelly, Gordon. "Windows 10 Upgrades Cannot Be Stopped." Published Jun. 26, 2015. Forbes.Com. http://www.forbes.com/sites/gordonkelly/2015/06/26/free-windows-10-upgrades-danger/.

[22] Alkove, Jim. "Windows 10 for Enterprise: More secure and up to date." Published Jan. 30, 2015. Microsoft Windows for Your Business Blog. http://blogs.windows.com/business/2015/01/30/windows-10-for-enterprise-more-secure-and-up-to-date/.

[23] Goretsky, Aryeh. "Windows 10 patching process may leave enterprises vulnerable to zero-day attacks." Published Mar. 12, 2015. Virus Bulletin. https://www.virusbtn.com/blog/2015/03_12.xml.

Windows Branches

The concept of branches is a new one for Windows desktop operating systems. Simply put, a branch is the name given to a specific release cycle of builds for Windows 10 and determines when a computer will receive that particular version of the operating system. The different branches of Windows 10 vary by how much testing they have received, both internally by Microsoft and externally through beta testers and even from deployments to home PCs.

For consumers who buy Windows 10 pre-loaded onto computers (or have taken advantage of Microsoft's offer to upgrade from earlier versions of Windows for free) only one release branch is readily available, called the Current Branch (CB). More adventurous consumers can sign up for access to Microsoft's Windows Insider Program (WIP) branch, which allows them, along with software developers, QA engineers, and IT professionals, to look at the newest builds of Windows 10 with the latest features — and bugs.

Business and organizational customers, on the other hand, have two additional branches from which to choose, as discussed later.

While having different release schedules for operating system upgrades may be new to Windows, this has been an established practice for other operating systems, such as Linux, for a while. Some hardware vendors and software developers have used similar scheduling, to denote to customers the difference between "bleeding edge" and "well-tested" code.

Various distributions of Linux often have two or more branches available, one of which is the "final," "general distribution," "production release" or "stable" branch for production, and one or more other branches labeled "beta," "daily," "experimental," "test," "unstable" or something similar to indicate it is not ready for use in a production environment.

Microsoft has **four** branches of Windows 10 (at the time of publication). The following chart identifies the four branches and briefly explains the editions they apply to, and why customers might choose them.

Branch Name	Available For	Updates Provided	Delivery Schedule & Release Mechanism
Windows Insider Program (WIP) *	Education, Enterprise, Home and Pro Editions	Experimental, bleeding edge features. Critical security and stability updates as well as feature upgrades are provided immediately as they become available. Extensive telemetry collected.	Released ~4-6 months after internal testing. Deployed via Windows Update.
Current Branch for Consumers (CB)	Education, Enterprise, Home and Pro Editions	Critical security and stability updates as well as feature upgrades are provided after they have passed Preview Branch testing.	Released ~4 months after WIP Branch. Deployed via Windows Update.
Current Branch for Businesses (CBB)	Education, Enterprise and Pro Editions	Critical security and stability updates are provided after they have passed Preview Branch testing. Feature upgrades can be deferred for up to 12 months.	Released ~4 months after CB Branch. Deployed via Windows Update, WSUS and WUfB.
Long Term Servicing Branch (LTSB)	Enterprise Edition	Critical security and stability updates can be deferred forever. New features cannot be added except by installing a new build of Windows 10.	Release schedule TBD. Deployed via WSUS and WUfB.

**WIP is a preview branch only available to those who sign up for Microsoft's Windows Insiders beta test program.*

Even ESET is not immune to the concept of branches. For several years now, ESET has been offering users a choice between receiving two types of releases to its software: "pre-release updates" which have passed through internal testing but not been widely-deployed yet, and "regular updates" which are thoroughly tested and vetted.[24] By using this method of updating, ESET's customers can obtain the latest "pre-release" malware and threat detection signature updates, modules, and sometimes new features to evaluate on a subset of computers. At the same time, "regular" updates which provide well-tested protection can be deployed on the majority of their systems. If needed, updates can even be paused or rolled-back to an earlier version.[25, 26]

While this approach works well for something as complex as security software, an operating system is still orders of magnitude more complex, which explains why Microsoft has a multitude of separate branches for denote the status of releases. For Microsoft, these act largely as schedules for when a particular build of Windows 10 will be available to a customer on that particular branch.

It should be noted that Windows 10 Mobile as well as Windows 10 IoT Core will likely be released on schedules different from the branches for desktop versions of Windows 10 due to both technical and market reasons.

Windows Defender

Windows Defender was originally released by Microsoft in 2005 as an anti-spyware program, the result of one of its many acquisitions in the security space. For seven years it functioned as Microsoft's free anti-spyware program, available for download from Microsoft's web site and sometimes bundled with Windows. For Windows 8, Microsoft made a significant change: In 2012, Microsoft took its *Microsoft Security Essentials* program, which detects all types of malware and not just spyware, rebadged it as *Windows Defender*, and bundled it into Windows 8. Microsoft has continued this practice of bundling *Windows Defender* with all subsequent releases of desktop versions of Windows.

Microsoft considers running anti-malware software important enough that *Windows Defender* cannot be uninstalled from Windows 10. Installing a third-party anti-malware program **disables** *Windows Defender*; however, it still remains present and will continue to download updates. As noted above, these database updates fall under the heading of Windows 10's security updates, and cannot be blocked.

The reason Windows 10 keeps *Windows Defender* up-to-date is simple: When a third-party anti-malware program's license expires, it will be disabled **immediately** by Windows 10 and *Windows Defender* will be automatically switched on to protect the system. This is slightly different behavior than in previous versions of Windows. In previous versions, *Windows Defender* could be installed or uninstalled, and there was a grace period of a few days between an anti-malware program's license expiring and *Windows Defender* taking over from it. This new approach ensures there is no gap in coverage. A system will never be unprotected, nor protected only by increasingly obsolete malware definitions.

---

[24] ESET. "How do I enable or disable pre-release updates in my ESET product?" Published Jul. 7, 2015. ESET Knowledgebase. http://support.eset.com/kb3415/.
[25] ESET. "How do I roll back virus signature database updates in ESET Smart Security/ESET NOD32 Antivirus?" Published Nov. 20, 2015. ESET Knowledgebase. http://support.eset.com/kb3351.
[26] ESET. "How to I roll back virus signature database updates on ESET business products? (6.x)" Published Apr. 13, 2016. ESET Knowledgebase. http://support.eset.com/kb3676/.

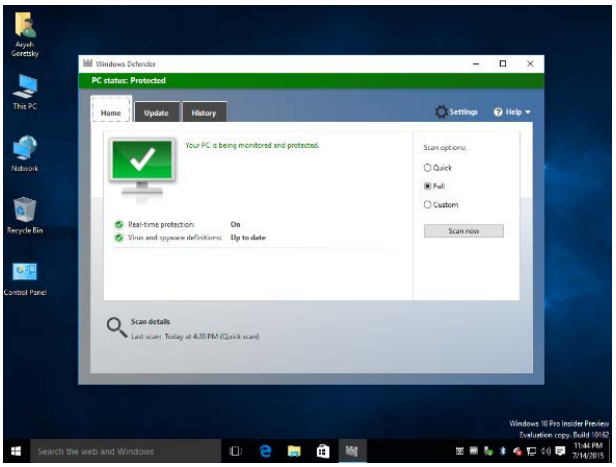


Figure 3: Windows Defender's home screen remains largely unchanged under Windows 10.

While the user interface for the Windows 10 version of *Windows Defender* remains largely unchanged from its predecessor (and, indeed, shared the same version number—4.8—as the version for older editions of Windows), it is worth noting that there are some subtle differences.

For example, the *Settings* tab has been removed and replaced with a single *Settings* button to the right of the other tabs. Selecting this opens the Settings app, Windows 10's replacement for the Control Panel, for accessing *Windows Defender*'s options. From here, the program's options can be toggled on and off, as well as viewing version information for *Windows Defender*'s various components.

As with all anti-malware programs, though, the user interface only constitutes a small portion of the actual program, and *Windows Defender* is no exception to this rule.

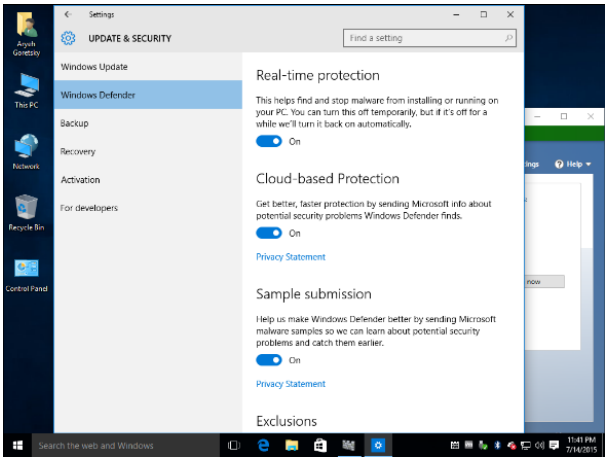


Figure 4: Once you drill down into Windows Defender's settings, the changes become more apparent.

Most of the changes in *Windows Defender* for Windows 10 are "under the hood", having no user interface. There are several new "invisible features" in the Windows 10 release:

- More sensitive scanning of files based on the location from which they are downloaded or run. For example, files downloaded from the Internet or run from USB flash drives will be subject to more thorough scanning. While this will slightly increase the chance of a false positive, it is better to have false positives on files that are newly-introduced to a computer, rather than on those that have been installed on a computer for some time. However, Microsoft will use its cloud-based scanning back-end to help reduce the risk of false positives on these scans.

  Interestingly enough, these have been staples of ESET's software since at least 2005 when I joined the company, and I suspect competitors have similar features in their programs. Although the functionality was never prominently mentioned in any ESET literature, questions about it sometimes appeared on ESET's support web forum.[27, 28]

- Detection of file-less malware in memory. There are some forms of malware that do not write any files to the file system, but instead work by executing themselves entirely in memory without ever

[27] Marcos. "ThreatSense.NET question." Published May 21, 2005. Wilders Security Forum. http://www.wilderssecurity.com/threads/threatsense-net-question.81126/.

[28] Marcos. "Extra heuristics for web access protection?" Published Nov. 23, 2008. Wilders Security Forum. http://www.wilderssecurity.com/threads/extra-heuristics-for-web-access-protection.226058/#post-1354214.

writing themselves to a file. While this is not a new technique, as anyone who had to deal with the `SQL/Slammer` or `CodeRed` worms will confirm, it is once again being used by malware authors. One recent example of this is `Win32/Poweliks`[29], a family of malware that maintains persistence on Windows by encrypting its code and writing that into the system registry, from which it will be restored and launched each time the system is booted. Malicious scripts are another example: When written using Microsoft's PowerShell scripting language, they can be executed directly from memory without being written to disk.

Again, as with download-context-sensitive scanning, this is not a brand new technology. Scanning for in-memory, diskless threats has been a staple of third-party anti-malware software for several years.[30, 31]

- A new version of *Windows Defender Offline* will be made available that boots the existing operating system in an offline mode for cleaning. This will require a much smaller download than the current version of *Windows Defender Offline*.

Windows Defender continues to use the *Microsoft Malware Protection Engine* (MMPE), the same anti-malware engine and signatures used by Microsoft's other anti-malware offerings, such as *System Center Endpoint Protection* (SCEP), *Microsoft Security Essentials* (MSE) and the *Malicious Software Removal Tool* (MSRT).[32] By reusing the same engine and signatures, Microsoft can quickly develop multiple anti-malware solutions without having to create a new product each time that would require separate service and support infrastructures.

In both Windows 10 and Windows Server 2016, the underlying *Microsoft Malware Protection Engine* used by both the free version of *Windows Defender* and Microsoft's commercial offering, *System Center Endpoint Protection*, will be fully unified. The only different components will be the management and user interface portions. A computer running *Windows Defender* can be upgraded to *System Center Endpoint Protection* simply by purchasing appropriate licensing and then pushing out a small software package to deploy the missing components to the computer, instead of completely replacing *Windows Defender*.

Windows Defender in the enterprise?

Windows Defender is bundled with Windows 10, just as it was with Windows 8 and 8.1. While Microsoft has been bundling its anti-malware offerings with desktop versions of Windows for several releases (and years) now, until Windows Server 2012 was released it shied away from bundling anti-malware software with the server versions of Windows.

System administrators and IT professionals and others looking at technical previews of Windows Server 2016 coming from a Windows Server 2008 R2 environment might be surprised to find *Windows Defender* is installed.

---

[29] ESET. "Win32/Poweliks." Published Apr. 3, 2014. ESET Threat Encyclopedia. http://www.virusradar.com/en/Win32_Poweliks.A/description.

[30] ESET. "What's new in ESET Smart Security 7 and ESET NOD32 Antivirus 7?" Published Nov. 20, 2015. ESET Knowledgebase. http://support.eset.com/kb3343/.

[31] ESET. "ESET Technology: Advanced Memory Scanner." ESET, spol. s r.o. http://www.eset.com/int/about/technology/#advanced-memory-scanner.

[32] Microsoft. "Microsoft Malware Protection Engine deployment information." Microsoft Knowledgebase. https://support.microsoft.com/en-us/kb/2510781.

This represents a growing shift in how Microsoft views server security: Up until a few years ago, Microsoft did not bundle any anti-malware software on its servers, instead emphasizing authentication, access control, least-privilege principles, and software restriction policies for security. While this is not incorrect, anti-malware was largely viewed as a separate piece, with customers having to obtain separate licenses for System Center Endpoint Protection (formerly Forefront Endpoint Protection) if they wanted a manageable Microsoft solution.[33]

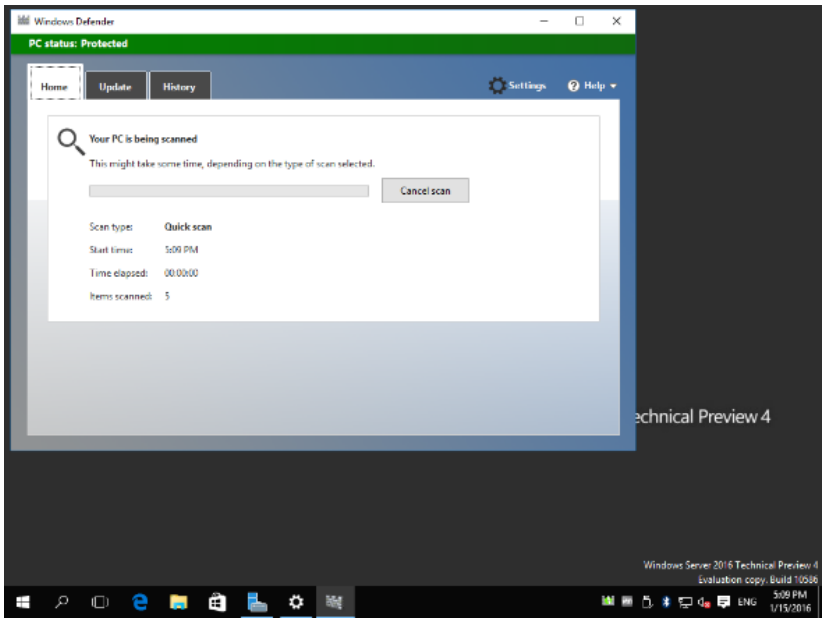


Figure 5: Windows Defender on Windows Server 2016 Technical Preview 4

There are several probable reasons for the lack of a managed anti-malware client in previous Windows Server versions: One might be concern over cannibalizing sales of Microsoft's commercial offering in this space. Another might be due to worries about how third-party anti-malware developers might respond to such a program being bundled.

In both Windows 10 and Windows Server 2016, *Windows Defender* will now be manageable through several interfaces, including OMA Device Management, PowerShell, WMI v2, Group Policy and the command line interface.[34, 35] These interfaces will allow for the centralized collection of **`EventID`** information (telemetry) that can then be used by the enterprise for home-grown management and reporting solutions.

Defending Windows Defender

Microsoft has been criticized by independent third-party testers for several years now over the protection level offered by its anti-malware products. The company has responded by explaining that their goal had always been to provide a baseline level of protection and that adding detection for new malware was prioritized by the telemetry they collect from computers running Windows.[36, 37] With

---

[33] Hornbeck. J.C. "More information on Microsoft antimalware protection on Windows 8 and Windows Server 2012." Published Nov. 5, 2012. Microsoft Endpoint Protection Team Blog. http://blogs.technet.com/b/clientsecurity/archive/2012/11/05/more-information-on-microsoft-antimalware-protection-on-windows-8-and-windows-server-2012.aspx.

[34] Open Mobile Alliance. "Device Management." Open Mobile Alliance Ltd. http://openmobilealliance.org/about-oma/work-program/device-management/.

[35] Microsoft. "Windows Management Infrastructure." Microsoft Developer Networks. https://msdn.microsoft.com/en-us/library/jj152383%28v=vs.85%29.aspx.

[36] Gandhe, Shreyas. "Microsoft: Security Essentials provides 'baseline' protection." Published Sep. 26, 2013. Neowin. http://www.neowin.net/news/microsoft-security-essentials-provides-baseline-protection.

[37] Samson, Ted. "Microsoft admits Security Essentials offers bare-bones protection by design." Published Sep. 30, 2013. Infoworld. http://www.infoworld.com/article/2612376/microsoft-windows/microsoft-admits-security-essentials-offers-bare-bones-protection-by-design.html.

around 850 million computers reporting telemetry to Microsoft every month through various conduits, this sounds like a reasonable idea for prioritizing malware detection. However, prevalence alone should not be the sole mechanism for prioritization, as volume alone does not tell you anything about the severity of malware or its potential for damage or data loss.

This lack of top results in third-party tests in spite of the large volume of telemetry collected has left many to speculate that *Windows Defender* has been on a kind of institutional life support for several years. Microsoft continued to fix bugs and keep signatures up to date, but otherwise not investing the resources that would allow *Windows Defender* to distinguish itself.

With *Windows Defender* for Windows 10 (and Windows Server 2016), Microsoft claims it will be increasing resources. It may take some time for these changes to show up in *Windows* Defender, but if new features appear in its rather Spartan interface, and more researchers are added to the Microsoft Malware Protection Center for analyzing malware and writing definitions, *Windows Defender* could go from being the baseline by which other anti-malware programs are judged to a contender in the anti-malware space.

However, moving up in third-party tests and comparatives is only a small part of the equation: Microsoft will need to do more than just demonstrate to customers that it's going to keep staffing levels up and provide resources to *Windows Defender*'s continued development. Microsoft is going to have to overcome its own track record as well to prevent further brand erosion.

BitLocker

Device Encryption, the unmanaged version of Microsoft's full-disk encryption software BitLocker, will be turned on by default on modern devices, the same as it was in Windows 8.1. In this context, a "modern device" means one with UEFI firmware, instead of firmware based on the now-deprecated BIOS standard.[38, 39, 40, 41] A Trusted Platform Module Version 1.2 (or 2.0) chip is also required inside modern devices.[42, 43] Almost all new PCs, smartphones and tablets ship with UEFI firmware and TPM v2.0 chips, so full-disk encryption managed by BitLocker or unmanaged Device Encryption will be available to businesses and consumers who wish to use this feature. For more information about the advantages and disadvantages of using Microsoft's full-disk encryption, see the previous ESET white paper, *Windows 8.1 Security – New and Improved*.[44]

---

[38] Wilkins, Richard and Richardson, Brian. "UEFI Secure Boot in Modern Computer Security Solutions." Published Sept. 2013. UEFI Forum. http://www.uefi.org/sites/default/files/resources/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf.

[39] Wikipedia. "United Extensible Firmware interface." Published Sept. 15, 2015. Wikimedia Foundation. https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface.

[40] Microsoft. "What is UEFI?" Microsoft Windows 8.1 How-to. http://windows.microsoft.com/en-us/windows-8/what-uefi.

[41] Wikipedia. "Unified Extensible Firmware Interface." Wikimedia Foundation. Published Feb. 2, 2016

[42] Trusted Computing Group. "TPM 2.0 Library Specification." Published Oct. 2014. Trusted Computing Group. http://www.trustedcomputinggroup.org/resources/tpm_library_specification.

[43] Wikipedia. "Trusted Platform Module." Published Sept. 1, 2015. Wikimedia Foundation. https://en.wikipedia.org/wiki/Trusted_Platform_Module.

[44] Goretsky, Aryeh. "Windows 8.1 – Security Improvements." Published Nov. 17, 2013. ESET We Live Security Blog. http://www.welivesecurity.com/2013/11/17/windows-8-1-security-improvements/.

Still, full-disk encryption remains largely an enterprise feature, and the changes incorporated into BitLocker in Windows 10 reflect this:[45]

- Support for managing Device Encryption is now available in Azure Active Directory domains. As Azure Active Directory is a key component of Microsoft's cloud and Windows as a Service aspirations; this is a welcome, if not unsurprising development.

- There are new policies to block access to computer ports that use Direct Memory Access (DMA), such as IEEE-1394 (more popularly known as FireWire) and ExpressCard interfaces to transfer data while Windows is booting. This is to prevent attacks that could allow the BitLocker passphrase to be recovered from memory, although the same technique could also be used to inject malware into a computer's memory. [46, 47]

  Attacks on DMA interfaces have been known for over 10 years, but they require attackers to connect their computers to the targets, limiting widespread use. Up until now, Microsoft's advice has been to recommend that enterprises disable interfaces that use DMA on computers with BitLocker that are vulnerable to attack, such as executives' laptops, and this has worked well, especially since computers with built in FireWire and ExpressCard interfaces have exited the market. [48] That said, increased concerns over determined adversaries conducting sophisticated attacks ranging from industrial espionage to nation-state surveillance, coupled with increasing interest from consumers in computers equipped solely with DMA-based Thunderbolt ports for data and power, Microsoft needs a more granular approach than telling users to "just switch it off." [49]

  Readers who want to know more about DMA attacks should read the article *Where there's smoke, there's FireWire* published on We Live Security.[50]

- In Build 10586 (also known as the Threshold, TH1, or v1511 release) of Windows 10, Microsoft added a new encryption algorithm XTS-AES to BitLocker that is intended to increase protection against attacks on plaintext.[51] Support for the existing AES-CBC is being maintained for sharing removable media with older versions of Windows.

---

[45] Microsoft. "What's new in BitLocker?" Published Nov. 12, 2015. Microsoft TechNet. https://technet.microsoft.com/en-us/library/mt403325%28v=vs.85%29.aspx.

[46] IEEE-1394 Working Group. "1394 WG – High Performance Serial bus Working Group." IEEE. http://standards.ieee.org/develop/wg/1394_WG.html.

[47] USB-IF. "About ExpressCard® Technology." USB Implementers Forum. http://www.usb.org/developers/expresscard.

[48] Microsoft. "Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker." Published Jun. 21, 2014. Microsoft TechNet. https://technet.microsoft.com/en-us/library/mt403325%28v=vs.85%29.aspx.

[49] Intel. "What is Thunderbolt™ 3 Technology?" http://www.intel.com/content/www/us/en/io/thunderbolt/thunderbolt-technology-consumer.html

[50] Goretsky, Aryeh. "Where there's smoke, there's FireWire." Published Jul. 28, 2011. ESET We Live Security Blog. http://www.welivesecurity.com/2011/07/28/where-theres-smoke-theres-firewire/.

[51] Dworkin, Morris. "Recommendation for Block Cipher modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices." Published Jan. 2010. National Institute of Standards and Technology, U.S. Department of Commerce. http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf.

Additionally, new Group Policy settings for BitLocker to manage these settings, as well as pre-boot messaging, have been introduced as well.

SmartScreen Filter

Originally developed to protect against phishing and malware in Internet Explorer under Windows 7, SmartScreen's reputational analysis system has been extended over the years to protect and collect threat data from Microsoft's various web properties such as Hotmail.Com, Outlook.Com, Office 365, and Bing. More recently, it was integrated into Windows 8 to check programs when run.

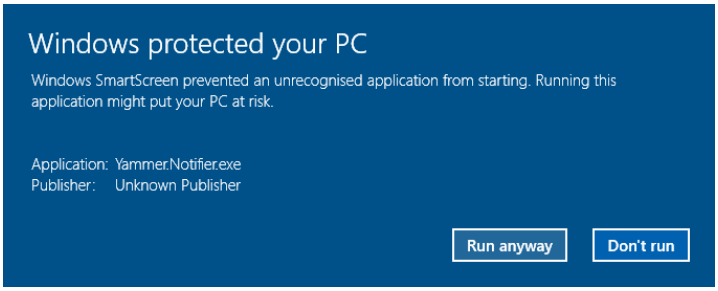


Figure 6: Windows SmartScreen filter in action. Credit: Noel Burgess

In Windows 10, support for SmartScreen has been added to Microsoft Edge as well.[52, 53] Beginning on January 1, 2016, SmartScreen automatically reports digitally signed files with weak certificate technology, such as SHA-1 hashes, when *downloaded* under supported versions of Windows (Windows Vista or higher) or *run* (Windows 8 and higher).[54] Whenever a file with a weak certificate is run under Windows 10, SmartScreen warns the user via the dialog shown in figure 6.

As in previous editions of Windows and web browsers, the SmartScreen Filter can be disabled, although doing so removes a layer of protection from the computer.

What's New in Windows 10

Conditional Access

Conditional Access is the replacement for Network Access Protection (NAP), Microsoft's version of network access control technology for limiting a computer's access to a network until it is proven to be safe enough to access all of the network's resources.[55,56] This was accomplished in NAP by creating a "ticket" with the computer's health state that was reported to a specialized service on the network called an enforcement point. In this context, "system health" meant having the latest operating system updates installed, up-to-date signatures for the anti-malware software, and having a software-based firewall enabled. Computers failing the health check would be blocked from accessing the network, or put into a "walled garden" network only allowing access to Windows and anti-malware updates.

---

[52] Microsoft. "SmartScreen Filter: FAQ." Windows How-to. http://windows.microsoft.com/en-us/internet-explorer/use-smartscreen-filter.

[53] Microsoft. "SmartScreen Filter: Frequently Asked Questions." Microsoft SmartScreen Feedback. https://feedback.smartscreen.microsoft.com/smartscreenfaq.aspx.

[54] Microsoft. "Microsoft Security Advisory 2880823: Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program." Published Nov. 12, 2013. Microsoft Security TechCenter. https://technet.microsoft.com/en-us/library/security/2880823.aspx.

[55] Microsoft. "Network Access Protection (NAP)." Published Aug. 23, 2009. Microsoft NAP Blog. http://blogs.technet.com/b/nap/.

[56] Wikipedia. "Network Access Control." Published Dec. 21, 2015. Wikimedia Foundation. https://en.wikipedia.org/wiki/Network_Access_Control.

Introduced with Windows Vista and Windows Server 2008, the technology was never broadly standardized or supported across vendors and received its last major update for Windows 7. NAP was deprecated in Windows Server 2012 R2 and not included in Windows 10 or Windows Server 2016.[57]

With Conditional Access, Microsoft is taking a slightly different approach, refocusing the effort as a way for businesses to manage their Bring Your Own Device (BYOD) policies.[58, 59, 60] Like its predecessor, it will consist of a health attestation. Unlike NAP, it will be based in the cloud and work with Windows Intune and mobile device management (MDM).

Conditional Access determines if a PC is healthy enough based on system integrity data such as measured boot data and Secure Boot state, which were not features of NAP. Additionally, BitLocker status, Windows updates, anti-malware signature database and so forth can be checked as well, and a "health claim" ticket to connect to network resources issued only when the system health is verified. Checking system integrity comes at a price, technically and possibly financially. You can only implement Conditional Access on computers with UEFI firmware and a TPM chip so deploying across the entire enterprise requires upgrading the entire fleet of computers to more modern systems.

Control Flow Guard

Control Flow Guard (CFG) is a feature for developers of applications for Windows 10, not its users, so while technically out-of-scope for this paper, it is interesting enough to at least mention. Control Flow Guard is **not** an add-on technology like Microsoft's *Enhanced Mitigation Experience Toolkit* (EMET) but rather implemented as a new option in Visual Studio 2015 for use when compiling programs.[61, 62, 63]

Originally implemented to deal primarily with use-after-free attacks that worked by trying to corrupt memory in the browser stack, the technology evolved into a more general purpose mechanism to prevent buffer overruns by blocking indirect calls into any program.[64] While Control Flow Guard will not make programs totally impervious to use-after-free attacks, it will help raise the bar against attacks on their code, and developers should be able to implement it with little or no changes to their code merely by recompiling it with the new option.

---

[57] Microsoft. "Features removed or Deprecated in Windows Servers 2012 R2." Published Oct. 29, 2014. Microsoft TechNet. https://technet.microsoft.com/en-us/library/dn303411.aspx.

[58] Microsoft. "Control the health of Windows 10-based Devices." Published Oct. 29, 2015. Microsoft TechNet. https://technet.microsoft.com/en-us/library/mt592023%28v=vs.85%29.aspx.

[59] Microsoft. "Azure AD, Microsoft Intune and Windows 10 – Using the cloud to modernize enterprise mobility!" Published Jun. 12, 2015. Microsoft Active Directory Team Blog. http://blogs.technet.com/b/ad/archive/2015/06/12/azure-ad-microsoft-intune-and-windows-10-using-the-cloud-to-modernize-enterprise-mobility.aspx.

[60] Nair, Anoop C. "Windows 10 Conditional Access with Azure AD Join and Intune MDM Auto Enrollment." Published Nov. 26, 2015. Anoop's SCCM ConfigMgr Troubleshooting Tips. http://anoopcnair.com/2015/11/26/windows-10-conditional-access-with-azure-ad-join-and-intune-mdm-auto-enrollment/.

[61] Microsoft. "Control Flow Guard." Windows Dev Center. https://msdn.microsoft.com/en-us/library/windows/desktop/mt637065%28v=vs.85%29.aspx.

[62] Microsoft. "/guard (Enable Control Flow Guard)." Microsoft Developer Network. https://msdn.microsoft.com/en-us/library/dn919635.aspx.

[63] Ionescu, Alex. "How Control Flow Guard Drastically Caused Windows 8.1 Address Space and Behavior Changes." Published Jan. 21, 2015. Alex Ionescu's Blog. http://www.alex-ionescu.com/?p=246.

[64] OWASP. "Using freed memory." Published Jan. 22, 2016. OWASP Foundation. https://www.owasp.org/index.php/Using_freed_memory.

Control Flow Guard has been backported to Windows 8.1, and is transparent to earlier versions of Windows, which will be able to run programs compiled with the option, but not make use of its additional security functionality. Control Flow Guard is, strictly, a software developer feature and not something end users can enable. However, customers can still ask—or make it a requirement—for Control Flow Guard to be implemented in software they want to use.

Device Guard

Device Guard is a combination of multiple hardware and software features to enable strong control of what is run on a computer, including from administrator accounts, in order to make Windows 10 more resistant to targeted attacks from determined adversaries. Also known as advanced persistent threats (APTs), such attacks come from knowledgeable, well-funded sources such as nation-states, espionage groups, organized criminal hackers and other operators in this space.

Such attacks may not rely upon malware in the traditional sense; they usually begin with exploration of the target through open source intelligence and social engineering, followed by the brief use of malware to provide initial entry to the target environment. Once inside, attackers use existing credentials and administrative tools on the network to escalate privileges. Protection against such attacks requires additional security controls in the operating system in addition to security software.

Code Integrity in Device Guard is enforced through a mixture of hardware and software technologies, including the Secure Boot feature of UEFI firmware and in Windows 10 through Kernel Model Code Integrity (KMCI), User Mode Code Integrity (UMCI) and AppLocker. [65, 66, 67, 68, 69, 70, 71] Device Guard brings a Windows Mobile-like experience to Windows in terms of how programs are locked down from running by introducing a "default deny" model of program execution. Windows will only run programs from a trusted list of apps created by the system administrator, which can be based on the application developer, availability in the Windows Store (public or a private instance hosted by Microsoft for the organization) or other programs that have been digitally-signed by the organization (useful in situations when a legacy program that was never digitally-signed needs to be used).[72]

---

[65] Microsoft. "Device Guard overview." Published Jan. 14, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/library/dn986865%28v=vs.85%29.aspx.

[66] Lich, Brian. "Device Guard overview." Published Apr. 6, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/itpro/windows/whats-new/device-guard-overview.

[67] Hallum, Chris. "Windows 10 Security Innovations at RSA: Device Guard, Windows Hello and Microsoft Passport." Published Apr. 21, 2015. Microsoft Windows Blog. https://blogs.windows.com/business/2015/04/21/windows-10-security-innovations-at-rsa-device-guard-windows-hello-and-microsoft-passport/.

[68] Anderson, Scott and Sutherland, Jeffrey. "Dropping the Hammer Down on Malware Threats with Windows 10's Device Guard." Published May 8, 2015. Microsoft Ignite 2015 Conference. https://channel9.msdn.com/Events/Ignite/2015/BRK2336.

[69] Microsoft. "Device Guard deployment guide." Microsoft TechNet. Published Jan. 28, 2016. https://technet.microsoft.com/en-us/library/mt463091%28v=vs.85%29.aspx.

[70] Lich, Brian; Poulsen, Heather; Ross, Elizabeth. "Device Guard deployment guide." Published Apr. 26, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide.

[71] Microsoft. "Windows AppLocker." Microsoft TechNet. https://technet.microsoft.com/en-us/library/dd759117.aspx.

[72] Microsoft. "Device Guard signing." Microsoft TechNet. Published Dec. 3, 2015. https://technet.microsoft.com/en-us/library/mt606940%28v=vs.85%29.aspx.

Scripts will now need to be digitally-signed in order to run, as they can perform dangerous activities. This includes VBScript (**.VBS**), JavaScript (**.JS**), Windows Script File (**.WSF**) and Windows Script Component (**.WSC**) scripts, but interestingly enough, not **.BAT** and **.CMD** script files. PowerShell will now run non-digitally-signed scripts in "`ConstrainedLanguage`" mode. MSI installation packages need to be digitally-signed as well in order to be installed on Device Guard-enabled systems.

Apps that run under Device Guard must be distributed through the Microsoft Store, including private versions of the Store. For corporations who do not use the Windows Store, a signing portal will be available to corporations wanting to use Device Guard without uploading their line of business apps into the Microsoft Store. The signing catalog will be stored in the portal for the customer.

Because it takes advantage of recent hardware features, Device Guard has specific requirements: It requires modern hardware that first shipped with Windows 8 or newer, such as a TPM 1.2 or 2.0 chip, UEFI firmware version 2.3.1 Errata B (or higher) with Secure Boot, and 64-bit CPU with virtualization support (Intel VT-x or AMD-V I/O memory management unit, and Second Level Address Translation).

As the latter requirement implies, only 64-bit versions of Windows 10 are Device Guard-capable, and only Windows 10's Enterprise and Education editions. Windows Server 2016, which is only available in a 64-bit version, is also supported.[73] Hardware manufacturers may also need to update, or at least test, their device drivers for compatibility.[74, 75]

It is possible to run Device Guard in Audit Mode, which logs when untrusted programs are run instead of blocking them. While primarily intended for testing and troubleshooting purposes to identify applications that are not yet trusted (or to verify that trust has been set up correctly), it is still useful for catching changes in environments that cannot yet fully implement Device Guard.

Device Guard is managed through Group Policy, SCCM and PowerShell. Several computer manufacturers are introducing "Device Guard-ready" PCs, with all of the requirements for Device Guard enabled by default. These include Acer, Fujitsu, Hewlett-Packard, Lenovo, NCR, PAR and Toshiba at the time of writing.

Device Guard: Is it for you?

While Device Guard sounds like it might be a solution against all current and future malware, it is only applicable in a few scenarios, such as: environments where the computers are already tightly-managed, have very well-defined software and hardware configurations, are low-churn (software on them does not get updated frequently) and run without a user (embedded) or as standard user only (e.g. ATMs, Point of Sale machines, kiosks and so forth). Device Guard will not work very well (or perhaps even at all) in unmanaged environments, organizations that have a BYOD policy or have devices running older versions of Windows.

---

[73] Microsoft. "Get apps to run on Device Guard-protected devices." Published Nov. 12. 2015. Microsoft TechNet. https://technet.microsoft.com/en-us/library/mt158214%28v=vs.85%29.aspx.

[74] Microsoft. "Driver compatibility with Device Guard in Windows 10." Published May 22, 2015. Microsoft Windows Hardware Certification Blog. http://blogs.msdn.com/b/windows_hardware_certification/archive/2015/05/22/driver-compatibility-with-device-guard-in-windows-10.aspx.

[75] Microsoft. "DF – HyperVisor Code Integrity Readiness Test." Microsoft Hardware Dev Center. https://msdn.microsoft.com/en-us/library/windows/hardware/dn955152%28v=vs.85%29.aspx.

UEFI Secure Boot, TPM and CPU virtualization also have a part to play in Device Guard, which relies on the attestation of trust provided by these technologies in order to perform secure white-listing of apps (along with specially-configured hardware delivered from OEMs/integrators). A failure in any one of these technologies, while highly unlikely, could leave systems vulnerable to bypasses.

It is also important to understand what Device Guard is not: It is not a replacement for anti-malware software, which is still needed since malware can come preloaded on systems, through supply chains, via watering hole attacks on administrators, from already-infected computers in the organization and from outside in the form of removable media and email attachments. It does, however, offer additional protections that anti-malware software does not, adding defense in depth provided Windows 10 is implemented on all computers in an environment, along with Windows Server 2016 on all servers.

Virtualization-Based Security

Virtualization-Based Security (VBS), known as Virtual Secure Mode while Windows 10 was still under development, is a security mechanism designed to make it harder to exploit the operating system. VBS does this by moving parts of the operating system's kernel into a separate partition (virtual machine) on a Type I hypervisor.[76]

Included in the hypervisor will also be the Local Security Authority Subsystem Service (LSASS), responsible for enforcing security policies on Windows, which means that Kerberos tickets, NTLM hashes, Ticketing Granting Tickets and other frequently targeted controls will exist outside of the operating system. With the kernel and LSASS thus isolated, decisions about code integrity and security can be handled outside of the operating system instead of inside it, where they are vulnerable to compromise through code injection and buffer overruns by admin/kernel level malware.

Virtualization-Based Security will be enforced through Hypervisor Code Integrity (HVCI), which will prevent pages of memory from being both writeable *and* executable, and memory pages will need to be validated by HVCI before being marked as executable. HVCI will be enforced through a monitor that controls memory allocation. In a sense, this provides an AppLocker-like experience, except for protecting memory pages in the Windows kernel instead of files.

A virtual TPM (vTPM) stack is also included in Virtualization-Based Security. While not a malware-resistance feature *per se*, it will help with the adoption of BitLocker on Windows Server 2016 Hyper-V virtual machines.

Virtualization-Based Security is a prerequisite for Device Guard, and shares similar hardware requirements, such as requiring a CPU capable of supporting Intel VT-x and VT-d or AMD AMD-V IOMMU extensions. Like Device Guard, Virtualization-Based Security will only be available for the Enterprise and Education editions of Windows 10.

Microsoft Edge

With the release of Windows 10, and with the stated goal of replacing Internet Explorer with a more modern and more secure web browsing experience, Microsoft introduced its first new web browser in

---

[76] Stocco, Gabe; Anderson, Scott; Manangi, Suhas. "Overview of Windows 10 Requirements for TPM, HVCI and SecureBoot." Published May 18, 2015. UEFI Spring Plugfest. http://www.uefi.org/sites/default/files/resources/UEFI_Plugfest_May_2015%20Windows%2010%20Requirements%20for%20TPM,%20HVCI%20and%20SecureBoot.pdf.

two decades, Microsoft Edge.[77, 78, 79, 80] Microsoft Edge is replacing its older sibling, which has long been a target of attackers.[81] One of the ways in which Microsoft Edge will do this is by being written from the ground up. For one thing, it is being written as a Universal Windows App, and not using the "legacy" Win32 API, allowing the web browser to run inside *Universal Windows Apps'* app container sandbox. This means that Microsoft Edge is not a refactored version of Internet Explorer nor will it even contain code from Internet Explorer, although it will certainly borrow design concepts from it as well as other browsers such as Google Chrome and Mozilla Firefox.

Starting from scratch like this means that Microsoft Edge will have a smaller codebase and, coupled with secure development practices, should mean the browser has a reduced attack surface, as well as lead to some improvements that are not security-related but still welcome, such as decreased memory usage and increased performance.

EdgeHTML, Microsoft Edge's layout engine, is a fork of Microsoft's Trident layout engine for Internet Explorer, however it has been significantly rewritten to be fully compatible to remove support for legacy technologies (more on this below).[82, 83, 84] Microsoft's goal with EdgeHTML is to make it functionally identical to the WebKit engine used by Chromium-based browsers such as Google Chrome and Apple Safari.

Microsoft Edge supports HTTP Strict Transport Security (HSTS) to connect to sites automatically using `https://` when `http://` is specified in the address field. Microsoft Edge gets the list of sites that support HSTS from `https://hstspreload.appspot.com`, the same place Google Chrome, Mozilla Firefox and Internet Explorer do. Microsoft Edge and Internet Explorer will be updated quarterly from the list.

Extension Support

Another way in which Microsoft Edge will improve browser security is by breaking with Microsoft's long practice of making programs backwards compatible with previous versions. For example, Edge will not

---

[77] Microsoft. "Microsoft Edge Browser." Microsoft. https://www.microsoft.com/en-us/windows/microsoft-edge.

[78] Ali Husein, Masood. "Getting the Most out of Microsoft Edge." Published Nov. 16, 2015. Microsoft IT Showcase. https://download.microsoft.com/download/2/F/B/2FBEBC08-69F8-4CC2-9542-2493AFD49496/6053_Microsoft_Edge_WSG_External.docx.

[79] Microsoft. "Changelog: Microsoft Edge Dev." Microsoft Developer Technologies. https://dev.windows.com/en-us/microsoft-edge/platform/changelog/.

[80] Wikipedia. "Microsoft Edge." Published Feb. 23, 2016. Wikimedia Foundation. https://en.wikipedia.org/wiki/Microsoft_Edge.

[81] Microsoft Edge Team. "Microsoft Edge: Building a safer browser." Published May 11, 2015. Microsoft Edge Dev Blog. https://blogs.windows.com/msedgedev/2015/05/11/microsoft-edge-building-a-safer-browser/.

[82] Microsoft. "A break from the past: the birth of Microsoft's new web rendering image." Published Feb. 26, 2015. Microsoft Edge Dev Blog. https://blogs.windows.com/msedgedev/2015/02/26/a-break-from-the-past-the-birth-of-microsofts-new-web-rendering-engine/.

[83] Cowan, Crispin. "Protecting Microsoft Edge against binary injection." Published Nov. 17, 2015. Microsoft Edge Dev Blog. https://blogs.windows.com/msedgedev/2015/11/17/microsoft-edge-module-code-integrity/.

[84] Yason, Mark. "Understanding EdgeHTML's Attack Surface and Exploit Mitigations." Published Apr. 28, 2016. IBM Security Intelligence. https://securityintelligence.com/understanding-edgehtmls-attack-surface-and-exploit-mitigations/.

support binary extensions including ActiveX Controls.[85, 86, 87, 88] Edge will also not support Browser Helper Objects (BHOs). Both ActiveX and BHOs have long been staples of Internet Explorer.[89, 90, 91] ActiveX was originally developed as a proprietary extension to allow Internet Explorer to run more complex programs inside the web browser, while BHOs were a framework to create plugins to handle file formats not directly supported by the web browser, to add toolbars and so forth. ActiveX was adopted by many enterprises for creating proprietary line of business applications and even by financial institutions for access control mechanisms, and BHOs were used to provide plugins for viewing media, such as PDF files. Unfortunately, both technologies were also abused by malware authors, causing Microsoft to enter into a never-ending race to develop countermeasures, such as blacklisting malicious ActiveX controls, distributing and maintaining an anti-spyware program, and so forth.[92]

With Microsoft Edge, the company has gone down a different path: While the version of Edge that shipped with Windows 10 came with *some* extensions (most notably the Adobe Flash Player plugin), it was limited to what Microsoft provided. There was no way for developers to add their own extensions to Edge. Microsoft has announced that extensions will be supported in Edge, but in the form of JavaScript script files and not as executable programs as they were with Internet Explorer. While this will allow for the development of extensions with many capabilities, developing them as scripts means there will be security limitations that ActiveX controls, delivered as executable programs could bypass. It also means extension development for Microsoft Edge will be similar to how extensions are written for Google Chrome and Mozilla Firefox web browsers. As an additional layer of security, extensions for Microsoft Edge will run inside Windows 10's AppContainer sandbox.

As of this writing, Microsoft Edge is limited to viewing PDFs (via Microsoft's own plugin) and accessing the video driver for graphics acceleration, both of which are through interfaces brokered by Microsoft. Adobe Flash, a non-Microsoft plugin, is also supported, but distributed with and updated as part of the operating system, as it has been since Windows 8. While it is always possible these may introduce attack vectors into the operating system, Microsoft Edge's smaller code base should make it easier to defend against attacks. A version of Microsoft Edge with third-party extension support and a handful of extensions is available in builds of Windows 10 on the Windows Insider Program Build release channel.[93]

---

[85] Microsoft. "About ActiveX Controls." Microsoft Developer Network. https://msdn.microsoft.com/en-us/library/aa751971%28v=vs.85%29.aspx.

[86] Microsoft. "Use ActiveX Controls." Microsoft Windows How-to. https://www.microsoft.com/en-us/security/pc-security/activex.aspx.

[87] Microsoft. "Protect yourself when you use ActiveX controls." Microsoft Safety & Security Center. https://www.microsoft.com/en-us/security/pc-security/activex.aspx.

[88] Wikipedia. "ActiveX." Published Feb. 14, 2016. Wikimedia Foundation. https://en.wikipedia.org/wiki/ActiveX.

[89] Esposito, Dino. "Browser Helper Objects: The Browser the Way You Want It." Published Jan. 1999. Microsoft internet Explorer Technical Articles. https://msdn.microsoft.com/en-us/library/bb250436%28v=vs.85%29.aspx.

[90] Schreiner, Tony; Sudds, John. "Building Browser Helper Objects with Visual Studio 2005." Published Oct. 27, 2006. Microsoft Exploring Internet Explorer Column. https://msdn.microsoft.com/en-us/library/bb250489.aspx.

[91] Microsoft. "How to disable third-party tool bands and Browser Helper Objects." Microsoft Knowledgebase. Published Aug. 25, 2010. https://support.microsoft.com/en-us/kb/298931.

[92] Thurrott, Paul. "Microsoft Windows Anti-Spyware." SuperSite for Windows. Published Oct. 6, 2010. http://winsupersite.com/product-review/microsoft-windows-anti-spyware.

[93] Microsoft. "Preview extensions for Microsoft Edge today!" Microsoft Developer Technologies. https://developer.microsoft.com/en-us/microsoft-edge/extensions/.

To further ensure content integrity, non-Microsoft/non-WHQL-signed DLLs are not allowed to be called by Edge, with the exception of video drivers, which are allowed access to Microsoft Edge's sandbox in order to accelerate graphics.[94] Additional security enhancements to block binary extensions are planned.[95]

As with Google and the Mozilla Foundation, Microsoft will distribute extensions for its web browser through a store that it curates. This allows Microsoft to audit the security of third-party browser extensions before releasing them, just as Google and Mozilla do with their respective stores. It should be noted that despite these efforts, Chrome and Firefox do have problems with malicious, potentially unwanted and privacy-invasive browser extensions. Microsoft will need to do as good a job—if not better—than Google and Mozilla in managing the security of its extension store if it wants Edge to become the browser of choice for its Windows 10 customers.

Fail Fast

Another architectural difference between the old Internet Explorer browser and the new Edge browser is Microsoft's decision to make Edge "fail fast," or to explicitly crash when an error occurs, instead of trying to recover from it.

While this may seem counterintuitive, and an example of the browser being brittle or fragile, it actually has merit as a security mechanism: Historically, many of Internet Explorer's vulnerabilities were performed by getting the web browser to continue after it had encountered an exploit, allowing the browser to be a vector for code injection, elevation of privilege, sandbox escapes and other kinds of attacks.

By crashing Microsoft Edge, and then restarting it, Microsoft is attempting to remove the web browser from the leading edge of any exploit chain.

Edging towards a solution

Microsoft seems to be on the right track with securing Microsoft Edge, coupling its current knowledge of best secure coding practices, developed through its Security Development Lifecycle, with analysis of two decades of vulnerabilities to create a more secure browser.[96] However, this does not mean Microsoft Edge will be invulnerable to attacks. The browser already has received several updates to fix vulnerabilities within its own code and, because it supports extensions such as Adobe Flash, there is always the possibility that those will be targeted as well.[97, 98, 99]

---

[94] Microsoft. "WHQL Release Signature." Microsoft Hardware Dev Center. https://msdn.microsoft.com/en-us/library/windows/hardware/ff553976%28v=vs.85%29.aspx.

[95] Weston, David. "The Cutting Edge of Browser Security." Published Apr. 4, 2016. Microsoft Edge Web Summit 2016. https://channel9.msdn.com/Events/WebPlatformSummit/edgesummit2016/ES1604.

[96] Microsoft. "Security Development Lifecycle." Microsoft. http://www.microsoft.com/en-us/sdl/.

[97] Microsoft. "MS16-038: Cumulative security update for Microsoft Edge: April 12, 2016." Published Apr. 12, 2016. Microsoft. https://support.microsoft.com/en-us/kb/3148532.

[98] Microsoft. "Microsoft Security Bulleting MS16-038 - Critical: Cumulative Security Update for Microsoft Edge (3185232)." Published Apr. 12, 2016. Microsoft Security TechCenter. https://technet.microsoft.com/library/security/MS16-038.

[99] Microsoft. "Microsoft Security Bulleting MS16-050 - Critical: Security Update for Adobe Flash Player (6154132)." Published Apr. 12, 2016. Microsoft Security TechCenter. https://technet.microsoft.com/en-us/library/security/ms16-050.

Also possible is the discovery of flaws in other subsystems used by Microsoft Edge, like video acceleration and font rendering, to name but two. These subsystems have the potential to introduce vulnerabilities that can be exploited by attackers.

As Microsoft's new, recommended web browser, Microsoft Edge will be targeted by attackers, especially if it gains a reputation as the browser of choice for banking, shopping, and other financial activities. So, while Microsoft may be developing a *more secure* web browser, please remember there's still no such thing as a *totally secure* web browser. Protect yourself and act accordingly while online.

Microsoft Passport

Microsoft Passport is Microsoft's new implementation of a two-factor authentication system for identity verification.[100, 101] Originally developed as a single-sign-on mechanism in the late 1990s for web-based ecommerce sites, Passport has had several names and functions over the years, including its best well-known identity as the authentication system for Microsoft's Hotmail web-based email accounts.[102]

For the past decade-and-a-half, Microsoft Passport has taken on different functions, and today it is designed to replace—or at least heavily augment—passwords in Windows 10. This covers not just logging on to a device locally, by also to any Active Directory or Azure Active Directory accounts, as well as those from federated services.

For Windows 10, Microsoft Passport encompasses Microsoft's implementation of the FIDO Alliance's authentication system, which means this could be extended even further in the future to other devices and services, such as those from fellow FIDO Alliance members Apple and Google. [103]

Microsoft Passport works by allowing the user to log onto an enrolled device by using a new kind of credential, paired with biometric authentication or a PIN code.[104, 105] This credential is stored as cryptographic keys in the device's TPM chip, or in a virtual TPM if a chip is not present. By using these techniques, Microsoft hopes to make it extremely difficult for an attacker to steal credentials from users and reuse them to penetrate further into an organization.

Ultimately, Microsoft Passport is meant to replace PKI in the enterprise with a simpler solution, as well as offering the same level of authentication that PKI systems provide to consumers, but this will require a broad, long-term effort, and it is still too early to see if Microsoft's solution is compelling enough to replace the investment enterprises have made in their existing PKI infrastructure.

---

[100] Hallum, Chris. "Microsoft Passport guide." Published Apr. 20, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/microsoft-passport-guide.

[101] Windows Apps Team. "Convenient two-factor authentication with Microsoft Passport and Windows Hello. Published Jan. 26, 2016. Microsoft Building Apps for Windows Blog. https://blogs.windows.com/buildingapps/2016/01/26/convenient-two-factor-authentication-with-microsoft-passport-and-windows-hello/.

[102] Wikipedia. "Microsoft account." Published Apr. 17, 2015. Wikimedia Foundation. https://en.wikipedia.org/wiki/Microsoft_account.

[103] FIDO Alliance. "About The FIDO Alliance." https://fidoalliance.org/about/overview/.

[104] Lich, Brian. "Microsoft Passport overview." Published Apr. 6, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/itpro/windows/whats-new/microsoft-passport.

[105] Decker, Jared. "Managed identity verification using Microsoft Passport. Published Apr. 14, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/manage-identity-verification-using-microsoft-passport.

Windows Hello

The biometric authentication system used by Microsoft Passport is called Windows Hello, and it will employ a variety of biometric sensor technologies, both new and old, to identify a device's user.[106, 107]

To date, Windows Hello supports the following biometric technologies:

- Swipe- and touch-style fingerprint reader sensors, such as those from Authentec/UPEK, and Synaptics (formerly Validity), which are used on a variety of business laptops, ultrabooks, and tablets.[108]
- Facial recognition using 3-D cameras, such as Intel's RealSense camera, which combines a conventional camera, an infra-red camera, and an infra-red laser for depth sensing to detect whether a person is in front of the camera.[109]
- Iris recognition cameras, such as the model used in the Microsoft Lumia 950 and 950XL, the first smartphones shipped by Microsoft with its Windows 10 Mobile operating system. [110, 111]

Because Windows Hello is a framework, it is likely that support for other kinds of biometric sensors will be added during Windows 10's lifecycle, such as palm readers, blood vessel/vein-sensing readers and perhaps even other as-yet-to-be-discovered technologies.

One thing to note about Windows Hello is that as a prerequisite for enrolling any kind of biometric, you must first set up a PIN on the device, if you have not already done so.

In testing Windows Hello with AuthenTec's Eikon Mini USB Fingerprint Reader (a swipe-based fingerprint reader) and Intel's RealSense F200 3-D camera for facial sensing, I found enrollment and detection to work as advertised.

In the case of Intel's RealSense camera, I was detected with and without glasses, although a baseball cap seemed to stymie detection, possibly because the bill of the hat was in the way.

Figure 7: AuthenTec Eikon Mini USB Fingerprint Reader plugged into the author's Lenovo Yoga 900

---

[106] Microsoft. "Windows Hello." Get Started with Windows 10. http://windows.microsoft.com/en-us/windows-10/getstarted-what-is-hello.

[107] Protalinski, Emil. "Windows Hello and Microsoft Passport: Unlock Windows 10 devices and apps with your finger, iris, or face." Published Mar. 17, 2015. VentureBeat. http://venturebeat.com/2015/03/17/windows-hello-biometric-authentication-will-let-you-unlock-windows-10-devices-with-your-finger-iris-or-face/.

[108] Synaptics. "Area Touch and Swipe Fingerprint Sensors." Synaptics. http://www.synaptics.com/products/biometrics.

[109] Intel. "Intel RealSense Technology Overview." Intel. http://www.intel.com/content/www/us/en/architecture-and-technology/realsense-overview.html.

[110] Microsoft. "Microsoft Lumia 950 Smartphone." Microsoft Lumia. https://www.microsoft.com/en-us/mobile/phone/lumia950/.

[111] Microsoft. "Microsoft Lumia 950 XL Dual-SIM Smartphone." Microsoft Lumia. https://www.microsoft.com/en-us/mobile/phone/lumia950-xl-dual-sim/.

On a Microsoft Lumia 950 smartphone with Windows 10 Mobile, I was unable to enroll my iris or be recognized without taking off my glasses. It should be noted, however, that this feature was in beta when I tested it. Windows 10 Mobile will work with Windows Passport and Windows Hello just as its desktop brethren does, and be MDM-manageable, as well.

Windows 10 Mobile

While Windows 10 Mobile is out of scope of this whitepaper, we did briefly want to discuss some of its security features.

Windows 10 Mobile smartphones, phablets and tablets (7-inch screen and under) will use ARM or Intel CPUs, but will only be capable of running Universal Windows Apps (formerly known as Modern and even before that as Metro). These large phones (or small tablets) are a new class of device and will have UEFI, TPM 2.0 and Secure Boot always enabled, and run apps in a sandbox, just like Windows Phone 8.1 does.[112]

The underlying security of Windows 10 Mobile is largely the same as Windows Phone 8.*x*. All apps run in a least-privilege chamber (sandbox) only with privileges announced via manifest at install time. New privileges require a new installation of the app, similar to the way in which apps on Android OS and iOS behave.

As with Windows Phone 8.1, Windows 10 Mobile devices will not be able to run software that directly accesses the operating system, such as anti-malware software. Other kinds of security software, such as two-factor authentication, should still work, although they may need to be recompiled as Universal Windows Apps.

Older tablets with 7-inch screens, such as those from Dell, Toshiba, Hewlett-Packard, WinBook (MicroCenter) and so forth that run 32-bit versions of Windows 8.1 on an Intel Atom (x86) core will not be offered Windows 10 Mobile as their Windows 10 upgrade, but instead will receive the regular Windows 10 32-bit (x86) version offered for PCs. This ensures those devices will continue to run "legacy" Win32 applications and that those applications will continue to be able to access their data, and so forth. This also means that security software such as anti-malware programs will run on them as well.

Privacy

Microsoft talks a great deal about "the Windows experience", wanting the operating system to feel seamless and to be responsive to users. For Windows 10, *frictionless* is a word which has been bandied about. From most other companies, this could (and should) be safely ignored as marketing drivel; however, in Microsoft's case, they are dead serious about providing users with a positive Windows experience. Of course, the interesting part of all of this for consumers and businesses is figuring what Microsoft considers a positive Windows experience to be.

It always makes sense to review the privacy settings and the policies of whatever software or services you are using, and Windows 10 is no exception.

---

[112] Meeus, Alain. "Windows 10 for Mobile Device: Secure by Design." Published May 8, 2015. Microsoft Ignite 2015 Conference. https://channel9.msdn.com/Events/Ignite/2015/BRK3309.

For Windows 10, this means allowing the user to move between different devices such as smartphones, tablets and PCs, not just so that they have all of their information at their fingertips, but in a way that is appropriate for the way in which we interact with different devices, and even those devices' locations in time and space.

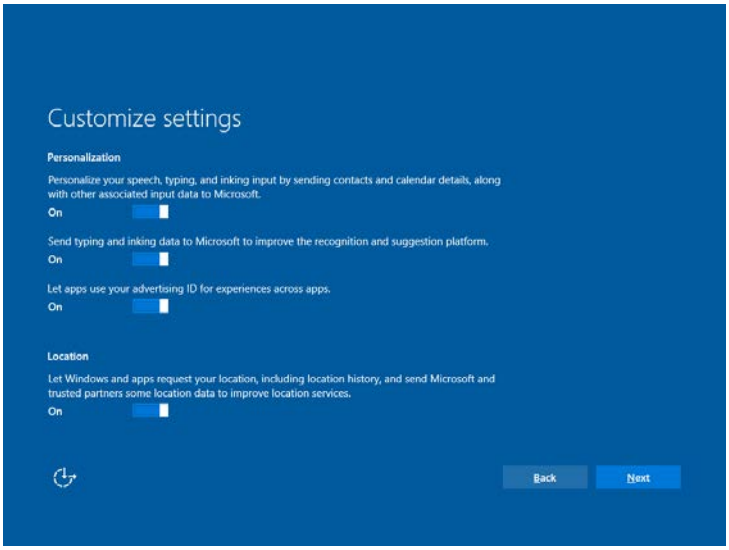


Figure 8: "If you do not choose the Express Setup option during installation, Windows 10 offers the ability to tweak its privacy-related settings.

While none of this may be new to those of us using smartphones over the past few years, Windows 10 marks the first time this level of personalization and integration has been offered via a desktop operating system in what had previously been the realm of smartphones, and that has some interesting ramifications for privacy in a world where your computers are always on, always listening, and always watching you.

Or does it?

Microsoft's privacy policies have traditionally been rather dry, but have basically been customer-centric. Measurements and other data (aka *telemetry*) that are collected are used for the sole purpose of improving Microsoft's products and services, and the company goes to great lengths to avoid intentionally collecting any personally-identifiable information (PII), always anonymizing or scrubbing it to ensure the origin of any private data they collect cannot be used to identify individuals.

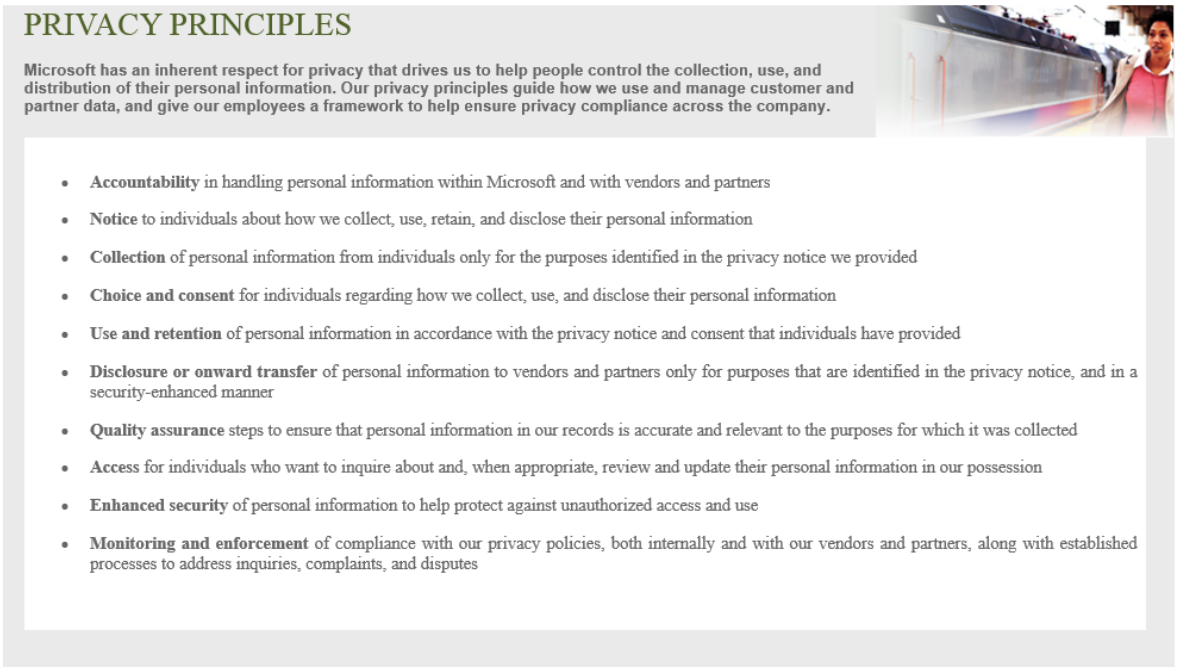


Figure 9: Microsoft Privacy Principles

Microsoft's collecting of anonymized telemetry for the purpose of improving its offerings is not particularly new. The Customer Experience Improvement Program (CEIP), was launched in February 2009, when Microsoft Windows Vista was the apex of Windows architecture.[113]

Even then, Microsoft was thinking about the privacy implications; hence it had its own set of Frequently-Asked Questions and Privacy Policies to provide additional information about how the company safeguards its customers' data.[114, 115] Microsoft continued its Customer Experience Improvement Program in Windows 7 and in Windows 8-8.1, as well as their Windows Server counterparts.[116, 117]

So, your computers may have been sharing anonymized data with Microsoft for over seven years. But long before Microsoft began its Customer Experience Improvement Program, in 2001 it introduced Windows Error Reporting (WER) in Windows XP to automate the collection of data on application crashes and faults.[118, 119] WER has been present and expanded in every version of Windows since then to collect more information to help troubleshoot and diagnose system errors, including those from third-party programs.

Cortana Search Agent

With Windows 10, Microsoft believes a key reason for users to upgrade is having access to Cortana. Cortana is a search agent with voice recognition capabilities that can mine data such as your emails and contacts in order to give you information that is relevant to your interests, and this poses a privacy dilemma for some people.

While I have yet to see (or hear) Cortana offer me any information at my desktop (most likely due to it not having a microphone connected to it) it has given me results on smartphones. Under Windows Phone 8.1 and Windows Mobile 10, Cortana has offered to put a flight into my schedule after the airline sent me a confirmation email and when packages will be delivered. These are not unique value propositions for Windows, either:

An Android smartphone offered status updates on packages I'm receiving as well when it saw orders I'd placed with online retailers come through via email. These are just two examples of how companies such as Microsoft and Google can scan your emails.

---

[113] Microsoft. "Microsoft Customer Experience Improvement Program." Microsoft TechNet. https://technet.microsoft.com/en-us/library/cc766341(v=ws.10).aspx.

[114] Microsoft. "Windows Customer Experience Improvement Program and Resulting Internet Communication in Windows Vista." Microsoft TechNet. https://technet.microsoft.com/en-us/library/cc766341%28v=ws.10%29.aspx.

[115] Microsoft. "Privacy Statement for the Microsoft Customer Experience Improvement Program." https://www.microsoft.com/products/ceip/en-us/privacypolicy.mspx.

[116] Microsoft. "Windows Customer Experience Improvement Program and Resulting Internet Communication in Windows 7 and Windows Server 2008 R2." https://technet.microsoft.com/en-us/library/ee126127%28v=ws.10%29.aspx.

[117] Microsoft. "Manage Privacy: Windows Customer Experience Improvement Program and Resulting Internet Communication." https://technet.microsoft.com/en-us/library/jj618322.aspx.

[118] Microsoft. "What are WER Services?" Microsoft MSDN. http://blogs.msdn.com/b/wer/archive/2008/12/26/what-are-wer-services.aspx.

[119] Wikipedia. "Windows Error Reporting." Wikimedia Foundation. Published Jun, 8, 2015. https://en.wikipedia.org/wiki/Windows_Error_Reporting.

Is this a violation of my privacy? No, I don't think so, since I was prompted to enable these services when setting up the devices and I did give my consent.

Is it convenient? Yes, in both instances I found it useful. Especially in the case of not having to go and copy and paste my flight itinerary into my calendar. Convenience trumps security, though, which I'll get to in a moment.

It is invasive, or merely borderline creepy? Those are bigger and more difficult questions to answer. And those answers are going to vary based on the privacy needs of the individual or the business.

I can definitely see situations where an individual might not want to have information about appointments with doctors, pharmacists, lawyers, family planning clinics and so forth parsed by an outside party, even if that outside party is a machine intelligence. Likewise, a business in a regulated industry – or one merely involved in a merger, acquisition or facing upcoming rounds of layoffs – may not want the particulars of those emails, calendar appointments and meeting requests to be examined at all, even if in aggregated form where the identifying data is anonymized.

It always makes sense to review the privacy settings and the policies of whatever software or services you are using, and Windows 10 is no exception. Before making the decision to migrate from Windows 7 or 8, you should carefully review these and think about what the implications might be for your home or business.

I'm from the government, and I'm here to help

Windows 10 potentially gives Microsoft access to the same information about your lifestyle that has previously only been accessible on smartphone operating systems such as Apple iOS and Google Android. And, for all of the numerous legal issues Microsoft has had over the past decades — and there have been many — the one issue Microsoft has generally not had much of is data breaches involving the disclosure of its customers' personally-identifiable information.

The same, though, may not be said of governments around the world, which may engage in activities such as requiring bloggers to register with the government, requiring a government-issued ID when purchasing Internet access, or merely purchasing devices *capable* of accessing the Internet (even if they don't), installing monitoring devices or state-operated firewalls and, of course, the wholesale monitoring of their citizens' communications.

Even if a government agency is only looking at the captured metadata and not the actual communications themselves, that metadata may be considered enough to justify extreme actions. Consider what Gen. Michael Hayden, former head of the NSA, stated in 2014: "We kill people based on metadata." [120, 121]

This makes it easier to understand why Microsoft has gone through great efforts to challenge the U.S. government's search warrant case for access to overseas data, and other governments are trying to

---

[120] Wikipedia. "Metadata." Published Aug. 10, 2015. Wikimedia Foundation. https://en.wikipedia.org/wiki/Metadata.

[121] Ferran, Lee. "Ex-NSA Chief: 'We Kill People Based on Metadata.'" Published May 12, 2014. ABC News. http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/.

help them do so (which is quite a change considering that some of the same agencies were investigating Microsoft a decade ago).[122, 123, 124, 125, 126]

There is still quite a bit of work to be done to secure the Internet, not just from criminals and rogue nation-states, but from well-meaning governments that are clueless about how technologies such as encryption work. Microsoft is increasingly finding itself in the position of advocating for its customers' privacy.[127, 128, 129]

Microsoft has been at the head of this fight for users' privacy, not just because they understand that people will not use their products and services if they don't have any privacy, but because it is the correct thing to do. As long as Microsoft is able to fight that battle, it should be safe for customers to use its products.

Microsoft on Privacy

Privacy issues have been discussed by Microsoft on their *Microsoft on the Issues* blog, to which I linked extensively in the preceding paragraphs.[130] However, that's not all they have to say on privacy. Microsoft is a gigantic company, and they have many privacy policies for their operating systems and services. Here are a few to read if you're so inclined:

- Microsoft Account Privacy
- Microsoft Privacy Statement
- Microsoft Services Agreement
- Trustworthy Computing – Privacy
- Trustworthy Computing – Privacy Overview
- Trustworthy Computing – Privacy Models

---

[122] Meisner, Jeff. "Brad Smith in WSJ interview: why we oppose government demands for personal data." Published Jul. 24, 2014. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/2014/07/24/brad-smith-wsj-interview-oppose-government-demands-personal-data/.

[123] Smith, Brad. "Our legal challenge to a US government search warrant." Published Apr. 9, 2015. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/2015/04/09/our-legal-challenge-to-a-us-government-search-warrant/.

[124] Meisner, Jeff. "Microsoft responds to ruling in warrant case." Published Jul. 31, 2014. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/2014/07/31/microsoft-responds-ruling-warrant-case/.

[125] Microsoft Corporate Blogs. "What if? Microsoft appeal ponders U.S reaction to foreign data demand." Published Dec. 8, 2014. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/2014/12/08/microsoft-appeal-ponders-u-s-reaction-foreign-data-demand/.

[126] Microsoft Corporate Blogs. "Government of Ireland, European MEP file amicus briefs in New York privacy case." Published Dec. 23, 2014. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/2014/12/23/government-ireland-european-mep-file-amicus-briefs-new-york-privacy-case/.

[127] Microsoft Corporate Blogs. "Unfinished business on government surveillance reform." Published Jun. 24, 2014. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform/.

[128] Microsoft Corporate Blogs. "Safety, privacy and the Internet paradox: solutions at hand and the need for new trans-Atlantic rules." Published Jan. 20, 2015. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform/

[129] Perlroth, Nicole. "Security Experts Oppose Government Access to Encrypted Communication." Published Jul. 7, 2015. New York Times. http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html.

[130] Microsoft. Microsoft on the Issues (blog). http://blogs.microsoft.com/on-the-issues/

- Windows 8 and Windows Server 2012 Privacy Statement
- Windows 8.1 and Windows Server 2012 R2 Privacy Statement

If you are concerned about ESET's own privacy policies you may find the privacy policy for ESET's *We Live Security* blog here, the privacy policy for our main ESET web site here, the privacy policy for ESET's support forum here, and a copy of our EULA agreement here. ESET is headquartered in Europe and abides by EU laws, which are some of the strongest in the world when it comes to customer privacy.

Closing Thoughts

Is Windows 10 a more secure version of Windows? Even from the limited information put into this white paper, we can tell that it is. However, the question that is likely to be on most Windows users' minds is whether it is a *better* version of Windows. The answer to that question is a little more complicated: Microsoft is clearly in the midst of transitioning from a waterfall development model of releasing a major new version of Windows every few years to a more agile development model which allows them to continuously update the operating system not just to add new features and functionality, but to change existing behaviors as well. For people used to relying on their computers working in a predictable way, this can be frustrating. But it also means that instead of purchasing new licenses every few years, they will always have the latest version of Windows, with all of updates and security features applied cumulatively to their operating system.

Microsoft has been heavy-handed in its pushing of Windows 10's upgrades to its "legacy installed base" of Windows 8.1 and Windows 7 users, which some find overly paternalistic and intrusive. Yet, at the same time, it has been shown that older versions of Windows are less secure and more likely to be attacked, serve as jumping-off points for further attacks, or both.

Ultimately, it is up to each computer owner to decide whether or not they want to upgrade to Windows 10. By presenting this white paper, we hope to have provided you with enough information about Windows 10's security benefits to help you make your decision.

For questions and comments relating to this white paper, please contact the author care of AskESET@eset.com.

Acknowledgements: Special thanks to my colleagues Chris Bono, Bruce P. Burrell, Stephen Cobb, Nick FitzGerald, David Harley and Fer O'Neil for their assistance in writing this white paper. I would also like to offer my thanks to Lenovo for providing access to pre-release hardware and BIOS/UEFI firmware, to Microsoft for providing access to pre-release versions of Windows 10 as well as answering several technical questions which came up during the research. Thanks also to VMware for the virtualization technology used while researching Windows 10.

Aryeh Goretsky, MVP, ZCSE
Distinguished Researcher, ESET