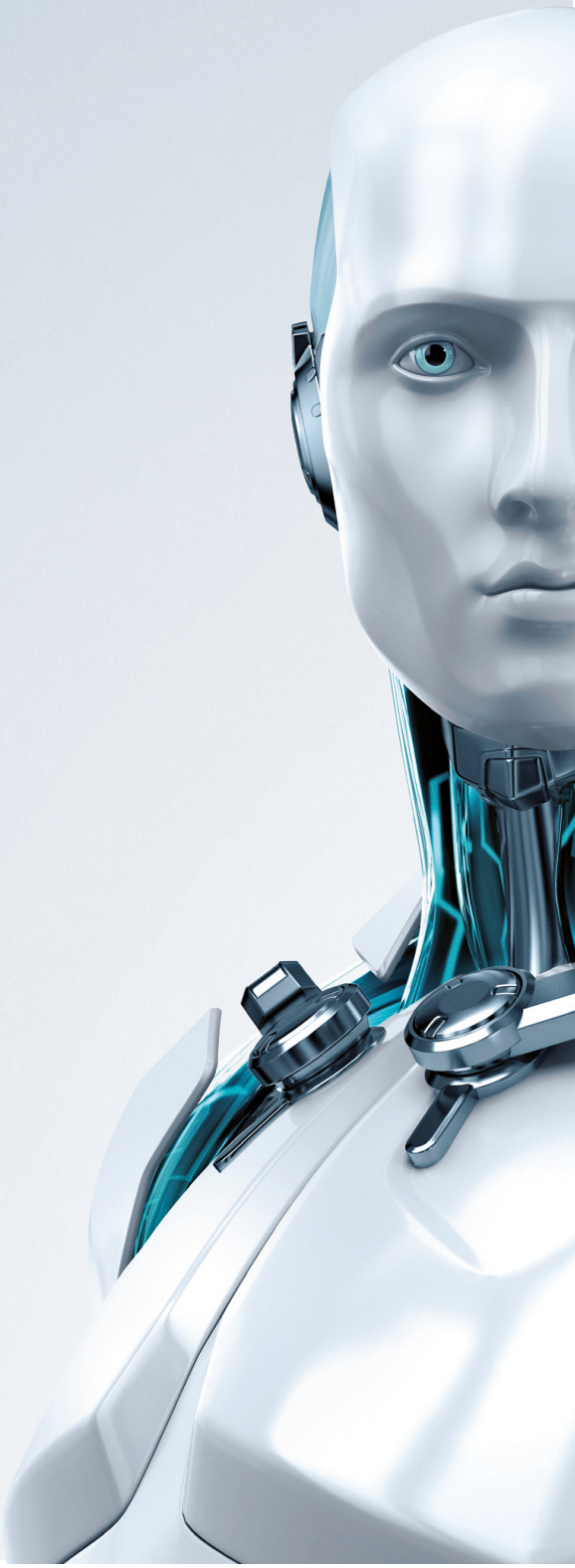
Microsoft Windows® 10 Anniversary Update Security and Privacy

An ESET White Paper



ENJOY SAFER TECHNOLOGY™

Windows 10 Anniversary Update Security and Privacy

An ESET White Paper

Version 1.0 – January, 2017

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 this 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of Windows 10 features (including screenshots), future changes made by Microsoft may make parts of the paper out of date. Please check with ESET for the latest version for the most accurate and up-to-date information we are able to provide on Windows 10.

Contents

Introduction 3
What's Been Removed 4
Wi-Fi Sense 4
Kid's Corner 5
App-V and UE-V 6
What's Been Changed 6
Group Policy 6
PIN-based Login 7
Windows Defender 8
Features and Options 9
Fast Ring Builds 9
Limited Periodic Scanning 10
Detection Issues 10
Microsoft Edge 11
Driver Signing 11
Privacy 12
Other Considerations 12
Closing Thoughts 15
For More Information 15
Acknowledgements and Contact Information 16

Introduction

Known variously as the Windows 10 Anniversary Update, v1607 (for its July 2016 release to manufacturing), Redstone 1 and Build 14393, this is the second major update of Windows 10 following the Threshold 2/v1511/Build 10586 update of November 2015. The Windows 10 Anniversary Update was released to consumers on June 29, 2016 as the Current Branch offering, and on November 29, 2016 to the enterprise as the Current Branch for Business offering[1,2].

The Windows 10 Anniversary Update adds new features likely to be welcomed by system administrators, IT Pros, power users and enthusiasts. However, it also *removes* some of the same features, functionalities and tweaks that previously worked under the Pro edition, relegating them to the Enterprise edition, which has only been available by licensing them from Microsoft. Traditionally, small businesses (and home users) have obtained their Windows licenses when purchasing a new computer, so this move allows Microsoft to monetize computer systems that would otherwise not generate recurring revenue for them.

While it may rankle small business owners and home users who have long relied on Pro editions of Windows, Microsoft has long wished to expand its Windows as a Service (WaaS) model from the enterprise and mid-sized businesses down into the small business space, and removing the ability to make certain tweaks to the operating system is one way for Microsoft to accomplish this goal.

The Windows 10 Anniversary Update also introduces a new edition of Windows 10, Education Pro. Unlike the Education edition, which is based on business-focused Windows 10 Enterprise, the Education Pro is based on the increasingly-consumer-focused Windows 10 Pro and is comparable in features and restrictions to it. As with the Education edition, Education Pro is only available under license from Microsoft.

The focus of this article, though, is not licensing changes or revenue models, but security and privacy. While we have discussed Windows 10's security and privacy features extensively at We Live Security, in our *Windows 10 Security and Privacy* guide, the new release contains some security features of interest, and perhaps even concern, to all Windows 10 users[3,4]. In this article, we look at the differences in security most likely to be noticed by, and impact upon, businesses and home users after they have upgraded.

---

[1] Lefferts, Rob. "Advancing Security for Consumers and Enterprises at Every Layer of the Windows 10 Stack." Published Jun. 29, 2016. Windows Business Blog. https://blogs.windows.com/business/2016/06/29/advancing-security-for-consumers-and-enterprises-at-every-layer-of-the-windows-10-stack/#pCO5ywAL4rk4J4Gj.97

[2] Neihaus, Michael. "Windows 10 1607 is now a Current Branch for Business (CBB) release." Published Nov. 29, 2016. Microsoft TechNet. https://blogs.technet.microsoft.com/windowsitpro/2016/11/29/windows-10-1607-is-now-a-current-branch-for-business-cbb-release/

[3] Goretsky, Aryeh. "Windows 10 security and privacy: An in-depth review and analysis." Published Jun. 15, 2016. ESET WeLiveSecurity blog. http://www.welivesecurity.com/2016/06/15/windows-10-security-privacy-depth-review-analysis/

[4] Goretsky, Aryeh. "Microsoft Windows 10 Security and Privacy: An ESET White paper." Published Jun. 15, 2016. ESET. http://www.welivesecurity.com/wp-content/uploads/2016/06/windows-10-security-privacy.pdf

What's Been Removed

To begin with, we are going to look at two features being removed from the Windows 10 Anniversary Edition: Wi-Fi Sense and Kid's Corner.

Wi-Fi Sense

Originally, Wi-Fi Sense was provided as a way to automatically share access to open Wi-Fi hotspots by sharing their names (SSIDs) and credentials with your *Contacts* when you logged into Windows 10 with your Microsoft Account which, for most people probably means a hotmail.com or outlook.com email account[5, 6]. For Contacts, this referred to people who are not just outlook.com contacts and Skype contacts, both of which are properties owned by Microsoft, but also their Facebook Friends as well.

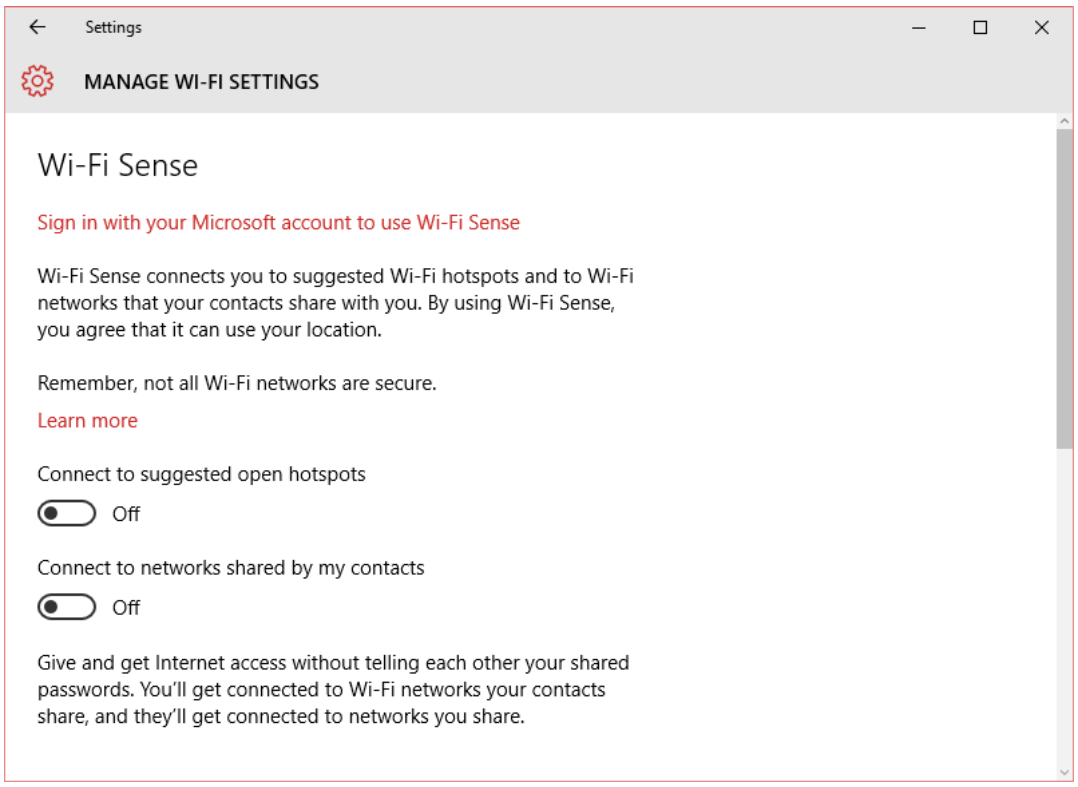


Figure 1: Wi-Fi Sense

Features like Wi-Fi Sense have been available since Windows Phone 8.1, but its appearance in Windows 10 is a first for Microsoft's desktop operating systems, and its inclusion has drawn some criticism from people concerned about their privacy. In May, 2016, Microsoft announced that Wi-Fi Sense was being discontinued due to high costs, coupled with low demand and usage[7].

---

[5] Microsoft. "About Wi-Fi Sense." Microsoft Privacy. https://privacy.microsoft.com/en-us/windows-10-about-wifi-sense

[6] Microsoft. "Sign in with a Microsoft account." Microsoft Support. https://support.microsoft.com/en-us/help/17201/windows-10-sign-in-with-a-microsoft-account

[7] Aul, Gabe. "Announcing Windows 10 Insider Preview Build 14342." Published May 10, 2016. Microsoft Windows Experience Blog. https://blogs.windows.com/windowsexperience/2016/05/10/announcing-windows-10-insider-preview-build-14342/

Kid's Corner

Another discontinued feature is Kid's Corner[8]. Originally introduced as part of Windows Phone 8.1 (and continued in Windows 10 Mobile), the Kid's Corner provided parents with a way to lock-down their smartphones so that children could only access specific, parent-approved apps and media content.

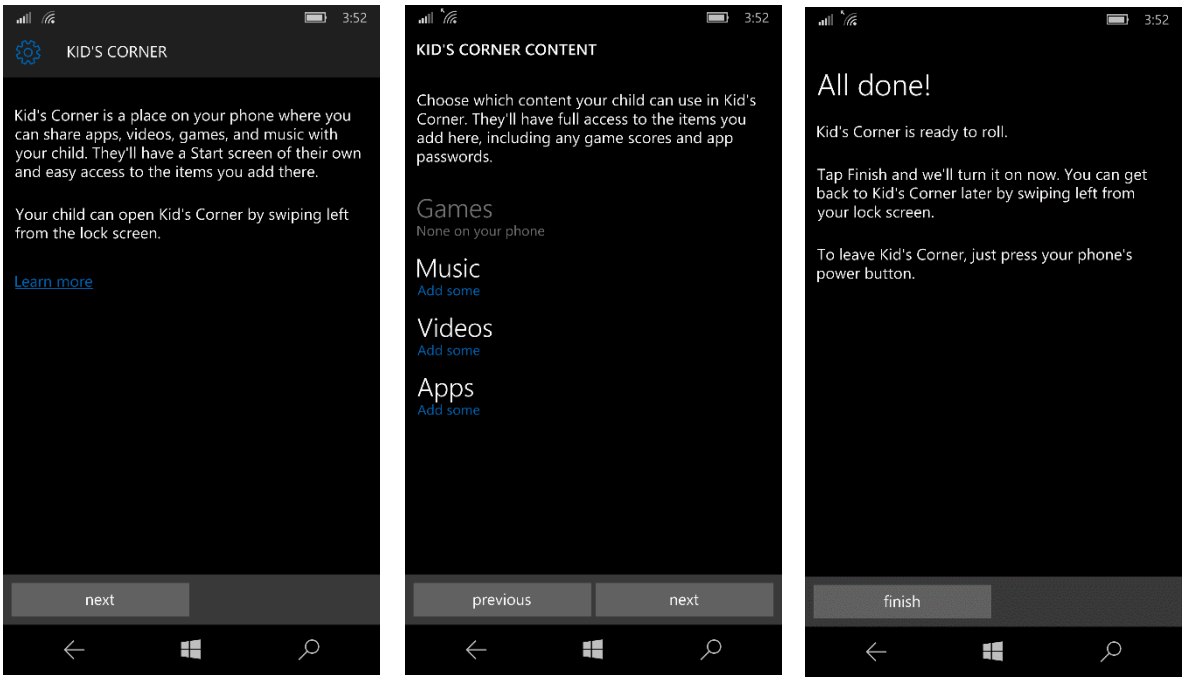


Figure 2: Kid's Corner

Apple and Google have offered basic versions of this feature in the form of Guided Access for the iPhone and restricted profiles for Android, and ESET has its own parental control offering, so while Microsoft's Kid's Corner was not a unique feature per se, it did provide an integrated option for parents wanting to control their children's experience on Windows smartphones[9,10,11]. As with Wi-Fi Sense, Microsoft indicated lack of use as the reason for ceasing further development of this feature for the Windows 10 Anniversary Update[12].

[8] Microsoft. "Set up and use Kid's Corner." Microsoft Support. https://blogs.windows.com/windowsexperience/2016/05/10/announcing-windows-10-insider-preview-build-14342/

[9] Apple. "Use Guided Access with iPhone, iPad, and iPod touch." Published Apr. 25, 2016. Apple Support. https://support.apple.com/en-us/HT202612

[10] Google. "Use restricted profiles on tablets." Nexus Help. https://support.google.com/nexus/answer/3175031?hl=en

[11] ESET. "Parental Control for Android." ESET. https://www.eset.com/int/home/parental-control-android/

[12] Sarkar, Dona. "Announcing Windows 10 Insider Preview Build 14367 for PC and Mobile." Published Jun. 16, 2016. Microsoft Windows Experience Blog. https://blogs.windows.com/windowsexperience/2016/06/16/announcing-windows-10-insider-preview-build-14367-for-pc-and-mobile/

The company did suggest as a replacement its Apps Corner feature, which provides basic control over running apps[13]. Like Kid's Corner, Apps Corner was introduced in Windows Phone 8.1 and included in Windows 10 Mobile. Another small change that will help parents is that Age Ratings, once considered optional, are mandatory for apps in the Windows Store as of September 2016[14,15].

App-V and UE-V

While not purely security features themselves, Application Virtualization (App-V) and User Experience Virtualization (UE-V) allow businesses to virtualize programs and user state data, respectively, by allowing them to be stored on a server instead of the end user's computer[16,17]. Previously, these features worked on Windows 10 Pro, but as of the Windows 10 Anniversary Update, they are now only available for Windows 10 Enterprise and Education[18].

What's Been Changed

For a lot of people, the first thing they think of when you mention computer security is anti-malware software. For some people, the basic anti-malware program bundled with Windows, namely Windows Defender, is the first anti-malware program they think of, which is understandable since it comes bundled with Windows. We discussed Windows Defender extensively in We Live Security's *In-Depth Review and Analysis of Windows 10 Security and Privacy* (blog, white paper), and while the Anniversary Update brings only incremental changes to Windows Defender, some of them may have a big impact on the stability and reliability of your system.

Group Policy

Using the Group Policy Editor (or the Registry Editor) has long been a way for administrators, IT pros and power users to change the behavior of the Windows operating system. With the Anniversary Update, Microsoft has made changes to Group Policy so Windows 10 Pro users can no longer block Windows Store tips, tricks and suggestions[19]. Changing the policy for Microsoft consumer experiences, which is the policy responsible for your seeing Candy Crush Saga, Twitter and other third-party Windows apps, is also blocked in Windows 10 Pro[20]. This follows up changes made in November 2015 with v1511 (Build

---

[13] Microsoft. "Set up Apps Corner." Microsoft Support. https://support.microsoft.com/en-us/instantanswers/7959c547-aa80-5ff1-9097-1784b6894845/set-up-apps-corner

[14] Microsoft. "Age ratings." Windows Dec Center. https://msdn.microsoft.com/en-us/windows/uwp/publish/age-ratings

[15] Zamora, Bernardo. "Now Available: Single age rating system to simplify app submissions." Published Jan. 6, 2016. Microsoft Windows Developer Blog. https://blogs.windows.com/buildingapps/2016/01/06/now-available-single-age-rating-system-to-simplify-app-submissions/

[16] Microsoft. "Application Virtualization." Microsoft TechNet. https://technet.microsoft.com/en-us/windows/hh826068

[17] Microsoft. "User Experience Virtualization." Microsoft TechNet. https://technet.microsoft.com/en-us/windows/hh943107

[18] Hornbeck, J.C. "App-V and UE-V to be included with Windows." Published Jul. 5, 2016. Official Microsoft App-V Team Blog, The. https://blogs.technet.microsoft.com/appv/2016/07/05/app-v-and-ue-v-to-be-included-with-windows/

[19] Decker, J. "Manage Windows 10 and Windows Store tips, tricks, and suggestions." Published Aug. 8, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/itpro/windows/manage/manage-tips-and-suggestions

[20] Niehaus, Michael. "Seeing extra apps? Turn them off." Published Nov. 23, 2015. Michael Niehaus' Windows and Office Deployment Ramblings Blog. https://blogs.technet.microsoft.com/mniehaus/2015/11/23/seeing-extra-apps-turn-them-off/

10586) of Windows 10 where the blocking of Windows Store was disabled in Windows 10 Pro[21]. While the options are still visible in the Group Policy Editor under Windows 10 Pro, changing them has no effect on the behavior of that operating system.

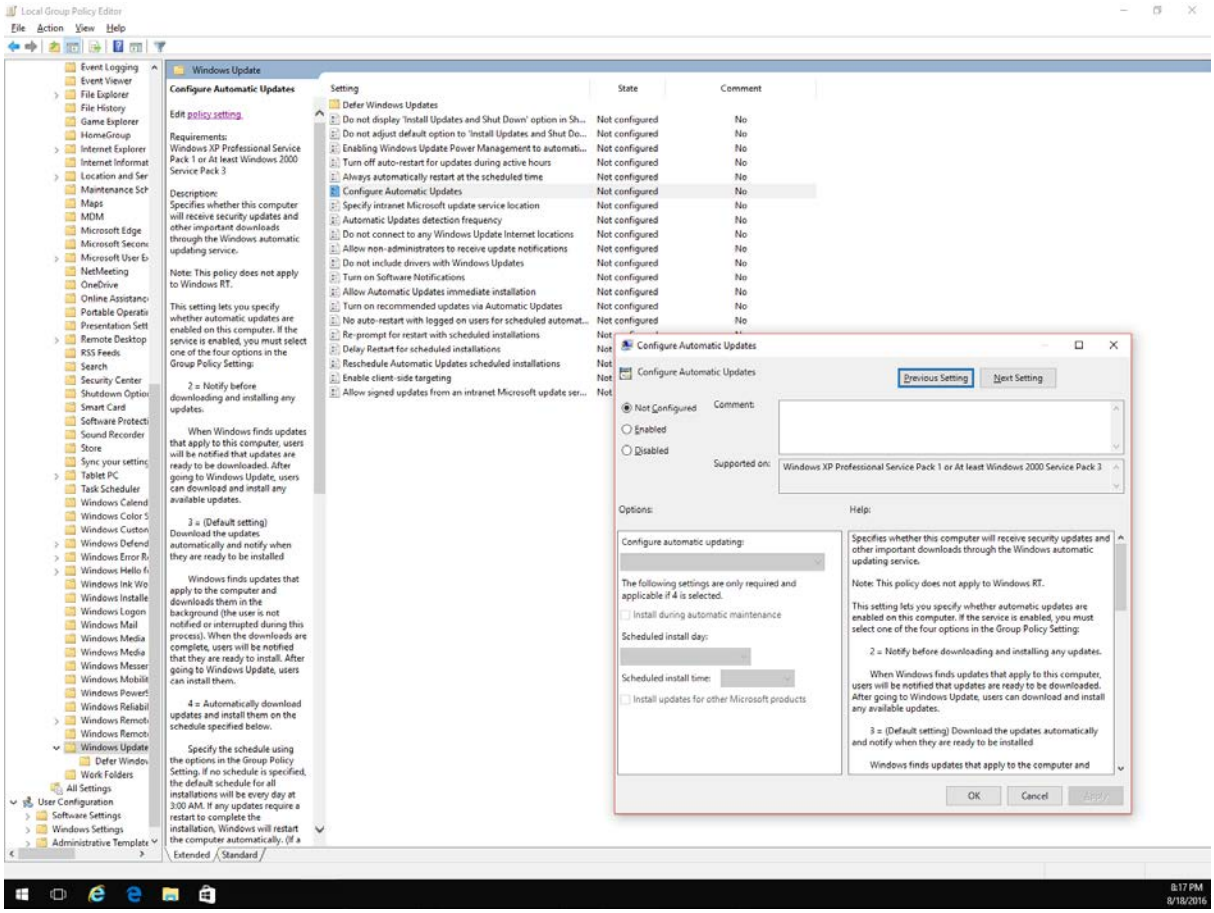


Figure 3: Group Policy Editor

While it is understandable that Microsoft would want to relegate such changes to customers with licenses for Windows 10 Pro and Education, there is always the risk that allowing end users to interact with third-party code could introduce system compromise, if not directly through malware then by increasing the system's attack surface via third-party code.

PIN-based Login

One of the features introduced in Windows 10 was PIN sign on, backed by Windows Hello. This allowed both home and enterprise customers to log into their computers using a secure PIN code. In the Windows 10 Anniversary Update, this feature is now disabled by default on domain-joined computers[22].

[21] Hakala, Trudy. "Configure access to Windows Store." Published Sep. 1, 2016. Microsoft TechNet. https://technet.microsoft.com/en-us/itpro/windows/manage/stop-employees-from-using-the-windows-store

[22] de Zylva, Ash. "Changes to Convenience PIN / Windows Hello Behavior in Windows 10 Version 1607." Published Aug. 13, 2016. Ash's Blog. https://blogs.technet.microsoft.com/ash/2016/08/13/changes-to-convenience-pin-and-thus-windows-hello-behaviour-in-windows-10-version-1607/

While not a major change, it is likely indicative that Microsoft's enterprise customers prefer complex passwords to PINs. Given that generating complex PINs has its own set of challenges—which differ slightly from passwords and problems with re-use by end users—this is not surprising[23].

Windows Defender

Microsoft wants Windows Defender to compete in the consumer and enterprise spaces, both in terms of quality and completeness of protection, and has been steadily working on improving its scores in tests by independent certification, by comparative and testing agencies. It seems the days of Microsoft saying its anti-malware solution is "*merely a 'baseline' that will 'always be on the bottom' of antivirus software rankings*" are firmly behind it, but whether it can become a top contender has yet to be seen[24]. A look at how Windows Defender's options have changed between Builds 10586 and 14393 shows how Microsoft has begun the process of transitioning from mere baseline into a competitive product offering.

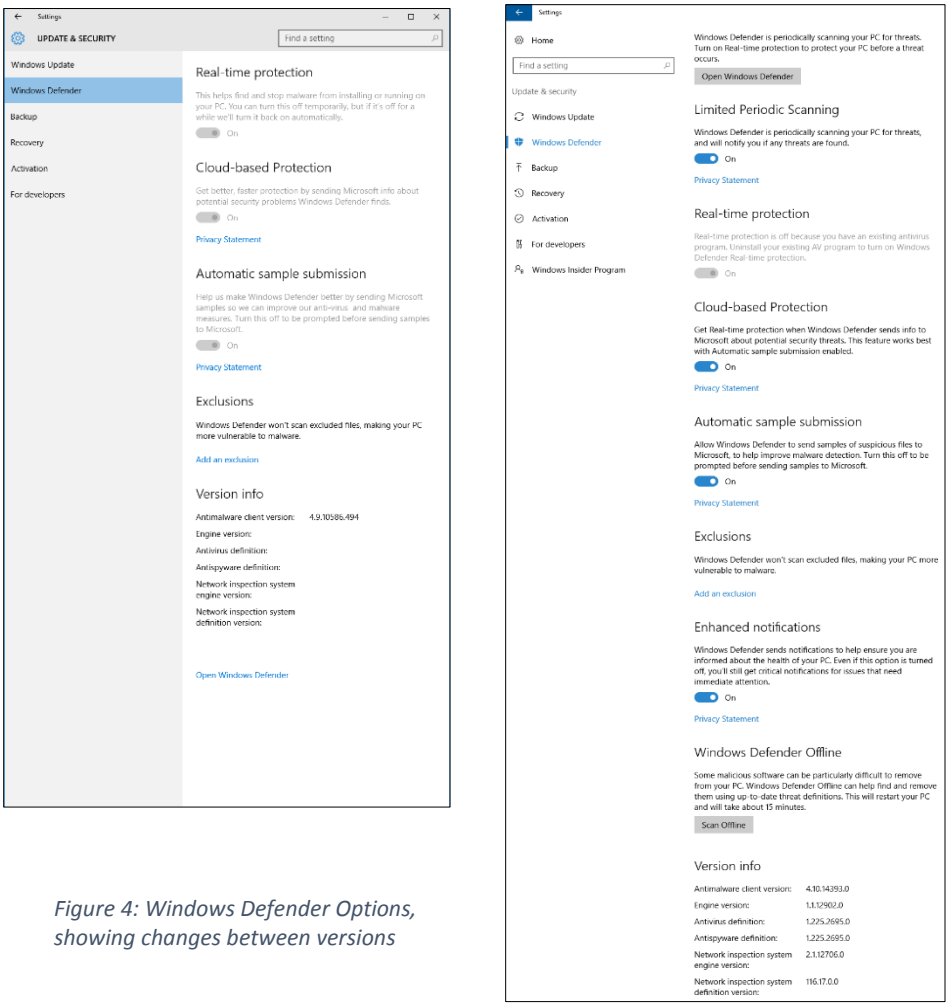


Figure 4: Windows Defender Options, showing changes between versions

[23] Goretsky, Aryeh. "Passwords and PINs: The Worst Choices." Recorded Nov. 6, 2013. BrightTalk - ESET Internet Security Threats Channel. https://www.brighttalk.com/webcast/1718/87601

[24] Kobie, Nicole. "Microsoft: Security Essentials is designed to be bottom of the antivirus rankings." Published Sep. 25, 2013. PC Pro [archived by Internet Archive Wayback Machine]. http://web.archive.org/web/20130925183000/http:/www.pcpro.co.uk/news/security/384394/microsoft-security-essentials-is-designed-to-be-bottom-of-the-antivirus-rankings

Features and Options

Although it still has quite some way to go before becoming as feature-filled as other free anti-malware programs, it is clear Microsoft is making progress on this front.

One of the improvements is Windows Defender's new offline scan mode. Previously, people had to download a separate program called Windows Defender Offline (WDO) in order to create a bootable CD, DVD or USB flash drive to scan a computer independent of the operating system[25]. In the Anniversary Update, WDO has been integrated into Windows Defender. Clicking on **Scan Offline** causes Windows 10 to reboot into a kind of safe mode from which only Windows Defender runs.

While this is not a new feature to anti-malware software by any means (ESET has had this since 2008, and the current incarnation can be downloaded here) it again shows how Microsoft is trying to make Windows Defender more competitive by making its advanced functions easier to configure[26].

Figure 5: Windows Defender

Fast Ring Builds

As the Anniversary Update to Windows 10 got closer to being released, some of the builds in the Fast Ring would notify users that Windows Defender is the recommended antivirus software. This might be a bit puzzling given that Microsoft has over three dozen trusted partners for anti-malware software according to its own website, including ESET[27,28,29]. But there is actually some logic behind this behavior.

Fast Ring builds are often short-lived in nature, sometimes only available for a day or two, and released by Microsoft specifically to test new features and get feedback on how changes made to the operating system are perceived and so forth. As such, they are often incomplete and can break existing applications, including security software.

Anti-malware developers may sometimes add support for Fast Ring builds, but doing so may be difficult or impossible on a consistent basis, especially given the short amount of time some Fast Ring builds are

[25] Microsoft. "Help protect my PC with Windows Defender Offline." Published Sep. 9, 2016. Microsoft Support. https://support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc
[26] Marcos. "ESET Smart Security v4 beta available for testing." Published Nov. 18, 2008. Wilders Security Forums. http://www.wilderssecurity.com/threads/eset-smart-security-v4-beta-available-for-testing.225559/
[27] Microsoft. "Consumer antivirus software providers for Windows." Published May 26, 2016. Microsoft Support. https://support.microsoft.com/en-us/help/18900/consumer-antivirus-software-providers-for-windows
[28] Microsoft. "Virus Information Alliance Membership Eligibility." Microsoft Malware Protection Center. https://www.microsoft.com/en-us/security/portal/mmpc/via/via-criteria.aspx
[29] Microsoft. "Microsoft Active Protections Program Criteria." Microsoft TechNet Security TechCenter. https://technet.microsoft.com/en-us/security/dn527821.aspx

available. Since Fast Ring builds are not stable and are for short term use only, it makes sense to use Windows Defender as a stop-gap security solution.

Limited Periodic Scanning

A new feature, *Limited Periodic Scanning*, allows Windows Defender to run an on-demand scan occasionally in the background, even when a third-party anti-malware software is already installed[30]. This is actually a form of "second opinion scanner" and the concept has been around for a long time. Microsoft has offered its own Malicious Software Removal Tool for over 10 years now, and it is downloaded and run automatically by default each month when Windows Updates are installed[31]. Other anti-malware companies have similar tools, including ESET, which has offered its free ESET Online Scanner for several years[32]. When it comes down to it, free anti-virus programs date back to the 1980s, although usually with limited feature sets, advertising, or as sponsored "freemium" applications in order to encourage the use and purchase of their commercial versions.

NOTE: Because of the possibility, no matter how slight, of conflicts and performance issues, ESET does *not* recommend using Windows Defender's Limited Periodic Scanning feature in conjunction with ESET's software on the same computer.

For the latest information about using Windows Defender and ESET's software on Windows 10, see ESET Support News Article #6148, *Windows Defender suggests that you disable ESET in Windows 10 Anniversary Update*.

Detection Issues

As previously mentioned, Microsoft has been steadily working towards improving its scores in independent test results. The company has had success in moving its detection from a "baseline" status to a more competitive footing, but not without cost. Microsoft's improvements to detection mean that Windows Defender no longer shows up at the bottom of detection test results as it has in the past, but there has also been an increase in false positive detections, as noted in recent tests by independent testing firms, like this one from SE Labs[33].

INTERACTION RATINGS			
Product	**Click to block (default block)**	**None (allowed)**	**None (blocked)**
AVG AntiVirus Free Edition	0	100	0
Kaspersky Internet Security	0	100	0
McAfee Internet Security	0	100	0
ESET Smart Security 9	0	100	0
Trend Micro Internet Security 11	0	100	0
Avast Free Antivirus	0	99	1
Norton Security	0	99	1
G DATA Internet Security	1	99	0
Microsoft Security Essentials	0	98	2

Source: *"Home Anti-Malware Protection: October-December 2016." SE Labs.*

[30] Microsoft. "Limited Periodic Scanning in Windows 10 to Provide Additional Malware Protection." Published May 26, 2016. Microsoft Threat Research & Response Blog. https://blogs.technet.microsoft.com/mmpc/2016/05/26/limited-periodic-scanning-in-windows-10-to-provide-additional-malware-protection/

[31] Microsoft. "Malicious software Removal Tool." Microsoft Safety & Security Center. https://www.microsoft.com/en-us/safety/pc-security/malware-removal.aspx

[32] ESET. "ESET Online Scanner." https://www.eset.com/online-scanner/

[33] SE Labs. "Home Anti-Malware Protection: January-March 2016." Published May 30, 2016. https://selabs.uk/download/consumers/january-march-2016-consumer.pdf.

This issue can be seen in a range of tests by independent testing firms including AV-Comparatives and AV-TEST [34,35,36,37,38,39,40,41]. This is particularly troubling given Windows Defender's long history of *not* having any significant false positive alarms. Microsoft will need to expend significant engineering resources to move its detection capabilities closer to the top as well as to get the number of false positives back down to a manageable level, which is arguably a more difficult task than detecting malware in the first place.

Microsoft Edge

While Microsoft has not announced any specific security-related changes to its new web browser, support for third-party extensions such as password managers and ad blockers is being made available in the Windows 10 Anniversary Update[42]. While only a handful of extensions were available during the Windows Insider Preview beta test leading up to the Windows 10 Anniversary Update, it seems likely that additional privacy and security extensions will become available in Edge as they are in Google Chrome and Mozilla Firefox.

Driver Signing

While not an end-user feature *per se*, Microsoft is now requiring that fresh installations of the Windows10 Anniversary Update load kernel mode drivers signed by Microsoft through its Windows Hardware Developer Center portal[43,44]. Right now, this only applies to new installations of Windows 10 Anniversary Update.

---

[34] AV-Comparatives. "File Detection Test March 2016." Published Apr. 15, 2016. http://www.av-comparatives.org/file-detection-test-march-2016/.
[35] AV-TEST. "23 Security Suites Put to the Test Under Windows 7." Published Oct. 13, 2016. https://www.av-test.org/en/news/news-single-view/23-security-suites-put-to-the-test-under-windows-7/
[36] AV-Comparatives. "File Detection Test September 2016." Published Oct. 14, 2016. https://www.av-comparatives.org/real-world-protection-test-september-2016/.
[37] AV-TEST. "AV-TEST Product Review and Certification Report – May-Jun/2016: Microsoft Windows Defender." https://www.av-test.org/en/antivirus/home-windows/windows-8/june-2016/microsoft-windows-defender-4.8-162247/.
[38] AV-TEST. "Test: 12 Security Solutions for Corporate Networks and Windows 7 Clients." Published Oct. 19, 2016. https://www.av-test.org/en/news/news-single-view/test-12-security-solutions-for-corporate-networks-and-windows-7-clients/.
[39] AV-Comparatives. "Real-World Protection Test October 2016." Published Nov. 10, 2016. https://www.av-comparatives.org/wp-content/uploads/2016/11/avc_factsheet2016_10.pdf
[40] AV-TEST. "Test: This is how well 8 security packages and 7 special tools come to the rescue after a virus attack." Published Dec. 5, 2016. https://www.av-test.org/en/news/news-single-view/test-this-is-how-well-8-security-packages-and-7-special-tools-come-to-the-rescue-after-a-virus-atta/.
[41] SE Labs. "Home Anti-Malware Protection: October-December 2016." Published Jan. 10, 2017. https://selabs.uk/download/consumers/oct-dec-2016-consumer.pdf.
[42] Microsoft. "Customize Microsoft Edge with Extensions!" Microsoft Developer Technologies. https://developer.microsoft.com/en-us/microsoft-edge/extensions/
[43] Baxter, Joshua. "Driver Signing changes in Windows 10, version 1607." Published Jul. 26, 206. Microsoft Windows Hardware Certification Blog. https://blogs.msdn.microsoft.com/windows_hardware_certification/2016/07/26/driver-signing-changes-in-windows-10-version-1607/
[44] Microsoft. "Dashboard." Windows Hardware Dev Center. https://sysdev.microsoft.com/en-US/hardware/member/

Computers upgraded from an older version of Windows — including previous builds of Windows 10 — will still to be able to load kernel drivers that are cross-signed by Microsoft, and kernel drivers that were cross-signed more than one year ago (July 29, 2015) will continue to load as well. Also, if Secure Boot is disabled (or not present), cross-signed drivers will also continue to load[45].

This is a security feature to help prevent malicious drivers from being loaded at boot time. While it may seem like an esoteric security step, it will improve Windows 10's security against certain types of sophisticated malware such as rootkits that make use of kernel mode drivers.

Privacy

While not a security issue, many readers of We Live Security have commented on Microsoft's practice of collecting telemetry and use of it in Windows 10. While Microsoft has not announced any substantial changes to this practice, they have provided more information about the Windows components that communicate with Microsoft, as well as how to disable these communications. This information can be found in the drily-named Microsoft TechNet article, *Manage connections from Windows operating system components to Microsoft services*[46].

Note that the ability to disable telemetry collection from Windows 10 components varies by edition, with the Enterprise and Education editions having the most flexibility as to what can be disabled.

Other Considerations

As with any software as complex as an operating system, Windows 10 Anniversary Upgrade is not without its problems, some of which may have some security implications, depending upon your use of the operating system:

- Some people have reported that Windows no longer recognizes volumes on their drives after installing the Windows 10 Anniversary Update. This has been reported in multiple places around the Internet including tech news sites such as Neowin, reddit and Microsoft's own support forums. The issue is not limited to a particular brand or drive, and affects both internal drives and external USB drives[47,48,49].

  If you work with external drives for swapping data between computers as part of your backup strategy or for other reasons, you may wish to hold off installing the Windows 10 Anniversary

[45] Goretsky, Aryeh. "A white paper: Windows 8's Security Features." Published Oct. 9, 2012. ESET We Live Security Blog. http://www.welivesecurity.com/2012/10/09/windows-8s-security-features/

[46] Lich, Brian. "Manage connections from Windows operating system components to Microsoft services." Published Sep. 23, 2016. Microsoft Windows IT Center – Manage. https://technet.microsoft.com/itpro/windows/manage/manage-connections-from-windows-operating-system-components-to-microsoft-services

[47] Dragontology. "Win10 AU can't read external FAT32 HDD; Win7 can." Published Aug. 5, 2016. Neowin Forums. https://www.neowin.net/forum/topic/1304856-win10-au-cant-read-external-fat32-hdd-win7-can/

[48] Signians. "[BUG] Windows 10 Anniversary Update Tanked Secondary Data Drive." Published Aug. 3, 2016. Reddit. https://www.reddit.com/r/Windows10/comments/4vyifo/bug_windows_10_anniversary_update_tanked/

[49] IanMcKeaveney, ""Partition won't mount after Windows 10 Anniversary Update." Published Aug. 2, 2016. Microsoft Windows Community. http://answers.microsoft.com/en-us/windows/forum/windows_10-files/partition-wont-mount-after-windows-10-anniversary/eff0ea6f-4c2c-4991-817e-4123d933e81e?auth=1

Update, or roll back to Windows 10 v1511/Build 10580 until the problem is resolved, which has not yet occurred as of the time of this writing. A Microsoft employee in the company's support forum acknowledged the issue, while an engineer reported that the root cause has been identified and a fix is being tested [50,51].

Keep in mind that even if Windows 10 can no longer read the drive, the files on it are still present. While there are numerous reports of using third-party tools to safely make the disks recognizable again by Windows 10, it may be better to wait for Microsoft to offer an official fix, especially if the drives in question are part of your backup or continuity-of-business operations.

- Another issue that has been reported is that many models of webcam no longer work after Windows 10 Anniversary Update is installed because support for some commonly-used video compression formats was withdrawn. Tech journalist Brad Sams of Thurrott Daily provides a high-level explanation of the problem initially reported in Microsoft's support forums as well as a potential workaround [52,53]. As of the time of this writing, Microsoft has reported that they believe the issue has been fixed; however, some customers continue to report webcam problems[54].

  While the issue specifically mentions USB-attached webcams and TV tuners, these types of devices are used in security camera systems and could possibly affect watching and recording video. As with the missing disk volume problem, rolling back to the previous build of Windows 10 is a temporary workaround until a complete solution is available.

- BitLocker, Microsoft's full disk encryption program, is subject to some issues which may present difficulties for some enterprises:

---

[50] Srinivasa, Sharath. "Partitions may be missing after installing the Anniversary Update." Published Aug. 11, 2016. Microsoft Windows Community. http://answers.microsoft.com/en-us/windows/forum/windows_10-files/partitions-may-be-missing-after-installing-the/ffafb34b-df6e-4c61-927d-babf29b46b87

[51] Dudgikar, Mahesh R. "[BUG] Windows 10 Anniversary Update Tanked Secondary Data Drive." Published Aug. 16, 2016. https://www.reddit.com/r/Windows10/comments/4vyifo/bug_windows_10_anniversary_update_tanked/d6ksjbg

[52] Less_Is_More. "MJPG encoded media type is not available for USB/UVC web-cameras after Windows 10 version 1607 (OS Build 14393.10 'anniversary)) update." Published Aug. 8, 2016. Microsoft Media Foundation Development for Windows Desktop Community. https://social.msdn.microsoft.com/Forums/windowsdesktop/en-US/9d6a8704-764f-46df-a41c-8e9d84f7f0f3/mjpg-encoded-media-type-is-not-available-for-usbuvc-webcameras-after-windows-10-version-1607-os?forum=mediafoundationdevelopment

[53] Sams, Brad. "Microsoft Has Broken Millions of Webcams With Windows 10 Anniversary Update." Published Aug. 19, 2016. https://www.thurrott.com/windows/windows-10/76719/microsoft-broken-millions-webcams-windows-10-anniversary-update

[54] Mike M. " MJPG encoded media type is not available for USB/UVC web-cameras after Windows 10 version 1607 (OS Build 14393.10 'anniversary) update." Published Oct. 27, 2016. Microsoft Media Foundation Development for Windows Desktop Community. https://social.msdn.microsoft.com/Forums/en-US/mediafoundationdevelopment/thread/9d6a8704-764f-46df-a41c-8e9d84f7f0f3/#e5f330ba-97fd-44e1-9eda-0c0cd748a4d8

- At Windows 10's release, Microsoft announced protection against DMA (direct memory access) attacks, which could be used to recover BitLocker's passphrase while the computer is still booting Windows 10[55,56,57]. While this is correct—the mitigation was introduced in Windows 10 Build 1507—the *default* operation is to allow DMA access, and the option can only be managed through MDM (mobile device management) policies using a product like Windows Intune[58,59].

- BitLocker full disk encryption is temporarily disabled when upgrading to the Windows 10 Anniversary Update. While this is normal behavior during operating system upgrades, Finnish computer security researcher Sami Laiho discovered that pressing `Shift+F10` during the update opens a **Command Prompt** (filename: `CMD.EXE`) running under the SYSTEM account, which has control of all files and services in Windows[60].

  Originally intended as a debugging tool when installing or upgrading to a new version of Windows, its presence opens a computer to data exfiltration or attack using a mechanism not normally present during an upgrade. Taking advantage of this does require physical access to the computer; however, companies often have branch offices or telecommuting employees where the environment cannot be closely monitored. While Microsoft does suggest that customers affected by these issues go back to Build 10586, some may no longer be able to: One of the changes introduced in the Windows 10 Anniversary Update was to reduce the length of time the previous build of Windows 10 is saved from thirty (30) to just ten (10) days, after which the old build is removed to free up space[61]. If reinstalling the older build is not an option, people may have to try the workarounds mentioned above while they wait for the final fixes to be delivered by Microsoft.

---

[55] Lich, Brian. "BitLocker Countermeasures." Published May 31, 2016. Microsoft Windows IT Center. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/bitlocker-countermeasures

[56] Lich, Brian. "Choose the right BitLocker countermeasure." Published May 31, 2016. Microsoft Windows IT Center. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/choose-the-right-bitlocker-countermeasure

[57] Hakala, Trudy. "What's new in Windows 10, versions 1507 and 1511." Published Nov. 29, 2016. Microsoft TechNet. https://technet.microsoft.com/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511#bitlocker

[58] Laiho, Sami. "DIY – penetration testing Windows environment." Published Sep. 29, 2016. Microsoft Ignite. https://www.youtube.com/watch?v=OtwT311mlwc

[59] Microsoft. "Policy CSP: DataProtection/AllowDirectMemoryAccess." Published Nov. 29, 2016. Microsoft Hardware Dev Center. https://msdn.microsoft.com/windows/hardware/commercialize/customize/mdm/policy-configuration-service-provider?f=255&MSPPError=-2147217396#dataprotection-allowdirectmemoryaccess

[60] Laiho, Sami. "Every Windows 10-in-place Upgrade is a SEVERE Security risk." Published Nov. 28, 2016. Win-Fu Official Blog. http://blog.win-fu.com/2016/11/every-windows-10-in-place-upgrade-is.html

[61] Hay, Richard. "Microsoft Shortens Recovery Rollback Period to 10 Days in Windows 10 Anniversary Update." Published Aug. 3, 2016. SuperSite for Windows. http://winsupersite.com/windows-10/microsoft-shortens-recovery-rollback-period-10-days-windows-10-anniversary-update

Closing Thoughts

Microsoft has made some genuine headway in improving Windows 10's security in its first anniversary update, removing little-used features and improving others. However, some changes take away security functionality that was previously available in the editions of Windows 10 most available to consumers and small businesses.

Microsoft's recommendation of Windows Defender as a "second opinion scanner" may be problematic, given concerns about compatibility issues and false positives. People following the recommendation to switch to it as their default protection may be decreasing the overall security of their computers: If Windows Defender does detect something during its "second opinion" scan that is not detected by installed third-party anti-malware software, it could be due to a false positive, or a conflict of some sort. We recommend contacting both companies to ascertain whether or not it is not one of these issues.

Despite the potential for increased false positive alarms with Windows Defender, it is still a good idea to install the Windows 10 Anniversary Upgrade for the security improvements it provides. If you perform a clean install of this new version of Windows 10, your computer will be able to take advantage of the improvements in driver signing. This will have to be carefully balanced against the amount of effort required to reinstall applications and restore data from backups.

The improvements to security in the Windows 10 Anniversary Update make it a useful upgrade for both consumers and businesses; however, the security issues noted in the *Other Considerations* section, above, mean that the Windows 10 Anniversary Update should not be treated as a simple upgrade, but instead needs to be carefully monitored.

Consumers should test as many applications and common activities as possible during the first week that Windows 10 Anniversary Update is installed, so that in the event that it is not compatible with a periodic task, the computer can be rolled back to its previous version of Windows before that is erased.

Businesses will likely want to take a phased roll-out approach to deploying groups, with each group being carefully monitored over a long enough period to ensure the Windows 10 Anniversary Update does not interfere with daily activities involving line-of-business software as well as activities which may be performed on a less frequent basis, for instance, weekly or monthly.

Businesses using BitLocker with branch offices or remote workers may wish to withhold upgrading to the Windows 10 Anniversary Update until it can be done with trusted IT staff on site, or computers come in from the field to a trusted location.

For More Information

For more information on Windows 10, see the following blog posts and articles:

- Windows Exploitation in 2016
- Windows 10 security and privacy: an in-depth review and analysis
- Should I stay or should I go… to Windows 10?
- Windows 10, Privacy 0? ESET deep dives into the privacy of Microsoft's new OS
- Will Windows 10 leave enterprises vulnerable to zero-days?

NOTE: ESET recommends installing the latest version of its software before installing the Windows 10 Anniversary Update in order to ensure your computer has the latest protection and up-to-date digitally-signed files. For instructions on how to do so, see ESET Knowledgebase Article #2476, *How do I upgrade my ESET Windows home product to the latest version?*

For instructions on how to install the Windows 10 Anniversary Update on a computer already running ESET's software, see ESET Knowledgebase Article #3747, *How do I upgrade to Windows 10 with my ESET software installed?*

For a list of issues with Windows 10 and their workarounds, see ESET Knowledgebase Article #3733, *Known issues with ESET products and Windows 10*.

Acknowledgements and Contact Information

The author would like to thank his colleagues Artem Baranov, Ranson B., Bruce P. Burrell, Stephen Cobb, Nick FitzGerald, David Harley, Miroslav J., Martin K., Marek L., Anne M., Fer O'Neil, Ignacio S. and Righard Zwienenberg for their contributions and feedback. Special thanks to Sami Laiho of Adminize for discussing his research into BitLocker. Special thanks also to Lenovo for providing access to pre-release drivers for Windows 10, and to Microsoft for providing access to pre-release versions of Windows 10 and answering questions which came up during this research. Thanks also to VMware for the virtualization technology used while preparing this paper.

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

Aryeh Goretsky, MVP, ZCSE
Distinguished Researcher