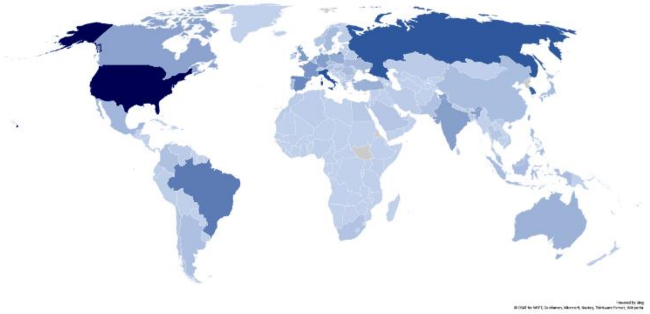
Windows

Next-gen ransomware protection with Windows 10 Creators Update

Ransomware is the most widespread digital threat to safety and productivity today. Its impact is felt around the world, across the full spectrum of computer users – from home users who might lose their ability to perform day-to-day Internet activities, to organizations whose business operations can be immobilized by ransomware infection.

The global scale of ransomware 2017


Powered by Bing
© DSAT for MSFT, GeoNames, Microsoft, Navteq, Thinkware Extract, Wikipedia

Multiple high-profile incidents have demonstrated that ransomware can have catastrophic effects on critical public and private services. Hospitals, transport systems, and other high-tech facilities across the globe have been affected.

Ransomware exemplifies the scale and complexity of cyberthreats that continuously assault computers, networks, and infrastructures. Traditional, signature-based solutions cannot scale or respond to the complexity of these types of advanced attacks.

At Microsoft, guided by our mission to empower every person and organization on the planet to achieve more, we continually strive to improve customer protection against threats like ransomware. We do this by building products and services that are designed with security in mind.

Security features built into Windows 10 reflect our next-generation, predictive approach to security. We use and develop technologies that are front and center in the evolution of malware prevention, protecting customers from threats they face today, as well as those that will emerge in the future.

Traditional, signature-based solutions can't defeat advanced attacks. Security features built into Windows 10 reflect our next-generation, predictive approach to security.

We continually improve our ability to stop attacks dead in their tracks by blocking never-before-seen malware at first sight. We make use of the cloud and threat intelligence from a vast network of sensors to provide real-time protection against attacks. Out of all malware blocked by Windows Defender Antivirus (Windows Defender AV), 99.992% were detected and blocked by machine learning and behavioral analysis, guided by expert threat research.

In this paper, we outlined the comprehensive next-gen protection components in Windows 10 Creators Update that help keep our customers safe from ransomware.

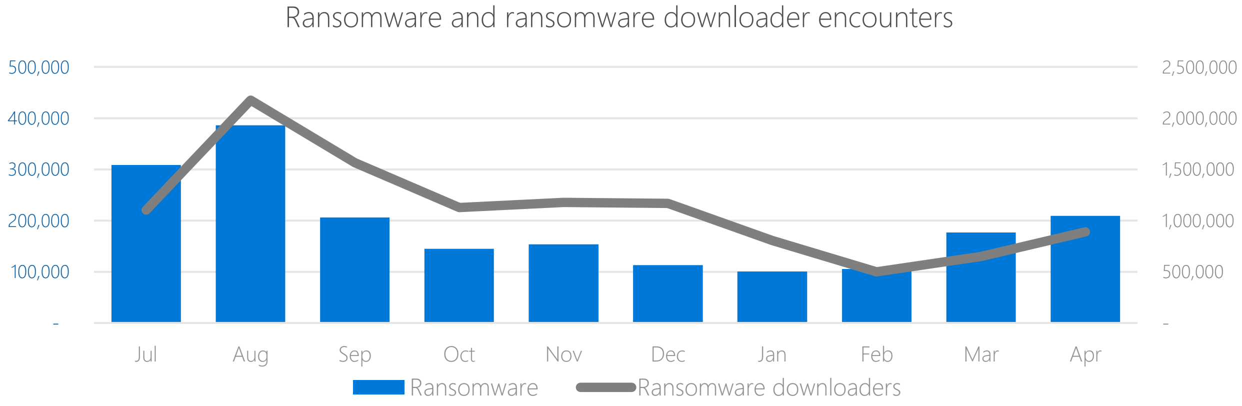
Ransomware in 2017: Growing in sophistication and reach

Over the last few years, ransomware has rapidly evolved into one of the most lucrative revenue channels for cybercriminals. Reports estimate that ransomware operators earned $1B in 2016 from ransom paid by victims.

Ransomware's low-risk-high-reward method of illegally extorting money comes from perpetrators' ability to:

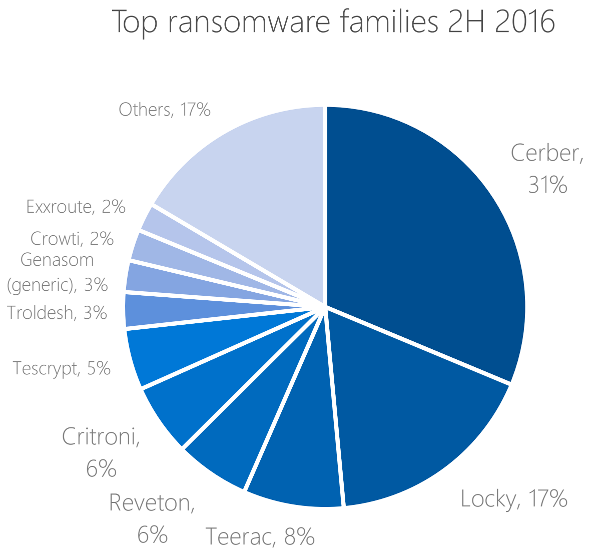
- Hide behind various command-and-control (C&C) servers
- Run nearly untraceable transactions using cryptocurrency, such as Bitcoin

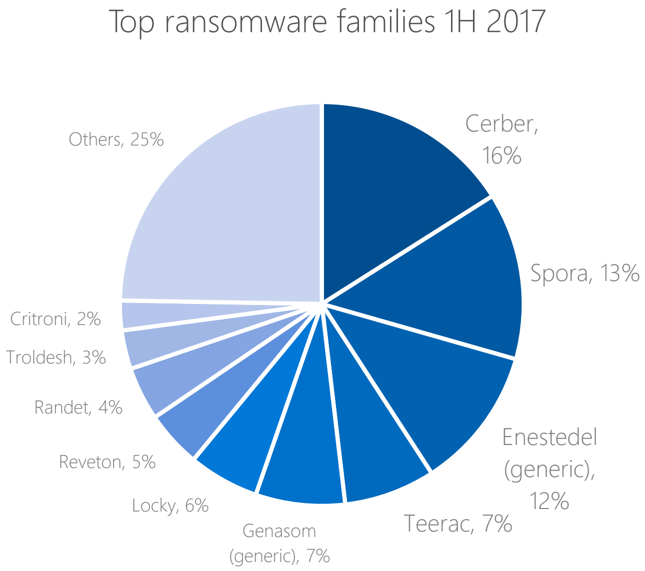
Ransomware-as-a-service (RaaS), which is a cybercriminal business model that makes the latest versions of ransomware available in underground marketplaces, accounts for a significant portion of ransomware and related Trojan downloaders, whose volume peaked in August 2016. We observed a downward trend towards the end of 2016, but the number of ransomware in the wild started to pick up again in February 2017.



Established ransomware operations like Cerber and Locky use RaaS to release new ransomware variants and continue to innovate in terms of distribution, functionality, and evasion.

In 2017, new ransomware families like Spora and WannaCrypt (also known as WannaCry) emerged with more complex behaviors, such as spreading capabilities and exploits. Spora, which surfaced in January, is already one of the most prevalent ransomware families today.





We also observed that ransomware operators have expanded to more ways of installing ransomware on target computers:

- **Browser** – Historically, ransomware operations heavily used exploit kits, which take advantage of browser vulnerabilities to download malware on vulnerable computers. However, there's been a sizeable decline in the use of drive-by downloads to install ransomware on computers.
- **Email** – The staple distribution channel continues to be email. Socially engineered emails carry Trojan downloaders that install ransomware payloads. Unfortunately, email distribution continues to prove effective in malware campaigns. Verizon's data breach investigation report in 2016 shows that if an attacker sends an email to 100 people in one company, 30 will open the email, and 12 will open the attachment or click the link.
- **Network** – Network propagation is not a typical ransomware behavior. However, new ransomware families like Spora have the capability to spread via mapped network drives and removable drives. We also observed new ransomware campaigns that start to use remote desktop services (RDP) brute force attacks to install ransomware on target machines. In 2017, we saw a ransomware family successfully use an exploit to propagate. WannaCrypt used a previously fixed Server Message Block (SMB) vulnerability to spread rapidly to out-of-date machines within a short span of time. WannaCrypt's use of an exploit gave it the ability to attain critical mass, impacting many out-of-date computers.

Active cybercriminal operations show that the threat of ransomware continues to evolve. Campaigns attempt to go unnoticed by operating for only a few hours, just enough time for some victims to pay the ransom. In addition, ransomware threats are increasingly more polymorphic and don't stop coming up with inventive ways to bypass both static and dynamic antivirus (AV) detections.

A multi-layered defense strategy is needed to fight the scale and sophistication of ransomware. At Microsoft, we are committed to delivering next-gen solutions like Windows Defender AV to provide a comprehensive defense stack against ransomware.

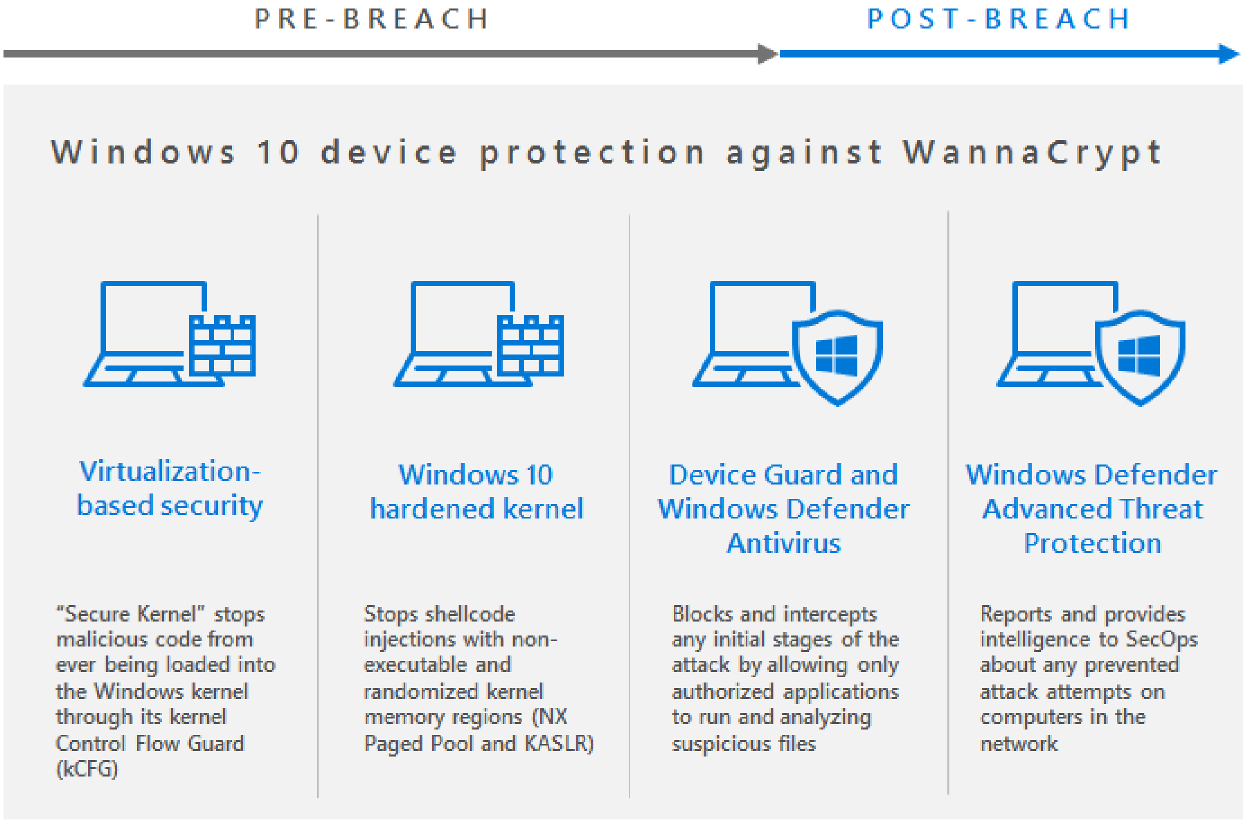
Windows 10 defense against WannaCrypt

The security posture of customers and the readiness of the security industry was tested in early May, when a new variant of WannaCrypt (also known as WannaCry) spread at speeds never before observed in ransomware.

The worm-like spreading capability is enabled by an exploit for an SMB vulnerability that was patched two months prior. Unfortunately, many computers around the world remained out-of-date and fell victim to this ransomware attack.

Windows 10 customers emerged unscathed in the aftermath of the WannaCrypt attack.

Windows 10 customers emerged unscathed in the aftermath of the WannaCrypt attack. The exploit used by the ransomware was meant to work only against unpatched Windows 7 and Windows Server 2008 systems. More importantly, however, Windows 10 has built-in security technologies that can help defend against WannaCrypt.



PRE-BREACH

POST-BREACH

Windows 10 device protection against WannaCrypt

Virtualization-based security

"Secure Kernel" stops malicious code from ever being loaded into the Windows kernel through its kernel Control Flow Guard (kCFG)

Windows 10 hardened kernel

Stops shellcode injections with non-executable and randomized kernel memory regions (NX Paged Pool and KASLR)

Device Guard and Windows Defender Antivirus

Blocks and intercepts any initial stages of the attack by allowing only authorized applications to run and analyzing suspicious files

Windows Defender Advanced Threat Protection

Reports and provides intelligence to SecOps about any prevented attack attempts on computers in the network

While security updates are automatically applied in most computers, some users and enterprises may delay deployment of patches. For older Windows versions like Windows 7 and Windows Server 2008 that didn't take the fix in security bulletin MS17-010, but had cloud protection turned on (in Microsoft Security Essentials or Windows Defender AV) WannaCrypt was prevented from executing. However, these older versions do not have the level of exploit hardening and platform features (e.g., Device Guard, instant cloud protection etc.) available in Windows 10 to effectively protect against the threat. Upgrading to the latest Windows version and keeping computers up-to-date remain to be the best defense.

How Microsoft protects you

Microsoft's security advantage

Windows Defender AV protects against threats in real-time using cloud-powered machine learning infrastructure and an unmatched scale of security intelligence. We're able to track and monitor billions of downloads, web pages, emails, and endpoints. Correlating intelligence from these sensors along with keen insights of our security researchers provides us a unique wide-angle view of real-world threats.

Windows Defender Antivirus
Signals from hundreds of millions of customers

Edge and Internet Explorer
8b internet downloads

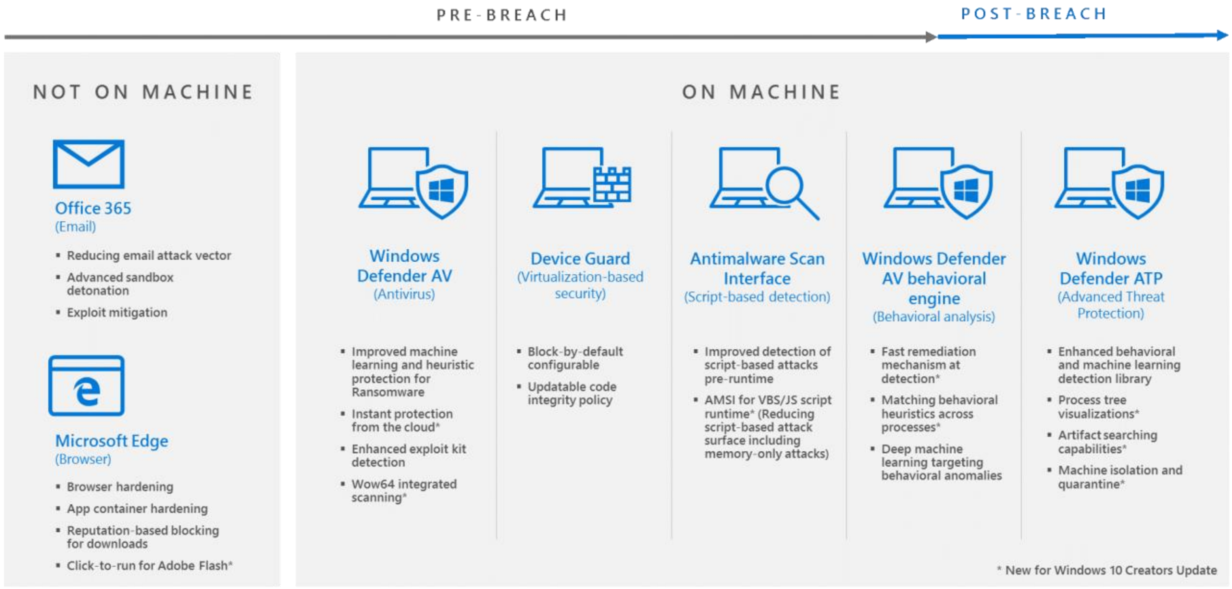
Bing
18b web pages scanned

Office 365
400b emails analyzed

Signals from our vast network of services, search engines, and Windows devices enrich the Microsoft Intelligent Security Graph, which helps Windows Defender AV to rapidly detect never-before-seen malware.

Windows 10 Creators Update: Security in depth

With Windows 10 Creators Update, we rolled out a wide range of protection components that built on top of the Windows 10 Anniversary Update. These security technologies work together to provide an end-to-end defense against known and new ransomware attacks. New features and continued investments are meant to further decrease the attack surface and empower our customers to prevent, detect, and respond to intrusion attacks.



Office 365
(Email)

- Reducing email attack vector
- Advanced sandbox detonation
- Exploit mitigation

Microsoft Edge
(Browser)

- Browser hardening
- App container hardening
- Reputation-based blocking for downloads
- Click-to-run for Adobe Flash*

Windows Defender AV
(Antivirus)

- Improved machine learning and heuristic protection for Ransomware
- Instant protection from the cloud*
- Enhanced exploit kit detection
- Wow64 integrated scanning*

Device Guard
(Virtualization-based security)

- Block-by-default configurable
- Updatable code integrity policy

Antimalware Scan Interface
(Script-based detection)

- Improved detection of script-based attacks pre-runtime
- AMSI for VBS/JS script runtime* (Reducing script-based attack surface including memory-only attacks)

Windows Defender AV behavioral engine
(Behavioral analysis)

- Fast remediation mechanism at detection*
- Matching behavioral heuristics across processes*
- Deep machine learning targeting behavioral anomalies

Windows Defender ATP
(Advanced Threat Protection)

- Enhanced behavioral and machine learning detection library
- Process tree visualizations*
- Artifact searching capabilities*
- Machine isolation and quarantine*

* New for Windows 10 Creators Update

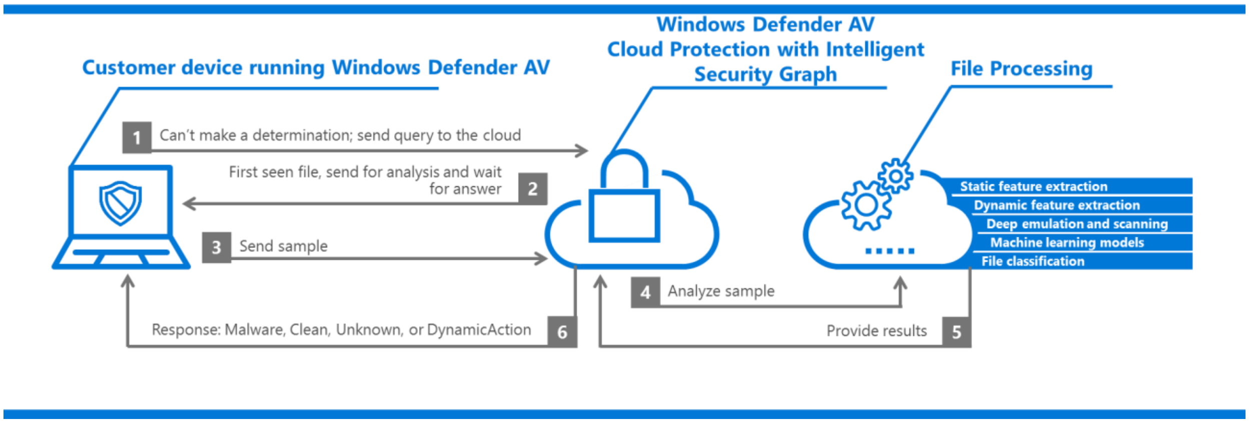
In Creators Update, we also introduced Windows Defender Security Center, which is a single dashboard that lets customers access some of the most important security settings in one place.

Windows Defender AV: Instant cloud-based protection against never-before-seen malware

Windows Defender Antivirus, built into Windows 10, automatically blocks most ransomware and other malware files at first sight using client-based machine learning models, behavioral analysis, and generic and heuristic-based detections.

It uses intelligence from the cloud protection service to verify the nature of suspicious files. New and unknown threats can be instantly blocked using cloud-based machine learning, deep neural networks, fuzzy matching, and other advanced automation technologies.

In Creators Update, Windows Defender AV can suspend a suspicious file from running and sync with the cloud protection service to further inspect the file. It sends the file to the cloud engine, which evaluates the file using static and dynamic analysis through a controlled detonation chamber.

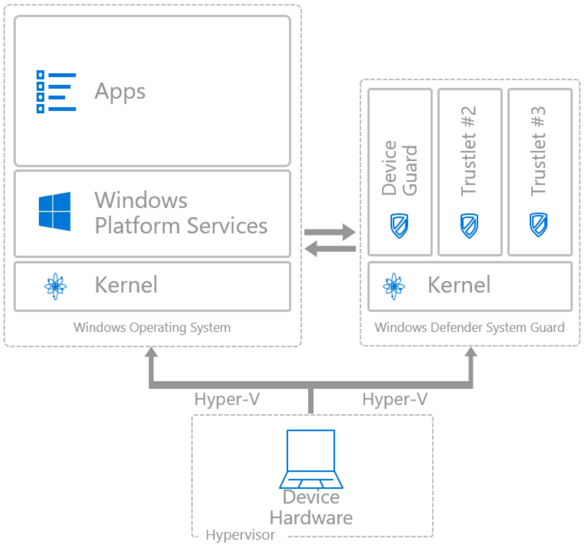

Customer device running Windows Defender AV
Windows Defender AV Cloud Protection with Intelligent Security Graph
File Processing
1 Can't make a determination; send query to the cloud
First seen file, send for analysis and wait for answer 2
3 Send sample
4 Analyze sample
Provide results 5
Response: Malware, Clean, Unknown, or DynamicAction 6
Static feature extraction
Dynamic feature extraction
Deep emulation and scanning
Machine learning models
File classification

Within seconds, Windows Defender AV cloud protection can determine if a new file is malicious or not. This information is stored in the cloud engine for future reference. Within minutes, this information is added to our machine learning classifiers and clustering, and is correlated with signals from the Microsoft Intelligent Security Graph. Windows Defender AV can then protect customers who might encounter the same or similar malicious file.

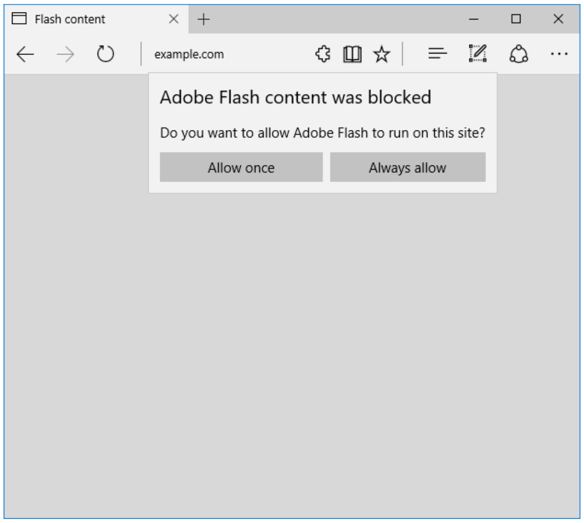
Device Guard: Virtualization-based lockdown security

Device Guard, introduced in Windows 10, is a combination of virtualization-based security and application execution control through code integrity policy. It helps protect devices by preventing threats like ransomware from running, limiting their impact even if they manage to get on the device.

Device Guard only allows apps to run that are authorized by the company. Code integrity policies can also be used to control applications and control whether specific plug-ins, add-ins, and modules can run from specific apps (such as line-of-business applications or browsers). This reduces the attack surface for malware embedding itself in a clean process to obfuscate its intent. See [Introduction to Device Guard: virtualization-based security and code integrity policies]() for more information.



Microsoft Edge: Hardened browser protection against threats from the web



Adobe Flash content was blocked

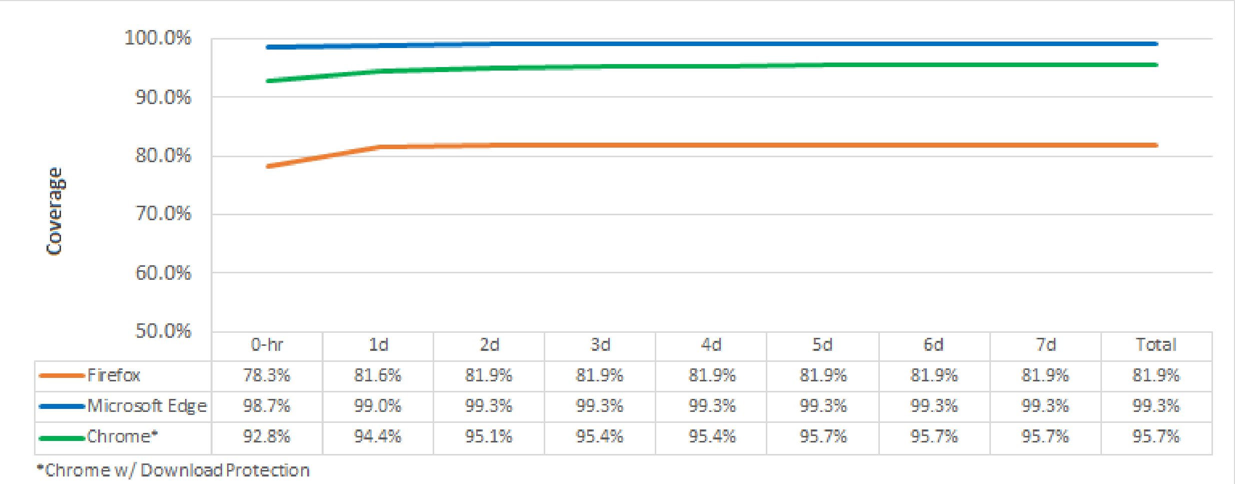
Do you want to allow Adobe Flash to run on this site?

Microsoft Edge browser defaults to a clean HTML5 experience for sites that support it. In Creators Update, if a site relies on Flash, Microsoft Edge lets users decide whether they want to allow Flash to run.

This can stop ransomware infections that automatically start with malformed Flash objects that exploit vulnerabilities in the Adobe software. Microsoft Edge thus limits the attack surface by giving users the ability to only run Flash content they desire.

We designed Microsoft Edge as a very secure platform, with stronger anti-phishing protection and defense against malicious and fake websites. It opens all pages within app container sandboxes and uses reputation-based blocking for downloads, ensuring that the system is not affected by malicious web content.

NSS Labs, a cybersecurity product research organization, recently released a web browser security comparative report testing Google Chrome, Microsoft Edge, and Mozilla Firefox against socially-engineered malware. The task was to determine protection on key areas important to customers, including how many and how fast a socially-engineered malware was blocked.



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Firefox	78.3%	81.6%	81.9%	81.9%	81.9%	81.9%	81.9%	81.9%	81.9%
Microsoft Edge	98.7%	99.0%	99.3%	99.3%	99.3%	99.3%	99.3%	99.3%	99.3%
Chrome*	92.8%	94.4%	95.1%	95.4%	95.4%	95.7%	95.7%	95.7%	95.7%

*Chrome w/ Download Protection

Note: SEM URL response histogram for Firefox, Microsoft Edge, and Chrome. Data from NSS Labs 'Web Browser Security Comparative Report.

In these tests, Microsoft Edge provided the most extensive zero-hour protection, blocking 98.7% of malware within the first hour. Microsoft Edge's blocking rate is 3.6% ahead of Google Chrome, and 17.4% ahead of Mozilla Firefox.

Improved detection for script-based attacks

Many ransomware infections begin with JS and VBS script-based malware. These malicious scripts employ obfuscation techniques to hide characteristic data and become polymorphic. These techniques have further evolved so that malicious code is dynamically built via payloads from command-and-control servers, resulting in malware that does not even get saved to the disk.

We saw a surge in such malicious script-based malware in the last two years. We investigated several thousands of these malware samples to understand them and identify effective choke points.

As a result, in Creators Update, we added additional code instrumentation as part of the operating system to enable Antimalware Scan Interface (AMSI) calls during strategic execution points in JS or VBS script runtime. This allows registered AMSI providers to conduct content inspection via AMSI, enabling them to identify and detect malicious code. This effectively bypasses obfuscation methods used by malware to mask malicious code.

Windows Defender AV uses these new AMSI features to detect malicious script files downloading and executing a ransomware payload.

Enhanced behavior analysis for faster remediation

We have made substantial investments to remediate ransomware infection and limit ransomware activity from minutes to seconds, reducing its damage from hundreds of encrypted files to a few.

One of the ways we achieve this is by improving Windows Defender AV's behavioral engine. Behavior analysis provides another layer of protection by identifying threats based on how files interact with the system, rather than on static characteristics. Behavior analysis is very powerful against obfuscators and code protectors (packers) that malware authors use to evade file-based antivirus detection.

Modern threats attempt to evade behavioral detection algorithms by separating attacks into multiple stages and splitting behavioral actions across multiple benign processes running in the system. Unless an antivirus solution has a behavior detection engine that can track and synthesize activities across these attack stages or processes, it can be bypassed.

With the Creator's Update, Windows Defender AV's behavioral engine can aggregate malware behavior across processes and stages. By tracking activities across multiple vectors, Windows Defender AV not only acts on these multi-stage threats but also provides valuable intelligence to identify and block similar components used in other attacks.

Moreover, Windows Defender AV can record how processes interact with the system and then allow cloud models to detect anomalous behavior. This record of systems event during normal operations can be likened to a flight data recorder, which can allow the reconstruction of the sequence of events.

Wow64 compatibility scanning

In Creators Update, Windows Defender AV added a process-scanning feature that uses the Wow64 compatibility layer, enabling it to better inspect system interactions of 32-bit applications running on 64-bit operating systems.

Windows Defender AV utilizes various system contexts and cloud intelligence to dynamically enable deeper process inspection during pivotal system interactions, all without compromising performance and user experience. This allows Windows Defender AV to better detect and remove polymorphic malware at runtime.

Windows Defender Advanced Threat Protection: Post-breach detection, rich investigation, and response

In Creator's Update, we enhanced Windows Defender ATP's capabilities in its behavioral and machine learning detection libraries across the ransomware infection process. These enhancements aim to identify patient zero as quickly as possible. The process tree visualization and artifact searching capabilities aggregate multiple detections and related events into a single view reducing the time to resolve cases and quickly pinpoint associated ransomware activities.

Security operations teams can hunt for evidence of attacks, such as file names or hashes, IP addresses or URLs, behaviors, machines, and users. They can do this immediately by searching the organization's cloud inventory, which covers even machines that are offline, have been reimaged, or no longer exist, for up to six months back in time.

Improvements in machine isolation, banning files, and process quarantines enable faster response and broader protection against subsequent infections.

With Windows Defender ATP, enterprise customers are well-equipped to quickly identify new ransomware outbreaks, investigate the scope of attacks, and respond early to malware delivery campaigns. As documented in the Windows Defender ATP ransomware playbook, these actions can contain attacks and prevent broader impact to the organization.

Windows 10 S: Microsoft-verified security

Windows 10 S is streamlined for security and performance and works exclusively with apps from the Windows Store. Any app that doesn't go through our Store onboarding, vetting, and signing process won't run. By allowing only verified apps to run, Windows 10 S protects devices against malware, ransomware, and other similar attacks.

Windows 10: Next-gen defense against ransomware

We designed Windows 10 to be the most secure platform, and we continue to harden it against the most advanced attacks.

Windows 10 Creators Update integrates new protection capabilities that provides a next-gen endpoint protection solution to defend against the latest malware and ransomware threats. These capabilities help:

- **Protect** against ransomware from getting to devices through platform and service hardening (browser, email, etc.) against malicious document and scripting files, and updated exploit mitigations
- **Detect** ransomware and stop it quickly. Limit infection by using Windows Defender AV, which uses deep machine learning models that target behavioral anomalies, context-aware detections for script-based attacks, integrated intel sharing for quick protection, and advanced cloud protection technologies
- **Respond** to ransomware attacks through Windows Defender ATP alerts that are critical in investigating and understanding the scope of ransomware infections and provide response options

Windows 10's next-gen technologies deliver a comprehensive defense stack that helps protect computers and networks from ransomware attacks:

Online safety and protection

Best browser & email protection through Microsoft Edge & Office 365 against phishing, exploit sites, malicious downloads

Windows 10 built-in security

Sensors built deep into the operating system, combined with human experts, unique optics through the Microsoft Intelligent Security Graph

Machine learning-based cloud protection

Cloud-based machine learning protects customers from the new threats in seconds. We also rely on the Microsoft Intelligent Security graph to amplify protection across our services

Rich investigation experience with Windows Defender ATP

Understand your current threat landscape, explore a rich machine timeline that unifies security events from Windows Defender ATP, Windows Defender AV, and Device Guard, to enable quick actions

Further reading

Antivirus evolved

Protecting against ransomware (Webinar)

WannaCrypt ransomware worm targets out-of-date systems

Customer Guidance for WannaCrypt attacks

Ransomware: a declining nuisance or an evolving menace?

Averting ransomware epidemics in corporate networks with Windows Defender ATP

Windows Defender Advanced Threat Protection - Ransomware response playbook

Windows Security blog posts on ransomware

Ransomware FAQ on Windows Security Intelligence website

Contributors

Eric Douglas
Security Research Team

Tanmay Ganacharya
Security Research Team

Karthik Selvaraj
Security Research Team

Elia Florio
Security Research Team

Holly Stewart
Security Research Team

Ram Gowrishankar
Security Research Team

Tim Kerk
Security Research Team

Brian Lich
Content Publishing Team

Daniel Simpson
Content Publishing Team

Dolcita Montemayor
Content Publishing Team

Eric Avena
Content Publishing Team

Justin Hall
Content Publishing Team

Sue Hotelling
Enterprise & Security Team

Debraj Ghosh
O365 Security Team

Heike Ritter
Product Marketing Team

Jason Conradt
Security Engineering Team

Matt Miller
Security Engineering Team

Randy Treit
Security Engineering Team

Scott Anderson
Security Research Team

Tommy Blizard
Windows Defender ATP Team

Microsoft