

May 14, 2019

Executing on the vision of Microsoft Threat Protection

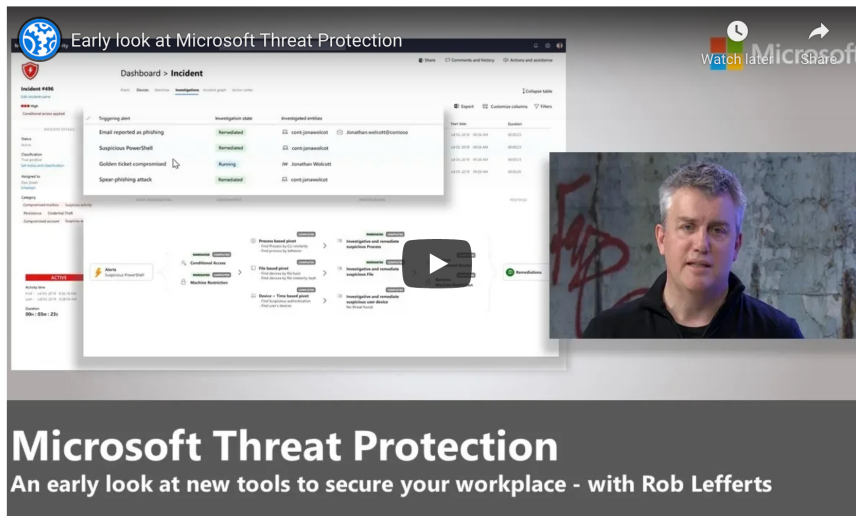
Rob Lefferts Corporate Vice President, Microsoft 365 Security

Share ▾

Over the last several months, we've provided regular updates on the rapid progress we're making with [Microsoft Threat Protection](#), which enables your organization to:

- **Protect your assets** with [identity-driven security](#) and [powerful conditional access policies](#) which ensure your assets are secured from unauthorized users, devices, or apps.
- **Connect the dots** between disparate threat signals and develop [threat incidents](#) by grouping alerts from different parts of your environment, stitching together the elements of a threat.
- **Empower your defenders**, providing in-depth analysis to identify the full scope and impact of a threat.

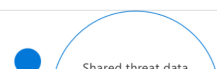
We support these capabilities by offering you [intelligent automation](#) as well as [human expertise](#) to quickly resolve situations and keep your business running. I recently shared our vision of Microsoft Threat Protection with Jeremy Chapman in a Microsoft Mechanics video broadcast:



We strongly believe in our vision and are confident our customers will benefit from enhanced security with Microsoft Threat Protection as we continue adding capabilities with unstoppable momentum. Today, I want to spend time highlighting what Microsoft Threat Protection *can already do for you*. While we're very excited about the vision and pushing towards releasing more features, it's important to share the significant advantages which are already available with Microsoft Threat Protection **today**. I'm going to use a real example of a common, yet lethal, threat type to showcase how Microsoft Threat Protection already makes your organization more secure.

Executing on our vision

The more threats we see, the more we can stop. This virtual cycle means that each threat we see helps further enhance our machine learning models, which in turn improves our ability to stop subsequent threats. As we've shared in the past, the [Microsoft Intelligent Security Graph](#) (Figure 1) enables us to see billions of threats and assess 6.5 *trillion* signals daily. Importantly, we don't only see a large quantity of threats, but we also see threats from a wide variety of sources. Through the Intelligent Security Graph, threat signals are seamlessly shared across all the services in Microsoft Threat Protection, providing comprehensive security across multiple attack vectors.



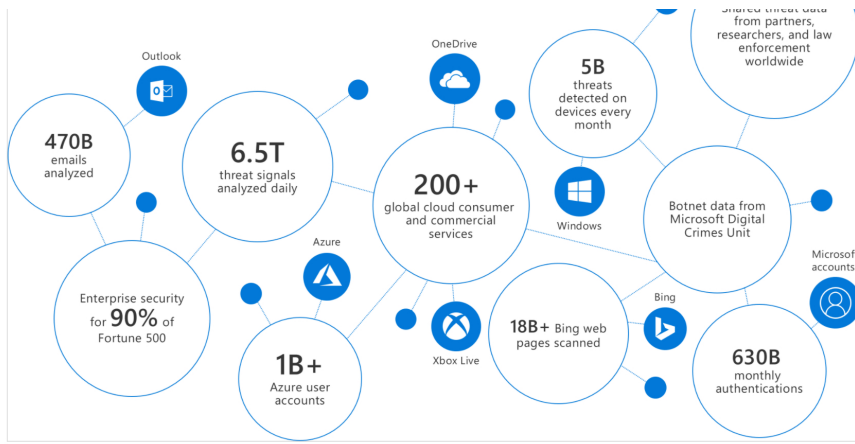


Figure 1. The strength of signal offered by the Microsoft Intelligent Security Graph.

A [great example](#) of how Microsoft Threat Protection is already executing on its promised vision is how we address phishing campaigns. Phishing has been on a steady rise over the last few years. As the provider of one of the largest email services on the planet, we expect to be a primary target for attacks. In 2018 alone, Microsoft's analysts analyzed (Figure 2) over 300,000 phishing campaigns and 8 million business email compromise (BEC) attempts.



Figure 2. Data from Office 365 security analysts on the phishing campaigns and BEC attempts from 2018.

While these numbers can be worrisome, Microsoft Threat Protection *is designed* to secure your organization from phishing, whether the campaign attacks the endpoint, email, or through the web. In a [recent campaign](#), anomaly detection algorithms in [Microsoft Defender Advanced Threat Protection \(ATP\) next-generation protection](#) pointed to multiple PDF files *that Microsoft could detect*. We were the only organization able to detect these phish PDFs because we leveraged the knowledge from multiple security services operating on various attack vectors. In this example, the malicious PDF files (Figure 3) were blocked by machine learning models, enhanced by assimilating signals from multiple services of Microsoft Threat Protection.

Figure 3 shows a screenshot of a VirusTotal scan for a PDF file. The file is identified as **Trojan:PDF/Sonbokli.A!cl** and was only detected by Microsoft. The scan results are as follows:

Detection	Details	Community	
Microsoft	Trojan:PDF/Sonbokli.A!cl	Ad-Aware	Clean
AegisLab	Clean	AhnLab-V3	Clean
ALYac	Clean	Antiy-AVL	Clean
Arcabit	Clean	Avast	Clean
Avast Mobile Security	Clean	AVG	Clean
Avira	Clean	Babable	Clean
Baidu	Clean	BitDefender	Clean
Bkav	Clean	CAT-QuickHeal	Clean
ClamAV	Clean	CMC	Clean
Comodo	Clean	Cylance	Clean
Cyren	Clean	DrWeb	Clean
Emsisoft	Clean	eScan	Clean
ESET-NOD32	Clean	F-Prot	Clean
F-Secure	Clean	Fortinet	Clean

Figure 3. One of several PDF files **that only Microsoft was detecting** (as Trojan:PDF/Sonbokli.A!cl) at the time it was first observed (Source: [VirusTotal](#)).

Through the Microsoft Intelligent Security Graph, the detection algorithm was enriched with URL and domain reputation intelligence from [Microsoft Defender SmartScreen](#), the service powering the anti-phishing technology in Microsoft Edge, as well as the [network protection](#) capability in Microsoft Defender ATP.

Additionally, [Office 365 Advanced Threat Protection \(ATP\)](#) provided rich optics from PDF phish files distributed via email. When Office 365 ATP detects a suspicious file or URL in emails, it can detonate the file and apply heuristics and sophisticated machine learning to determine a verdict. This verdict is shared with other services in Microsoft Threat Protection. In the case of these PDF files, all the services in Microsoft Threat Protection could immediately block the corrupted PDF files because the original signal from Office 365 ATP was shared with all the other services in Microsoft Threat Protection.

Microsoft Threat Protection also stops threats *quickly* because of its unique attributes. Every day, Microsoft [sees millions of new attacks](#) that run for just 60 minutes or less. This fast pace requires security to be automatic, in real-time, and accurate. The signal sharing and mitigation across Microsoft Threat Protection is robust and comprehensive. Below (Figure 4) is an actual timeline showing how the threat originally identified by SmartScreen provided signal to both Office ATP and Microsoft Defender ATP, which both blocked the threat.

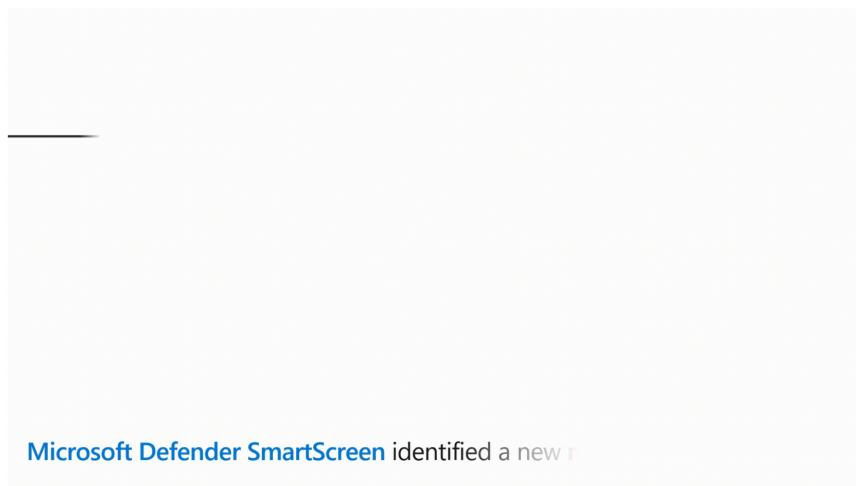


Figure 4. Threat timeline of this campaign from the first identification with SmartScreen to mitigations by Office ATP/Exchange Online Protection (EOP) and Microsoft Defender ATP.

Great intelligence enables great security

Our unparalleled intelligence, seamless integration, and best-of-breed solutions for multiple attack vectors leads to the staggering numbers of threats we can detect and mitigate across multiple threat vectors. Below are statistics of the threats which Microsoft Threat Protection mitigated in 2018 (Figure 5). What's important is not only the number of threats we've detected and blocked, but also the fact that we do so for threats across multiple, disparate attack vectors. This is the same strength of security you will benefit from when you implement Microsoft Threat Protection.



Figure 5. Microsoft Threat Protection in action. Some of the detections and mitigations already offered with the solution.

Revamped website to keep you up to date

Today, we're excited to launch our new [Microsoft Threat Protection website](#), where you'll find great collateral summarizing the full scope of capabilities offered by Microsoft Threat Protection. On the site,

you'll find *three new webcasts* where our engineers offer details and examples of:

- **Automated Incident Response**—Unique SecOps capabilities only available with Microsoft.
- **Azure Sentinel**—Our newly launched SIEM-as-a-service.
- **Microsoft Threat Experts and Threat and Vulnerability Management**—For endpoints.

The new site also links to all the services which are part of Microsoft Threat Protection with great collateral offering details on how the individual services help secure specific attack vectors.

Experience the evolution of Microsoft Threat Protection

Hopefully, I gave you a glimpse of how Microsoft Threat Protection has already started executing on the vision of securing the modern organization. Take a moment to [learn more about Microsoft Threat Protection](#), read our [previous monthly updates](#), and visit our [new website](#).

[Organizations](#) have already transitioned to Microsoft Threat Protection and [partners](#) are leveraging its powerful capabilities. Begin a trial of Microsoft Threat Protection services today to experience the benefits of the most comprehensive, integrated, and secure threat protection solution available to your organization.

- [Microsoft Threat Protection trial](#)
- [Microsoft Azure Sentinel](#)

Filed under:

[Evolution of Microsoft Threat Protection, Microsoft Intelligent Security Graph](#)

You may also like these articles



June 25, 2020

Lessons learned from the Microsoft SOC— Part 3d: Zen and the art of threat hunting

This blog provides lessons learned on how Microsoft hunts for threats in our IT environment and how you can apply these lessons to building or improving your threat hunting program. This is the seventh in a series.

[Read more >](#)

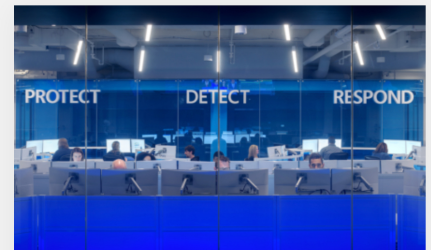


April 22, 2020

Defending the power grid against supply chain attacks: Part 3 – Risk management strategies for the utilities industry

By working with governments, trade organizations, and suppliers, the utility industry can improve security across the supply chain.

[Read more >](#)



April 21, 2020

MITRE ATT&CK APT 29 evaluation proves Microsoft Threat Protection provides deeper end to end view of advanced threats

During the MITRE ATT&CK evaluation, Microsoft Threat Protection delivered on providing the deepest optics, near real time detection, and a complete view of the attack story.

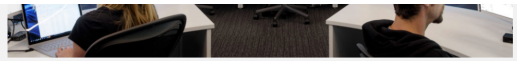
[Read more >](#)

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

[LEARN MORE >](#)





Get all the news, updates, and more at [@MSFTSecurity](#) 

What's new

- [Surface Duo](#)
- [Surface Laptop Go](#)
- [Surface Pro X](#)
- [Surface Go 2](#)
- [Surface Book 3](#)
- [Microsoft 365](#)
- [Windows 10 apps](#)
- [HoloLens 2](#)

Microsoft Store

- [Account profile](#)
- [Download Center](#)
- [Microsoft Store support](#)
- [Returns](#)
- [Order tracking](#)
- [Virtual workshops and training](#)
- [Microsoft Store Promise](#)
- [Financing](#)

Education

- [Microsoft in education](#)
- [Office for students](#)
- [Office 365 for schools](#)
- [Deals for students & parents](#)
- [Microsoft Azure in education](#)

Enterprise


- [Azure](#)
- [AppSource](#)
- [Automotive](#)
- [Government](#)
- [Healthcare](#)
- [Manufacturing](#)
- [Financial services](#)
- [Retail](#)

Developer

- [Microsoft Visual Studio](#)
- [Windows Dev Center](#)
- [Developer Center](#)
- [Microsoft developer program](#)
- [Channel 9](#)
- [Office Dev Center](#)
- [Microsoft Garage](#)

Company

- [Careers](#)
- [About Microsoft](#)
- [Company news](#)
- [Privacy at Microsoft](#)
- [Investors](#)
- [Diversity and inclusion](#)
- [Accessibility](#)
- [Security](#)

 [English \(United States\)](#)


[Sitemap](#) [Contact Microsoft](#) [Privacy](#) [Terms of use](#) [Trademarks](#) [Safety & eco](#) [About our ads](#) [© Microsoft 2021](#)

The most secure Windows ever

Windows 10 provides comprehensive, built-in protection—at no extra cost.¹ Learn how Windows Hello facial recognition and biometric logins, coupled with comprehensive antivirus protection, keep you more secure than ever.

[GET WINDOWS 10 >](#)

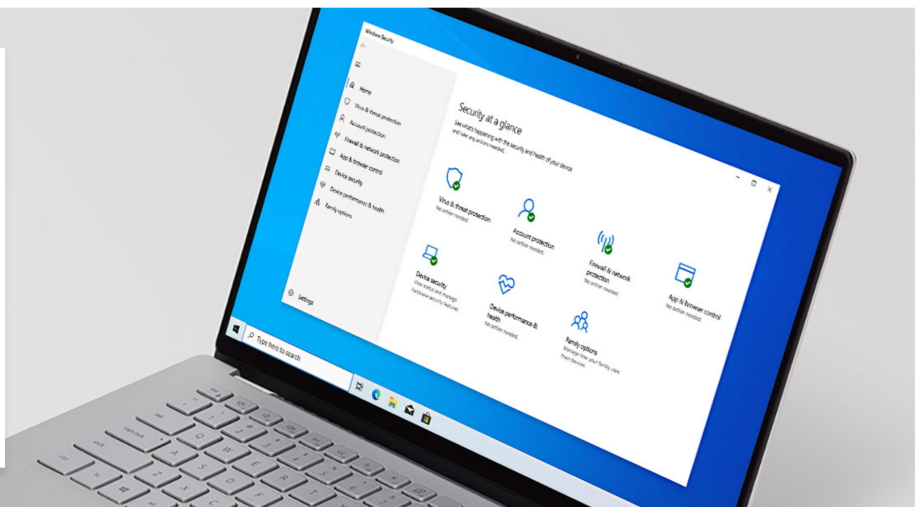




Microsoft Defender Antivirus

Formerly known as Windows Defender, Microsoft Defender Antivirus still delivers the comprehensive, ongoing, and real-time protection you expect against software threats like viruses, malware, and spyware across email, apps, the cloud, and the web.

[LEARN MORE >](#)



Always defending—at no extra cost

No need to download—Microsoft Defender comes standard on Windows 10, protecting your data and devices in real time with a full suite of advanced security safeguards.¹

Files are secured and accessible across devices

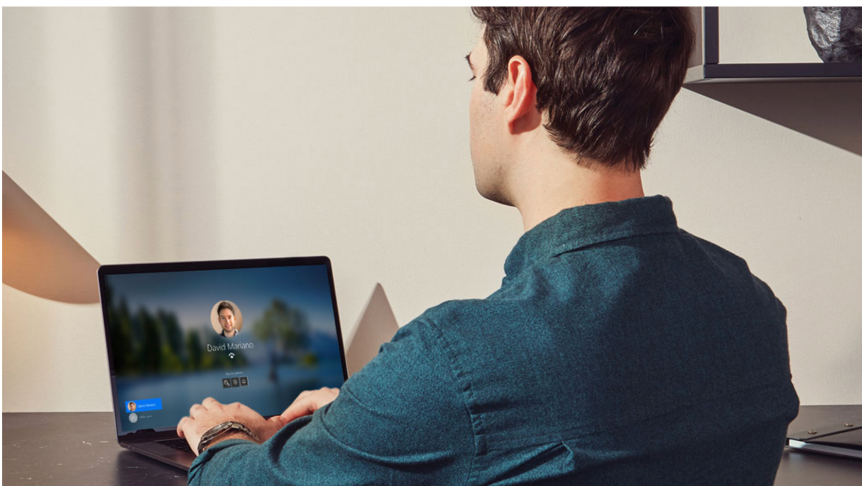
Save your files to OneDrive to keep them protected, backed up, and accessible from all your devices, anywhere.

You manage your privacy

Set your location, camera and data usage options in the easy-to-access account settings panel.

Help keep your family safer online

With Windows 10, schedule screen time, limit access to mature content and restrict online purchases, including apps, games and films.²



Say goodbye to passwords with Windows Hello

Windows Hello logs you in 3x faster than a password.⁴ Use your camera to recognise your face or try your fingerprint reader.³ You can always keep your PIN as a backup.

[LEARN MORE >](#)

Sign in your way

Apps enabled for Windows Hello

Your companion devices unlock

Sign in your way

Enabling Windows Hello turns on sign-in with your face or fingerprint.³ Log in faster and more securely to your laptop, tablet, device, app or even websites; you can even make in-app purchases.

Apps enabled for Windows Hello

Windows Hello works with compatible apps like iHeartRadio and Dropbox, so you can bypass the password and breeze right through with facial recognition biometric security.³

Your companion devices unlock your PC

Windows Hello lets you use your digital wristband, smart watch, phone and other companion devices to quickly unlock your Windows 10 PC without using a password.⁵

Prevent PC updates from interrupting your workflow

Windows 10 provides new features and security updates for free on an ongoing basis. Now you have the option to update when it's convenient for you.



You're in control with searching, streaming and gaming



Set parameters with Ask a Parent tool⁶

If your kids want more screen time or to purchase a game, app or film, you can require them to request your permission first.

[FAMILY SETTINGS >](#)

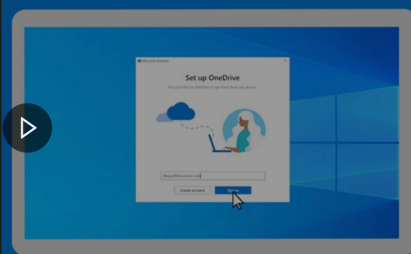


Get things done securely and quickly on the web

Microsoft Edge and Bing feature built-in learning tools, 4K⁷ streaming and advanced cyber protections—all optimised for Windows 10.

[BROWSE FEATURES >](#)

Sync OneDrive files and folders



Share and edit files in OneDrive

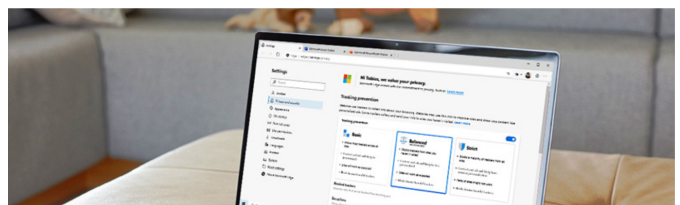
Save files to OneDrive to keep them protected, backed up and accessible from your iOS, Android and Windows devices, virtually anywhere.⁸ Even offline.

[LEARN MORE >](#)



Security and privacy you can count on

Privacy starts with putting you in control. You should have the tools



Privacy starts with putting you in control. You should have the tools and information to make informed choices. You can manage your data saved to the cloud.

[LEARN MORE >](#)



Find My Device

Find My Device is a feature that can help you locate your Windows 10 device if it's lost or stolen. It works for any Windows device, such as a PC, laptop, Surface or Surface Pen.

[LEARN MORE >](#)



[WINDOWS INSIDER PROGRAMME](#)



[WINDOWS SUPPORT](#)



[THE WINDOWS BLOG](#)



[ASK THE COMMUNITY](#)

¹ For the supported lifetime of the device. Internet access fees may apply.

² Requires a Microsoft family account with Device health sharing permissions enabled.

³ Windows Hello requires specialised hardware including a Windows Hello capable device, fingerprint reader, illuminated IR sensor or other biometric sensors and capable devices.

⁴ Based on average time comparison between typing a password respectively detecting a face or fingerprint to authentication success.



⁵ Available for selected companion devices and selected Windows 10 editions. Might require PC and companion devices to be joined in Azure Active Directory or Active Directory and paired via Bluetooth.

⁶ Requires a Microsoft family account with Device health sharing permissions enabled. Also requires Android devices with Microsoft Launcher installed and signed in with the same Microsoft account associated with their Microsoft family account. For a parent to access and view a child's locations and app activities through the [Family web page](#), Microsoft Launcher must be installed on each child's device. For a parent to access and view their child's location(s) and app activities through Microsoft Launcher, Microsoft Launcher must be installed on both the parent's device and each child's device. In each case, location and app usage permissions must be allowed through Microsoft Launcher on the child's device. Activity reporting features require Android 5.0+ on each child's device. Family settings available on Windows 10 and Xbox One devices. Some settings available on Android devices with Microsoft Launcher installed. Family settings work on the Microsoft Edge browser only.

⁷ 4K Ultra HD exclusivity is limited to PCs running Windows 10. 4K works in both Microsoft Edge and Netflix app. Only 7th Gen Intel® Core™ processor or higher devices can decrypt PlayReady 4K DRM. Netflix Ultra HD plan required. Requires Dolby Vision-supported PlayReady content and capable hardware.

⁸ Internet access may be required. Fees may apply.

Follow Microsoft Windows  

Share this page  

What's new

Surface Laptop Go

Surface Pro X

Surface Go 2

Surface Book 3

Microsoft 365

Windows 10 apps

HoloLens 2

Microsoft Store

Account profile

Download Center

Microsoft Store Support

Returns

Order tracking

Microsoft Experience Centre

Recycling

Microsoft Store Promise

Education

Microsoft in education

Office for students

Office 365 for schools

Deals for students & parents

Microsoft Azure in education

Enterprise

Azure

AppSource

Automotive

Government

Healthcare

Manufacturing

Financial services

Retail

Developer

Microsoft Visual Studio

Developer Center

Channel 9

Office Dev Centre

Company

Careers


About Microsoft

Company news

Privacy at Microsoft

Investors

Security

 English (United Kingdom)

[Contact us](#) [Privacy](#) [Manage cookies](#) [Terms of use](#) [Trademarks](#) [About our ads](#) [© Microsoft 2021](#)

