Microsoft Defender ATP’s antivirus capabilities boost malware protection

Today’s antimalware solutions must help protect against and combat increasingly sophisticated, malicious software. Frequently, traditional antimalware strategies put IT security professionals in the position of being reactive to attacks, instead of proactively preventing them; they don’t adequately address the challenges presented by a more mobile—and modern—workplace. More than ever, it’s important to have security solutions in place that are as agile and innovative as the new threats that are constantly emerging.

One of our missions at Microsoft Core Services Engineering and Operations (CSEO, formerly Microsoft IT) is to empower the modern enterprise by providing a trusted, more secure computing environment. We’ve protected client devices against malware for years, previously using traditional, sometimes third-party antivirus solutions, installed on client devices and managed through Microsoft System Center Configuration Manager. Windows 10, however, introduced a new, more modern way to protect client devices. Windows Defender Advanced Threat Protection (ATP) is the result of a complete redesign in the way Microsoft provides client protection. It is agentless, built directly into Windows 10, and was designed to learn, grow, and adapt to help security professionals stay ahead of incoming attacks.

With Windows 10, we can use the built-in security features to enable malware protection and other critical security capabilities that help protect devices right from the start. Microsoft Defender ATP is a unified platform for Windows protection that includes a broad range of capabilities, some of which include:

- Antivirus
- Exploit protection
- Attack surface reduction
- Application control
- Hardware-based isolation

Before we take a closer look at the security features in Microsoft Defender ATP, let’s discuss the evolution of malware protection in Windows.

Antimalware journey in Windows

Over the years, antimalware protection for Microsoft Windows has evolved from separate installations of System Center Endpoint Protection and third-party antivirus software to Microsoft Defender ATP and its antivirus capability. Let’s take a quick look at how—and, more importantly, why—we transitioned to it.

Windows 7: System Center Endpoint Protection and third-party solutions

Windows 7 didn’t include a built-in antimalware solution, so we installed System Center Endpoint Protection on client devices across Microsoft, using Microsoft System Center Configuration Manager to update and distribute malware definitions. We still use System Center Endpoint Protection to help protect earlier versions of Windows in our environment.

Windows 8: System Center Endpoint Protection updated to manage built-in antivirus

Windows Defender Antivirus was introduced in Windows 8 to help protect client devices, but it was mainly targeted to consumers, rather than large companies. Under the hood, though, it provided enterprise-grade antimalware
capabilities. At the time, Configuration Manager, which we use to manage System Center Endpoint Protection, couldn’t be used to manage Windows Defender Antivirus in Windows 8. Because we needed the additional capabilities, like telemetry and easier management of security-related tasks, we continued to install System Center Endpoint Protection on the Windows 8 devices in our environment.

Based on this, we encouraged the System Center Configuration Manager team to enhance it to be compatible with Windows Defender Antivirus. This way, we, and other security professionals, could take full advantage of the combined benefits of both applications. We wouldn’t need additional infrastructure to install or update antimalware and would spend less time and effort managing agent and definition updates. That could save us time and effort—and it offered a promising path toward more modern ways to manage, and even extend, client malware protection for the enterprise.

**Windows 10: Moved from System Center Endpoint Protection to Microsoft Defender ATP**

With Windows 10, and the introduction of Microsoft Defender ATP, the enterprise-grade antivirus capabilities we need are built directly into the operating system. Microsoft Defender ATP works seamlessly with Configuration Manager to deliver enterprise management and policy setting capabilities along with a collection of telemetry to enforce compliance. The antivirus capabilities are dynamic and are backed by cloud intelligence that helps defend us from known and unknown malware threats, even at first sight, instead of relying on virus signatures that have to be updated after new threats are identified.

Now that our malware protection is part of Microsoft Defender ATP, intelligent endpoint behavioral sensors and AI are doing the scanning for known viruses. We have cloud security analytics, and threat intelligence that help us quickly detect and respond to threats in our environment. We’re also excited that—in addition to the antivirus capabilities in Microsoft Defender ATP—we can use the built-in firewall and other security-related features, including:

- **Exploit protection**, which uses Microsoft Intelligent Security Graph (ISG) capabilities to identify active exploits and common behaviors to stop these types of attacks at various stages. Although underlying vulnerabilities, delivery mechanisms, and payload can differ and evolve, there’s a core set of behaviors and vectors to which many different attacks adhere. By correlating streams of events to various malicious behaviors with the ISG, Microsoft Defender ATP’s exploit protection has the capability and controls to handle emerging threats. The four components of Microsoft Defender ATP’s exploit protection are:
  - **Attack Surface Reduction (ASR)**: A set of controls that companies can enable to prevent malware from getting on computers by blocking Office-, script-, and email-based threats.
  - **Network protection**: Protects the endpoint against web-based threats by blocking any outbound process on the device to untrusted hosts/IP through Windows Defender SmartScreen.
  - **Controlled folder access**: Protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders.
  - **Exploit protection**: A set of exploit mitigations (replacing the Enhanced Mitigation Experience Toolkit) that can be easily configured to protect your system and applications.

- **Application control** helps mitigate security threats by restricting the applications that users can run and the code that runs in the system core (kernel). Using it, you can also create policies to block unsigned scripts and MSIs, and force Windows PowerShell to run in Constrained Language Mode.

- **Device integrity** uses multiple enterprise-related hardware and software security features to maintain and verify the integrity of the device. Specifically, it helps protect the integrity of the boot process and system runtime from being compromised in a way that would enable advanced malware and exploits from hiding from system defenses.

Let’s take a closer look at what we’ve experienced and some of the benefits we’ve seen since we started using Microsoft Defender ATP’s next-generation protection capabilities for malware protection at Microsoft.
Benefits of using advanced malware protection available in Microsoft Defender ATP

By using an antivirus that’s built into Windows 10, along with the additional antivirus capabilities from Microsoft Defender ATP, many policy management and other tasks we needed to perform to protect client devices in our environment are no longer necessary or have been optimized. We no longer need to deploy and manage third-party or standalone malware protection. Everything we need is built into the operating system and is updated through Windows Update. We don’t need to buy or maintain servers just to run antimalware or other hardware-operations tasks—tasks that once took up to 60 percent of our time. Now, we can capture telemetry, act on it, and spend more time on security instead of operations. We’re saving both time and money that we used to spend in planning, testing, installing, and upgrading antimalware for our environment.

In addition to those savings, our antivirus capabilities now provide additional protections that extend beyond scanning a device’s file system for malicious files and behaviors. Advanced analytics, machine learning, and AI are constantly improving recognition, and so we can block new and never seen before threats on first sight without signature updates.

Cloud-delivered protection

Microsoft Defender ATP provides cloud-delivered protection for near-instant detection and blocking of new and emerging threats. Dedicated protection is updated based on machine learning, human and automated big-data analysis, and in-depth threat resistance research.

Always-on scanning, using advanced file and process behavior monitoring

Microsoft Defender ATP’s next generation protection capabilities provide always-on scanning, using advanced file and process behavior monitoring and other heuristics (also known as “real-time protection”). With advanced in-memory capabilities, as well as Attack Surface Reduction controls, and network protection capabilities, it can also prevent fileless malware.

Blocking malware at first sight

By using a new antivirus capability from Microsoft Defender ATP called “Block at First Sight,” we have a new critical protection capability. Approximately 96 percent of all malware files detected and blocked by our antivirus capabilities are observed only once in the world. If a threat is unknown and metadata about the threat isn’t enough, we’ve configured the antivirus features to automatically collect and scan the sample in the Microsoft cloud to analyze it for zero-day threats. This includes running the suspicious file in a virtualized environment.

Simplified management

We’ve found that policy orchestration through the Microsoft Defender ATP portal is straightforward and uses fewer system resources and processes than solutions that require more orchestration. Fewer system resources and processes mean better computer performance.

Security updates

Now, we have an improved process for keeping antimalware on our client PCs up to date. Even if a user hasn’t signed in to the corporate network for a while, Windows Update will keep Microsoft Defender ATP’s next generation protection capabilities up to date. We don’t have to worry whether a server is delivering updates, or if it’s deploying the solution to the endpoints, because Windows Update automatically keeps the client up to date.
Additionally, the datacenter servers that supported installation and updates of client components were taken down. We don’t need to buy or maintain servers just to run antimalware or other hardware-operations tasks—tasks that once took up to 60 percent of our time.

**Using exclusion lists for better client performance**

Since using Microsoft Defender ATP’s next generation protection capabilities, we haven’t had to create broad exclusion lists, like those we used with third-party antivirus products to help us preserve user productivity and device performance. We now have the flexibility to allow users to exclude specific trusted files, processes, and directories for better performance. For example, excluding certain Windows files from antimalware scanning can make Windows start more quickly. Most Microsoft employees have administrator permissions on their local computers, so they can configure their own device because they know best what tools and files they’re using. This is particularly important at Microsoft because of the number of developers and test environments—we don’t want to interrupt compilers during malware checks, because the compilers would need to start all over again. A developer can request `<compile name>.exe` as an exception in Microsoft Defender ATP to prevent interference.

**Microsoft Defender ATP’s next generation protection capabilities in the datacenter**

We also use [Windows Defender ATP’s antivirus capabilities on Windows Server 2016](microsoft.com/itshower) in the datacenter. The functionality, configuration, and management are mostly the same for Windows 10 and Windows Server 2016, with only a few key differences:

- In Windows Server 2016, automatic exclusions are applied based on your defined server role.
- In Windows Server 2016, the antivirus capability won’t disable itself if you’re running another antivirus product.

*Note: For a list of server-related exclusions, see the [Microsoft Anti-Virus Exclusion List](microsoft.com/itshower) on the TechNet Wiki.*

**One solution to protect, detect, and respond to advanced attacks**

Microsoft Defender ATP’s next generation protection capabilities have provided excellent results as we’ve seen in our own environment and reflected in industry test scores. It’s easier to manage, there’s nothing to deploy, and with automated updates, we’re saving time and costs over what we used to see in antimalware-related maintenance, upgrades, servers, and operational tasks. Beyond offering advanced malware protection, Microsoft Defender ATP has been a game changer in how we protect client devices from cyber threats. With Microsoft Defender ATP, the power of the Windows security stack is providing preventative protection—it detects attacks and zero-day exploits, and we have centralized management for our end-to-end security lifecycle.

Microsoft Defender ATP detects advanced attacks and data breaches and automates security incidents. Using it, we have the intelligence and tools to investigate and mitigate threats within minutes, instead of the days or weeks it used to take. If you’re ready to learn more about how Microsoft Defender ATP can improve the security posture of your organization, you can download the [Windows Defender Advanced Threat Protection Information Kit](microsoft.com/itshower).

**For more information**

[microsoft.com/itshower]

[Windows Defender ATP helps analysts investigate and respond to threats](microsoft.com/itshower)

[Mitigate threats by using Windows 10 security features](microsoft.com/itshower)

[Upgrade to Windows 10](microsoft.com/itshower)

[Introduction to Windows Defender Device Guard: virtualization-based security and Windows Defender Application Control](microsoft.com/itshower)
Windows Defender Security Intelligence

Microsoft Secure

Why Windows Defender Antivirus is the most deployed in the enterprise

How artificial intelligence stopped an Emotet outbreak

© 2019 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.