DIFENDA

Why Microsoft Is Now the Leader in Endpoint Detection

Why Microsoft Is Now the Leader in Endpoint Detection

The cybersecurity industry is no stranger to assumptions. It's the reason why the same established technology providers have been the focus for over a decade. It's also the reason why Microsoft was historically overlooked as a reliable solution provider in this space.

But that's all changing now.

Microsoft is serious about security, having invested over $1 billion USD in security development. This has pushed Microsoft to the leading edge of security across many technology areas.

Today, endpoint protection is one of the most obvious areas of improvement. The decades of Windows vulnerabilities and generic antivirus solutions that earned Microsoft its mediocre reputation are over.

For security-focused companies and industries, Microsoft shouldn't be an afterthought—it should be the first choice.

Digital Transformation & Cybersecurity: What Happened?

The pandemic has transformed everything digital, increasing adoption rates across the board for cloud services. Some experts go as far as saying this rapid shift has accelerated adoption by seven years.

And the numbers don't lie. In Q3 2020, a Microsoft survey revealed that 58% of respondents increased their security budgets, 82% planned to add security staff, and 81% needed to lower security costs.

It became very clear that companies understood just how important cybersecurity was becoming, especially as businesses went all in on their digital transformations.

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

One look at the most recent Gartner Magic Quadrant for Endpoint Protection Platforms makes it clear that Microsoft deserves more than just a second look, outpacing the entire industry—now competing head-to-head with only industry darling CrowdStrike.

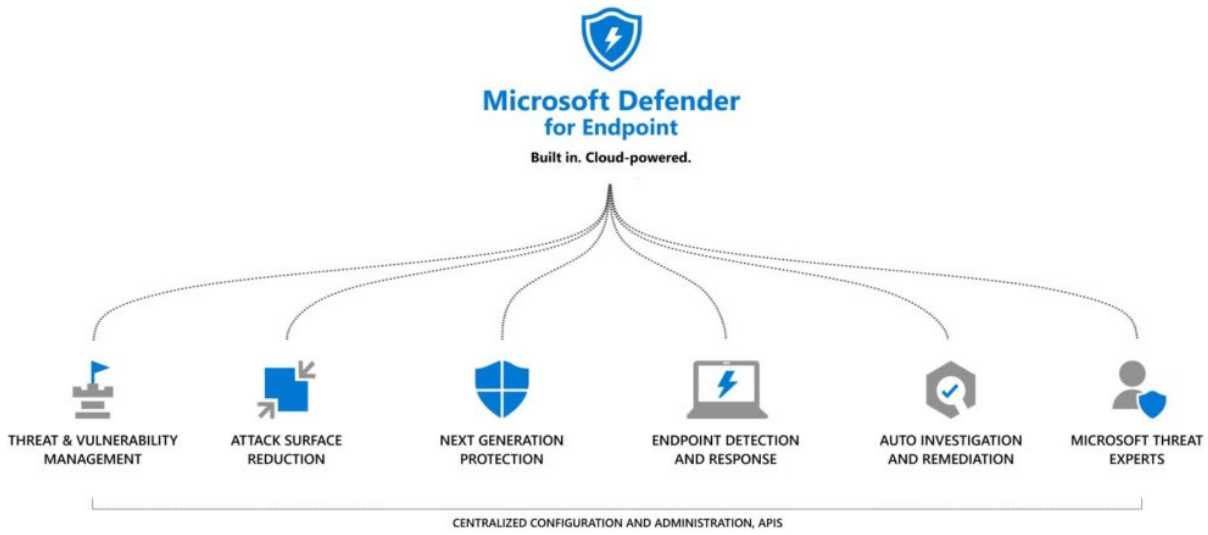
Being one of the leading cloud infrastructure providers, the owners of arguably the most popular operating system in the world, and an entire ecosystem of products that aim to empower the user experience—It was always a matter of time for Microsoft.

And this is something that Microsoft has embraced. Their significant investments in cybersecurity, in Azure Sentinel, Microsoft Defender, and other supportive technologies has created the winning formula for a truly integrated and protected experience.

The days of point (standalone) solutions are coming to an end. Companies are looking for modular services that provide complete protection at all touch points. And very few solutions provide the same level of security and visibility that Microsoft offers through its robust cybersecurity ecosystem.

Endpoint Detection & Response: More Than Meets the Eye

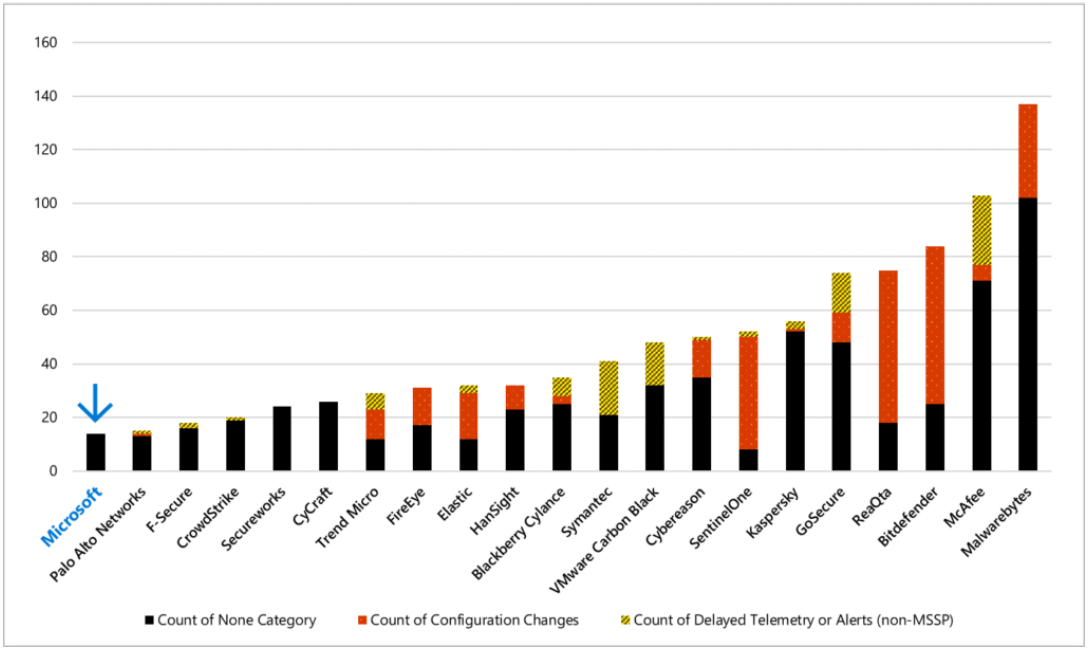
An Endpoint Detection & Response (EDR) solution is far more than just antivirus. Microsoft Defender for Endpoint is actually multiple technologies and services combined for powerful and easy-to-manage endpoint security.



Source: https://www.microsoft.com/en-ca/microsoft-365/security/endpoint-defender

So, how did they do it?

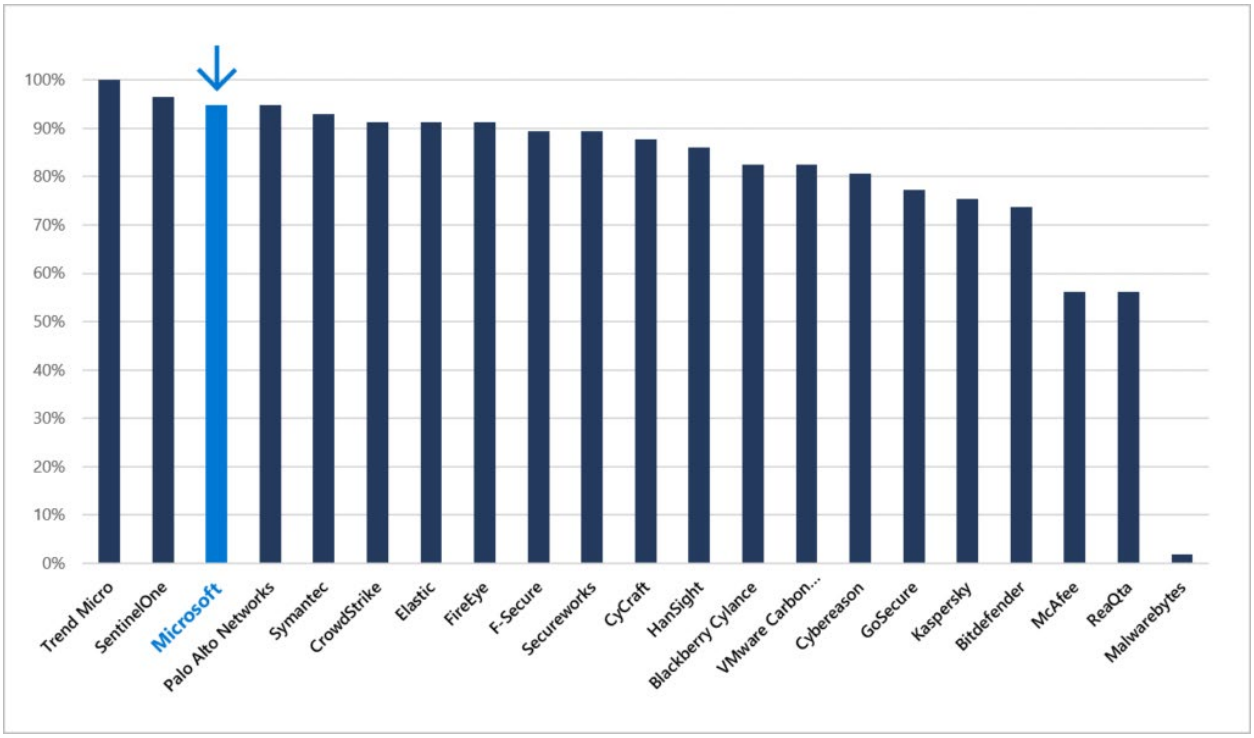
Providing full protection out-of-the-box required a lot of innovation, automation, and orchestration with other security products and services. In recent MITRE ATT&CK® evaluations, Microsoft Defender for Endpoint came out a clear winner with broad detection capabilities which required the least configuration.



Source: https://www.microsoft.com/en-ca/microsoft-365/security/endpoint-defender

Rather than addressing specific vulnerabilities, the MITRE ATT&CK® framework describes the tactics and techniques used by threat actors to gain an initial foothold, move laterally, and ultimately carry out their desired outcome—violating the availability, integrity, or confidentiality of systems.

By measuring EDR solutions' detection coverage of tactics and techniques, we get a better understanding of how they will perform in uncertain future situations in production environments.



Source: https://www.microsoft.com/en-ca/microsoft-365/security/endpoint-defender

Not surprisingly, Microsoft achieved 95% coverage for the techniques used in the test, beating out notable providers like CrowdStrike, FireEye, Blackberry Cylance, and more. This performance, when combined with the enhanced compatibility Microsoft's solutions offer, makes them an ideal choice for any company looking to get serious about cybersecurity.

What Can You Do With Microsoft Defender for Endpoint?

Microsoft Defender for Endpoint continues to be a notable focus for ongoing feature development by Microsoft, boasting a full roadmap and executive commitment to long term investment and support.

Security is perhaps one of the fastest growing areas within Microsoft as a whole. Of the many features provided by the Microsoft Defender suite, we've highlighted a few that we feel set it apart from the crowd:

- **Multi-Layered Protection:** Microsoft Defender for Endpoint provides multi-layered protection (built into the endpoint and cloud-powered) from file-based malware, malicious scripts, memory-based attacks, and other advanced threats.
- **Threat Analytics:** Contextual threat reports provide SecOps with near real-time visibility on how threats impact their organizations.
- **Threat & Vulnerability Management:** Real-time discovery, prioritization based-on business context and dynamic threat landscape, and built-in remediation process speed up mitigation of vulnerabilities and misconfiguration.
- **Built-In, Cloud-Powered Protections:** Real-time threat detection and protection with built-in advanced capabilities protect against broad-scale and targeted attacks like phishing and malware campaigns.

- **Behavioral Detections:** Endpoint detection and response (EDR) sensor built into Windows 10 for deeper insights of kernel and memory, and leveraging broad reputation data for files, IPs, URLs, etc., derived from the rich portfolio of Microsoft security services.
- **Easy Deployment and Maintenance:** Built directly into the Windows operating system, there are no delays or compatibility issues, and no additional performance overhead or conflicts with other products. Automated deployment and no on-premises infrastructure directly leads to lower TCO.
- **Threat Containment:** Dramatically reduces the risk by strengthening your defenses when potential threats are detected. Microsoft Defender can automatically apply conditional access to restrict the endpoint from accessing corporate data until the threat was remediated.
- **Response Automation:** From alerts to remediation in minutes – at scale. Microsoft Defender leverages AI to automatically investigate alerts, determine if a threat is active, what course of action to take, and then remediate complex threats in minutes.
- **Secure Score:** Microsoft Defender not only tells you that you have a problem, but Microsoft Defender also recommends how to solve it (and track the execution) with Secure Score. Vulnerability and configuration information provide weighted recommendations and actions to improve endpoint hardening and compare the current posture with the industry and global peers for benchmarking.

It's Time to Get Serious About Microsoft

There's no denying how far Microsoft has come in the cybersecurity space. They have long outgrown the initial growing pains they experienced when they launched their first antivirus solution in 2005.

They spent over a decade collecting and analyzing billions of data points for key usage insights, building outcomes-based solutions, innovating on functionality, and creating an integrated experience built around the foundations of security and visibility.

No one collects more data than Microsoft, and this data is what matters when it comes to building best-in-class systems that leverage the latest innovations in machine learning and artificial intelligence. The billions of Windows users have created arguably the most powerful set of cybersecurity training data in existence.

What does all of this mean for enterprises today? The answer is simple.

When it comes to implementing a successful cybersecurity program today, the Microsoft question shouldn't be a consideration, it should be the starting point.

About Difenda:

Difenda is a privately held SecOps-As-A-Service company founded in 2008. We deliver 24.7.365 security operations backed by our modernized PCI, SOC 2 Type 2 and ISO27001 certified Cyber Command Centers. Difenda's MDR practice is powered solely on the Microsoft security product stack and as a company proudly holds the Gold Security Service Provider certification for Microsoft. We are an outcome-driven security services company with a fully integrated and modular platform that leverages an agile, innovative and collaborative approach with our Difenda Shield, along with advisory and offensive security services.

VISIT US TO LEARN MORE