REPORT REPRINT

Microsoft expands capabilities and platforms for Microsoft Defender ATP

JULY 31 2020

By Fernando Montenegro

The company has been pouring significant resources into growing its capabilities as a provider of security functionality. It appears to be making significant inroads into the endpoint security space, given its role behind the Windows OS and on account of its Defender ATP offering, which was recently updated.

451 Research® Now a Part of

S&P Global Market Intelligence

Introduction

Endpoint security had been growing in importance as a key component of security architecture even before the COVID-19 health crisis. Back then, key trends such as user mobility, BYOD and increased use of encryption already meant that properly securing and capturing telemetry from endpoints was crucial for protection, detection and incident response. The COVID-19 crisis merely accelerated this as network connectivity patterns changed and corporate offices sat empty.

In recent years the endpoint security market has seen significant change, including the rise in popularity of Microsoft's offerings, particularly its Microsoft Defender Advanced Threat Protection (MDATP) component. The company has been expanding the capabilities of the product as it adds support for new environments and partners.

451 TAKE

In an age of user and workload mobility, the arc of security preferences is shifting back toward endpoint-centric security controls being heavily favored by enterprises, which has led to a crowded marketplace of endpoint security vendors. Microsoft has been growing as a competitor in this space with the combination of protection and detection/response offerings. Microsoft Defender ATP aims to offer a broad swath of capabilities around the typical workflows associated with endpoint security while integrating with the rest of Microsoft's broad portfolio and accounting for the typical resource constraints that many organizations face. Organizations have become more receptive to this approach and are considering Microsoft more often as they evolve their security architectures. Provided that Microsoft can address the concerns some may have about separation of duties and maintaining broad support for non-Windows environments, it should see its profile grow in endpoint security.

Context

Microsoft is one of the pillars of the IT industry and a household name for both consumers and enterprises. The company has taken a significant interest in security, having improved the security of baseline products such as Windows and Office and the Azure and Office 365 cloud services. Microsoft has made numerous purchases in security, including Adallom for cloud security, Hexadite for automation and CyberX for IoT security.

Microsoft's endpoint security capabilities have their roots in its acquisition of the GIANT AntiSpyware product in 2004. That functionality was incorporated into the operating system as Windows Defender Antivirus, with a focus on endpoint protection. Microsoft recently renamed the feature as Microsoft Defender Antivirus. The company later released Microsoft Defender ATP, which augments endpoint security functionality beyond protection features.

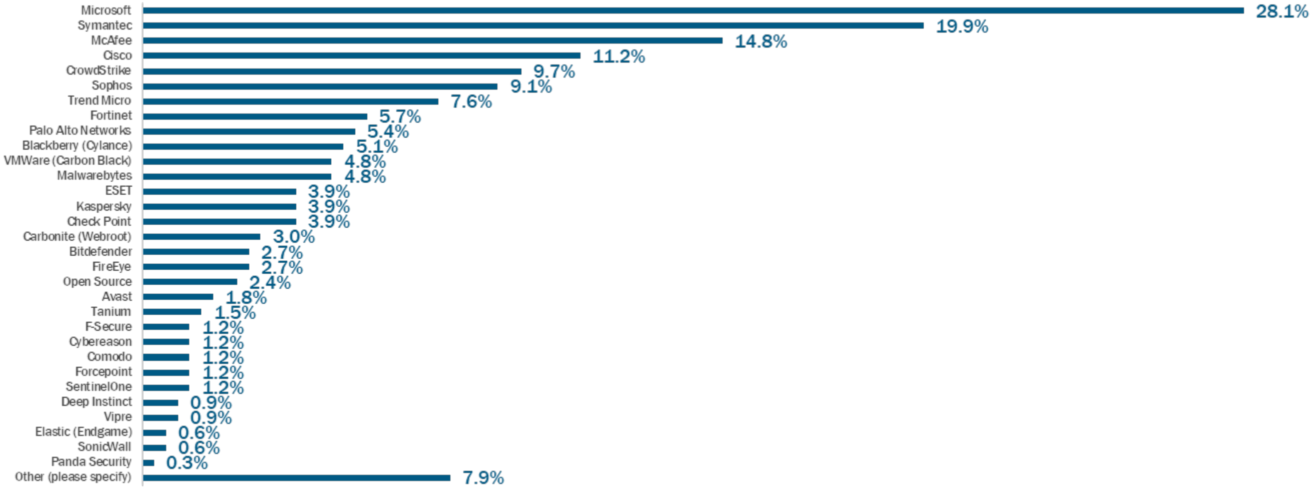
Market

While Microsoft does have presence in other markets, the Microsoft Defender ATP offering fits squarely within what 451 Research labels the endpoint security market. This market initially consisted of security vendors focusing on endpoint protection (antivirus, anti-malware and others). It then added use cases such as endpoint detection and response (EDR), which focuses on detecting, investigating and responding to security incidents on the endpoint. Later, it added use cases such as mobile device security and ancillary functions.

Some of the key trends in the market include the fusion of protection, detection and response use cases; the rise of machine learning (ML) techniques; and the use of cloud-based resources for analytics. There's also a strong push toward adding functionality without adding new software agents, which plays to Microsoft's strength in the context of Windows endpoints. According to 451 Research's Voice of the Enterprise research programs, a significant number of respondents with endpoint security pilots or plans to deploy in the next 6-24 months indicate that they look to Microsoft as a vendor 'in consideration.'

Which vendors are cited as 'in consideration' for endpoint security?

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2020



Sample Size = 331

Base: Respondents currently using Endpoint security technology

Strategy

As it makes a push into endpoint security, Microsoft's thesis is that it can combine three key strengths: its role in providing the underlying OS that underpins much of modern computing, its presence in numerous organizations of all sizes and verticals, and its reach as a provider of planetary-scale cloud services, which gives it access to significant telemetry across multiple domains.

While the company is positioning Microsoft Defender ATP for customers of different sizes and in different verticals, the offering typically aligns with workflows and practices associated with larger enterprise vendors. The company has emphasized partnerships it has developed or is in the process of developing with numerous technology and services partners, including but not limited to IBM, Splunk, Anomali, Red Canary and Secureworks.

While Defender ATP was originally bundled with pricier Microsoft 365 E5 licenses (both regular E5 and E5 Security) or as an add-on to a Windows 10 E3 license, the company recently released Defender ATP as a stand-alone license to be added to Windows Pro licenses. Server licenses are available for Windows and Linux.

Technology

Users looking for endpoint security functionality typically consider both endpoint protection and EDR use cases. Microsoft Defender ATP is the company's main offering for the EDR use case, although it cooperates with Windows Defender, the company's endpoint protection agent. The ATP moniker stands for Advanced Threat Protection, which is also used by Microsoft elsewhere in its portfolio (Azure ATP, Office 365 ATP).

MDATP is 'agentless' in modern Windows 10 and Windows Server installations since much of the functionality for deriving telemetry is already embedded into the operating system. Microsoft has released additional agents that can be used in different versions of Windows, as well as support for Mac and Linux endpoints. The company also recently introduced support for Android devices.

MDATP includes threat and vulnerability management functionality, which is used to discovery vulnerabilities, help prioritize corrections, and deploy IT and security workflows to remediate issues. The latest release of Defender ATP added, among other things, API access to data elements and ServiceNow integration support.

The Attack Surface Reduction (ASR) features in the product leverage operating system features and are used to isolate access to suspicious resources, be they files or sites. The recent developments to ASR include support for better managing local firewall rules, better support for certificates and more visibility into Web activity by the user.

The endpoint protection functionality of Microsoft Defender ATP is deeply tied to the Windows Defender protection engines and leverages a variety of techniques, including numerous machine learning models and built-in operating system security features. This integration also benefits from the telemetry captured by Microsoft within offerings such as Office 365 and Azure.

Endpoint detection and response use cases are the core functionality of Microsoft's offering. The product is used to correlate alerts, conduct investigations or threat hunting exercises, and coordinate response actions. It leverages the built-in telemetry from Windows devices, including process/file activity and signals from kernel, memory, registry and other components. Recent additions include better support for MacOS clients, newer EDR/behavior blocking, integration of live response capabilities and MITRE ATT&CK framework alignment.

Responding to incidents is a key step in any security practice, with many organizations struggling with overtaxed resources to respond at scale and in a timely fashion. As is the case with other EDR tools, MDATP includes support for auto investigations and remediations. The capabilities are aimed at assisting human response in the context of investigations and containment, if necessary. Microsoft recently added support for integrating MDATP responses with those on Office 365 ATP and Azure ATP.

Microsoft rounds out its offering with capabilities around integrated security management as part of a broader endpoint management strategy, as well as service offerings around providing remote incident-response support and independent threat hunting.

Competition

Despite significant consolidation in the past couple of years, large and small, the endpoint security market remains an active environment with several competitors looking to address specific nuances of the market.

In the context of large, well-known vendors, Symantec was acquired into Broadcom and shifted its go-to-market strategy, but is still present in large accounts and likely to remain a key competitor. Other well-known vendors, such as McAfee, Trend Micro, Sophos and Kaspersky, are also present across the world.

With the acquisitions of Cylance and Carbon Black by BlackBerry and VMware, respectively, those two vendors become stronger competitors, particularly as they look to offer unified endpoint management in a way that consolidates endpoint security functionality. Other large vendors – Cisco and Palo Alto Networks primarily, although Check Point and Fortinet are also present – offer a consolidation story of endpoint security into a network-centric view of security.

In the context of more focused endpoint security vendors, CrowdStrike has emerged from its IPO in 2019 as a significant provider of endpoint security functionality, while specialists Cybereason, SentinelOne and others are also present. Other vendors of note include FireEye, Tanium, OpenText, Malwarebytes, Bitdefender and ESET.

Microsoft is looking to differentiate based on the overall integration of endpoint security functionality into its broader IT management offerings, as well the combined effect of leveraging telemetry from its broad industry presence.

SWOT Analysis

STRENGTHS

Microsoft offers deep integration between Defender ATP and the rest of the operating system, and continues to add support for further functionality, new environments and integration with the rest of the Microsoft portfolio.

WEAKNESSES

Microsoft's non-Windows offerings – Mac and Linux – typically lag the main Windows-centric functionality and security features. Furthermore, the frequent branding, packaging and licensing changes to Defender ATP have introduced confusion in the market that may hamper increased adoption.

OPPORTUNITIES

The pressures faced by many organizations today have led to a broad push for simplification and streamlining of security controls. This simplification can exist in the form of relying on fewer, more-strategic vendors and by simplifying the technical footprint on endpoints. Microsoft can legitimately fit into both categories.

THREATS

Many organizations prefer to implement security technology following a 'segregation of duties' mindset, and may be hesitant to rely on the same vendor for both the technology platform and some of the security controls for that same platform.