MORPHISEC
Moving Target Defense

WHITEPAPER

OPTIMIZING
THE SECURITY STACK
WITH MORPHISEC AND WINDOWS DEFENDER

EXECUTIVE SUMMARY

The commonly accepted approach to protect endpoints from advanced, unknown cyber threats involves using multiple agents or a next generation EPP suite that includes multiple components. The expectation is that these agents together offer a much higher level of protection against advanced attacks than any single agent alone.

While this logic may be sound, the technologies themselves fall short. The agents must detect or predict malicious activity, which requires knowledge of what is being detected or predicted. Such agents prove ineffective against unknown attacks, fileless attacks, and evasive, polymorphic and in-memory techniques that are the preferred tools of modern adversaries. Moreover, they impact endpoint performance and IT operations. Detection agents monitor and/or apply rules, which is disruptive and computationally intensive. They also generate numerous alerts to analyze and act on as their predictions are probabilities, not certainties. The result is an endless process of adding more agents, with minimal incremental security benefit, for maximum cost and effort.

The inefficiency and ineffectiveness of this approach becomes evident when considering one of the most dangerous problems facing security practitioners: memory attacks. Memory attacks, or fileless attacks, use legitimate system applications and resources as an attack vector. Ponemon's 2020 State of Endpoint Security Risk study shows that 68% of organizations believe a fileless attack is likely to compromise their systems.

It is possible to build a powerful, inexpensive and easy-to-manage endpoint security stack that stops these attacks in their "unknown" stage deterministically, without guessing or predicting. The foundation of such a stack is moving target defense — dynamic morphing of the runtime environment. This prevents unknown attacks instantaneously, with zero dependency on discovery, analysis, characterization, detection, or updates.

Windows 10 itself forms the other cornerstone of this stack. When fully leveraged, the security tools embedded in the operating system become a formidable defense against known attacks, with protection on-par with any next generation antivirus technology.

This whitepaper examines the optimal way to protect endpoints from both known and unknown attacks. It reviews the Windows Defender Antivirus offering, barriers to adoption and mitigations provided through the Defender AV integration available in the Morphisec Unified Threat Prevention platform. It looks at how Morphisec's moving target defense technology, coupled with Defender, helps organizations build an endpoint security stack that is potent, cost-effective and easy to use.

CONTENTS

INTRODUCTION

Although enterprise spend on security is skyrocketing, ESG reports that **55% of organizations indicate that threat prevention/detection remains one of their greatest challenges**[1]. At the same time, other research by the analyst firm found that 25% of cybersecurity and IT professionals state their security teams spend too much time responding to and investigating alerts, many of which are false alarms. Clearly, the paradigm of more products and more layers does not work.

A better security stack can be built, but it requires revisiting the idea that true prevention is not possible. By making "prevention first" an imperative, and incorporating innovative technology that follows this imperative, the cyberdefense stack can be simplified to four basic layers: network defense, access control, protection against unknown and memory-based attacks, and antivirus to prevent known threats.

[1] Source: ESG Master Survey Results, *Modern Endpoint Management*, December 2018.

INTRODUCTION (CONTINUED)

Until recently, the recommended antivirus component of the security stack for Windows organizations was one of the top third-party vendors as most experts regarded the Microsoft security offerings as inadequate. Advanced evasive cyberattacks could easily bypass Microsoft tools such as ASLR, DEP, EMET and the fledgling Microsoft antivirus product.

However, the powerful array of embedded Windows 10 security tools — Device Guard, Application Guard, BitLocker and other controls, plus Windows Defender Antivirus — has changed the playing field. Originally Defender Antivirus was considered markedly inferior to leading third-party products, based on numerous independent AV tests. However, steady improvements and upgrades have beefed up Defender AV protection significantly, making it a worthy next gen antivirus contender. It provides protection against millions of known malware for desktops, portable computers, and servers.

Of course, like all detection-based security technology, Defender offers limited protection against unknown, evasive cyberattacks and memory-based attacks. The addition of a layer of memory and advanced threat protection is recommended to be used in conjunction with Windows Defender (or similar AV product).

This report investigates the viability of Windows Defender as an antivirus choice for enterprises as part of a modern and simplified stack. It looks at how the Morphisec-Windows Defender AV integration for endpoints and servers delivers protection far superior to other security solutions and combinations of solutions at considerably lower cost.

ABOUT WINDOWS DEFENDER ANTIVIRUS

BACKGROUND

Windows Defender started as a downloadable anti-spyware tool in Windows Vista and Windows 7 but was upgraded to a full-fledged antivirus program in Windows 8. While initial reviews were unfavorable compared to other antivirus tools, it has undergone substantial improvements, including enhanced anti-malware protection, and the Windows 10 version is considered among the best both in terms of protection and operational performance. Windows Defender AV is also included in Windows Server 2016 and later.

Microsoft Defender for Endpoint is a separate EDR product that Microsoft introduced in 2016 for enterprise businesses as part of its E5 offering. It has its own benefits and limitations, but that is outside the scope of this document. Morphisec is part of the Microsoft MISA program and has a separate integration with Defender for Endpoint.

HIGHLIGHTS

Windows Defender Antivirus provides multi-level protection against threats like viruses, malware and spyware, without slowing systems down. Defender has access to the same threat feeds and information sources as other next-generation antivirus products as well as its own massive malware repository.

CLOUD-DELIVERED PROTECTION

Works seamlessly with Microsoft cloud services to deliver next gen technologies that provide near-instant detection and blocking of new and emerging threats. These technologies use advanced machine learning models and work with large, interconnected data sets from the Microsoft Intelligent Security Graph to dynamically identify new threats.

ALWAYS-ON SCANNING

Uses advanced file and process behavior monitoring and other heuristics to identify malware based on known suspicious and malicious activities. It also can detect and block potentially unwanted applications.

DEDICATED PROTECTION UPDATES

Microsoft delivers regular engine updates and new malware definitions based on machine-learning, human and automated big-data analysis, and in-depth threat resistance research.

DOES NOT CAUSE CONFLICTS

As a built-in component of Windows, there are no conflicts between Defender and other endpoint products.

MANAGEMENT AND CONFIGURATION

Since Windows Defender AV is already installed with Windows 10, deployment is unnecessary. It is managed using System Center Configuration Manager or Microsoft Intune.

Multiple methods can be used to configured Windows Defender, including: System Center Configuration Manager (as System Center Endpoint Protection, or SCEP), Microsoft Intune, PowerShell, Windows Management Instrumentation (WMI) and Group Policy.

WHY WINDOWS DEFENDER?

For an Enterprise customer, Windows Defender is available by default and for free. It utilizes SCCM or Intune to manage the product, which Microsoft customers will already be familiar with.

Deployment is non-existent, eliminating what can be a real time sink for IT teams. Tasks such as troubleshooting, reaching remote systems and detailing compatibilities are all abolished.

There are other benefits to using built-in Windows security. There's no need to manage separate updates — new builds of Windows Defender are pushed via Windows Update. It can integrate more tightly and seamlessly with the Windows system, for example working with User Account Control requests and to scrub malware from the Windows Recovery Environment. It does not slow down systems with additional components, like additional registry cleaners, optimizers or browser extensions.

Until the release of Windows 10, Defender ranked as one of the weakest antivirus programs available. This is no longer the case. Windows Defender has successively improved with each update.

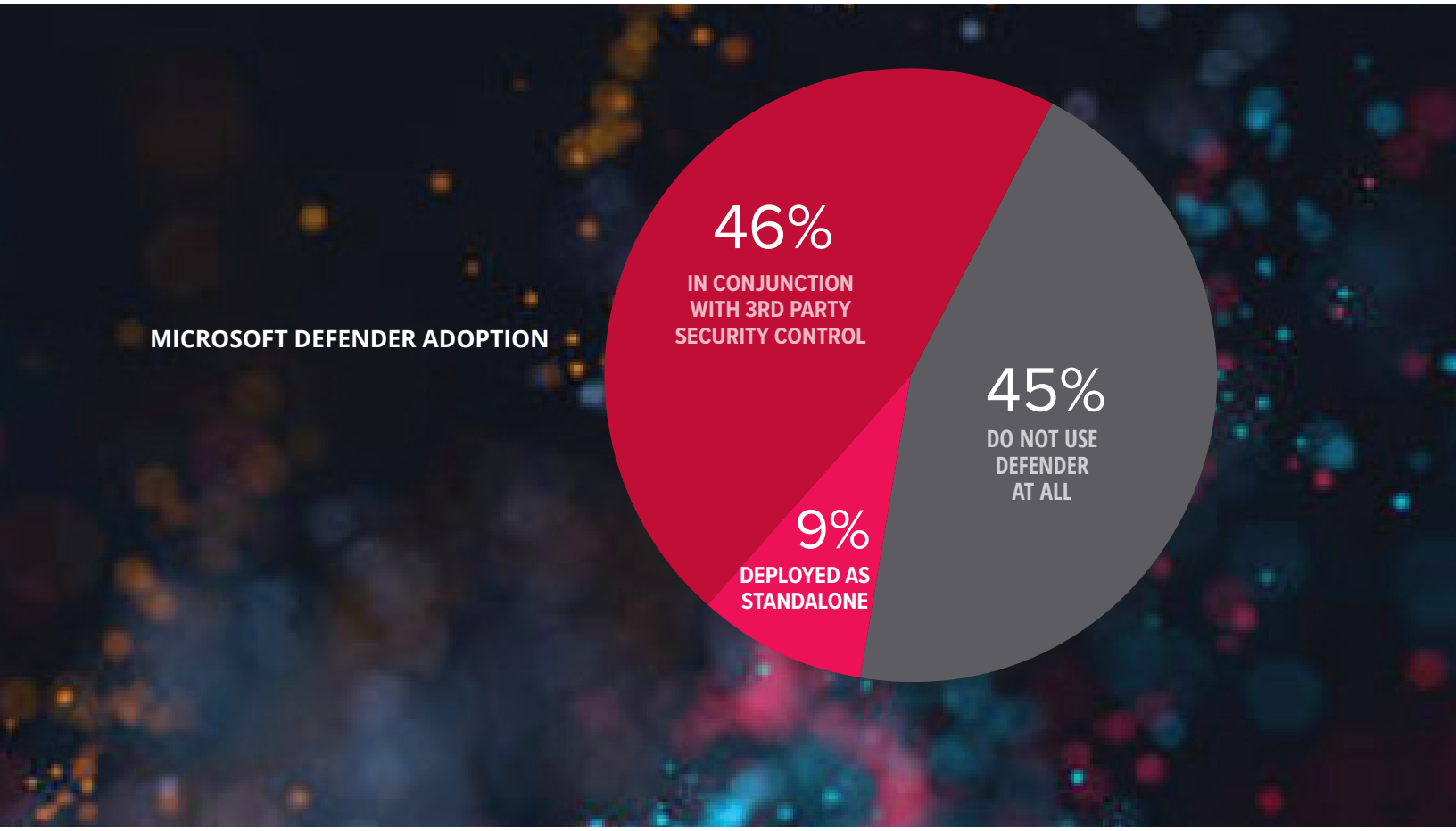
This is evidenced in the February 2020 evaluation performed by perhaps the most respected testing lab, AV-Test, where Defender received a "Top Product" award on a Windows 10 system. Defender received perfect scores for protection and usability and nearly as high in performance. What's more, Defender has achieved such scores in every test since June 2018.

Organizations looking to replace their antivirus can consider Microsoft Windows as a viable, highly cost-effective option, provided they migrate to Windows 10 OS in a consistent, phased manner.

BARRIERS TO WINDOWS DEFENDER ADOPTION

Given Defender's ratings and unbeatable price point, it is somewhat surprising that Defender adoption has not kept pace with its improvements. A recent ESG survey of IT professionals found that only 9% of organizations have deployed Defender as a standalone, antivirus/anti-malware endpoint security control, 46% use it in conjunction with third-party endpoint security controls and 45% do not use it at all. When asked why they don't use Windows Defender, 43% of organizations said it doesn't provide all the security features that they require, while another 41% indicated that they don't believe that Microsoft's endpoint security software and services are as strong or as comprehensive as other alternatives.

Another barrier to adoption is the lack of enterprise-wide visibility into events from Defender AV, unless the organization is also using Microsoft Defender for Endpoint and its Security Center. Otherwise, the security team would generally need to build custom policies to withdraw event logs to a central system such as an SIEM in order to view Defender AV alerts across the enterprise.



WINDOWS DEFENDER PLUS MORPHISEC

No detection-based security solution is enough. All require prior knowledge in order to detect or predict malicious activity, leaving them ineffective against unknown, evasive attacks. The technologies they use — whether signatures, static analysis, anomaly detection, file reputation or artificial intelligence — are known to and monitored by adversaries, who constantly engineer new attacks to bypass them.

Yet organizations cannot keep on adding security tool after security tool until their IT systems and security teams no longer function effectively. A sounder strategy consolidates technologies to a few trusted vendors, ensuring that existing staff has the skillset and experience to manage critical solutions and reducing the chances of misconfigurations and other missteps that can lead to potentially devastating consequences.

Organizations need a defense-in-depth approach that includes advanced attack protection against unknown threats, and where each component measurably reduces residual risk. Such a carefully considered strategy ensures that IT, business and security needs are all aligned.

Morphisec adds a critical protection layer to prevent highly evasive in-memory attacks that are able to bypass signature and AI-based solutions such as Windows Defender AV and other next-gen antivirus solutions.

Morphisec is based on Moving Target Defense, a transformational cyber defense technology that prevents threats at their very earliest stages, without detecting, guessing or hunting for missed attacks.

Morphisec works alongside more traditional protection layers such as Perimeter, Access Management and Antivirus as part of an overall defense in-depth posture. It prevents advanced, evasive attacks that exploit memory, applications and processes, and which often bypass detection-based products (such as signature, behavior, ML, AI, whitelisting and privilege management). Moreover, Morphisec is extremely simple to operate and has zero impact on performance at runtime, something no other security control can claim.

MORPHISEC-WINDOWS DEFENDER INTEGRATION

Enterprises have a unique opportunity to replace their legacy antivirus tools with the free, embedded Microsoft Defender AV, however the tool's lack of comprehensive reporting has been a major obstacle to adoption. Morphisec's Defender integration changes this. Morphisec provides a consolidated view of all attacks on the endpoint, including real-time attacks detected by Defender AV. Organizations can adopt Defender AV, and use Morphisec to see all Defender AV activity along with the severity level.

Security teams can correlate these events with Morphisec prevented threats to understand the impact of the events on the enterprise and make any necessary policy or remediation decisions. For example, a more restrictive Morphisec protection plan can be imposed on endpoints that are identified as highly targeted.

Windows Defender AV and Morphisec Unified Threat Prevention together provide the strongest, broadest endpoint protection within the most cost-effective and operationally sound strategy.

MORPHISEC KEY BENEFITS

Morphisec offers enterprises uncompromising protection yet is extremely simple to operate.

Prevents Zero Days and Advanced, Evasive Attacks

Other solutions use a combination of technologies to protect organizations against advanced attacks. These include signatures, sandboxing, AI and behavior anomaly detection. They rely on research to discover and patch vulnerabilities, and known attack patterns to predict new variants. These methods do not address the attacker's primary advantage — namely the static nature of systems and networks vs. dynamic, changing threats and attack techniques. Attackers design attacks for existing but not yet revealed vulnerabilities, and engineer new evasive variants that don't resemble known patterns.

Morphisec's Moving Target Defense is a pre-emptive early prevention strategy that makes the targets under attack dynamic and unpredictable. It does not require updates to protect against new attack trends and provides the same level of protection for the user irrespective of internet connectivity.

Virtual Patching for Applications and Operating Systems

Patch Management is a significant expense and headache for any organization and patches are often applied to critical systems first — only later are end user systems patched. Applications (browsers, Office Suite, Acrobat, Flash, etc.) usually have the lowest patching priority even though they are a favorite infiltration point for attackers.

Morphisec prevents the exploitation of vulnerabilities in commonly used applications and operating systems. It acts as a virtual patch, removing the need for any critical patch response and shrinking risk. It also provides a mitigating technology that qualifies as a compensating control for Windows 7 deployments after Microsoft ends support for the OS in January 2020.

No Business Disruption to Users

Unlike traditional endpoint solutions, Morphisec does not affect the stability and performance of the end-user system. It does not create any performance degradation, disruption to users, BSODs, or risk to operations.

Fast Deployment

Morphisec employs a single lightweight agent that can be deployed easily and quickly, resulting in immediate protection and faster ROI for the organization.

Reduces Security Operational Costs

Morphisec is a set and forget solution that stops attacks deterministically, as opposed to calculating the probability of malicious intent. This means there are no false alerts to investigate and there is no need to analyze or remediate missed threats.

CONCLUSION

A lean, highly effective cyber defense stack consists of perimeter control, identity access control, memory defense and antivirus protection. These components should be chosen carefully according to optimal performance, efficacy and cost-efficiency criteria.

Microsoft Windows Defender has emerged as a clear, viable candidate for next-gen antivirus protection. Upgrades to its protection abilities, combined with its native Windows integration and that it is available at no cost should make organizations seriously consider migrating to Windows Defender as they migrate to Windows 10.

Organizations seeking to strengthen their security posture, without increasing cost and complexity, can scrap their legacy antivirus, turn on the Windows 10 embedded Defender AV, and apply their savings to Morphisec to protect against advanced memory-based attacks that are able to bypass detection-based security tools. This combination allows organizations to build the optimal, defense-in-depth security stack.

ABOUT MORPHISEC

Morphisec has revolutionized endpoint protection with its Moving Target Defense technology, which instantly and deterministically stops the most dangerous and evasive attacks while allowing companies to cut operational costs. With a true prevention-first approach to stopping zero-days, with no false positives, Morphisec eliminates the complexity and burden for organizations struggling to respond to cyberattacks.