

Technical Validation

Efficient Efficacy with Morphisec Unified Threat Prevention Platform

By Jack Poller, Senior Analyst

June 2019

This ESG Technical Validation was commissioned by Morphisec and is distributed under license from ESG.



Contents

| | |
|---|----|
| Introduction..... | 3 |
| Background..... | 3 |
| Morphisec Unified Threat Prevention Platform..... | 4 |
| ESG Technical Validation | 5 |
| Operational Efficiency..... | 5 |
| ESG Testing | 5 |
| Attack Prevention Efficacy | 8 |
| ESG Testing | 8 |
| Integrations | 11 |
| ESG Testing | 11 |
| Microsoft Defender AV Integration | 12 |
| The Bigger Truth | 14 |

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Introduction

This ESG Technical Validation documents evaluation of Morphisec's moving target defense-powered Unified Threat Prevention Platform. We focused on understanding the operational simplicity of the platform and the efficacy of its threat prevention capabilities.

Background

The ever-increasing volume and velocity of threats has made cybersecurity one of the top IT concerns. In addition to securing the network, the on-premises infrastructure, and the cloud, IT must focus on the numerous endpoints in use. According to ESG research, organizations face myriad challenges securing their endpoints, and 55% indicate that threat prevention/detection is one of their greatest challenges, making it the second most cited challenge (see Figure 1).¹

Figure 1. Greatest Endpoint Security Challenges



Source: Enterprise Strategy Group

What is driving these endpoint protection challenges? ESG's annual technology spending survey revealed that cybersecurity has emerged as IT's top mandate, with 40% of organizations indicating that strengthening cybersecurity will be a top business driver for their technology spending in 2019. However, improving the business' security posture is complicated by the global skills shortage—53% of organizations report a critical lack of cybersecurity skills.²

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

² Source: ESG Research Report, [2019 Technology Spending Intentions Survey](#), February 2019.

As a result, organizations evaluating their options for strengthening cybersecurity are seeking more efficient and effective tools. Indeed, according to ESG research, 46% of surveyed IT and cybersecurity decision makers ranked effectiveness as the most important consideration when investing in cybersecurity products or services.³

Morphisec Unified Threat Prevention Platform

Morphisec, an Israeli-based cybersecurity vendor with headquarters in Boston, MA, provides advanced threat prevention defenses while maintaining operational simplicity.

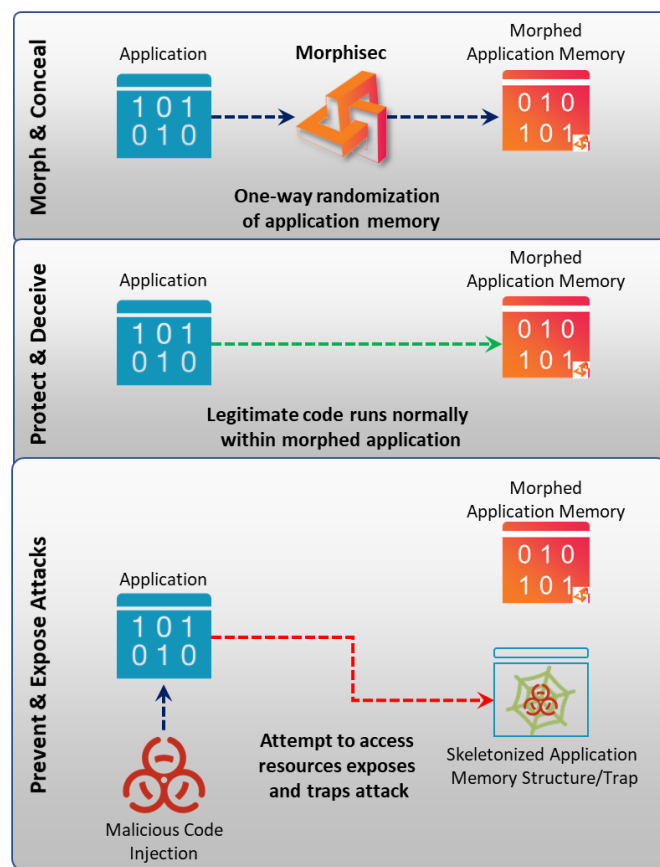
Morphisec designed its platform to prevent fileless attacks, zero-day exploits, and evasive malware at the earliest stage of attack without the need for IOCs. Using a lightweight, small-footprint agent that deploys into existing security infrastructure, Morphisec blocks threats pre-execution, preventing damage and lateral movement.

Morphisec’s “moving target defense” employs attacker stealth tactics—deception, obfuscation, modification, and polymorphism—to preemptively prevent attacks. When an application loads into memory, Morphisec’s polymorphic engine employs keyless, one-way randomization to transform the process structure, morphing libraries, functions, variables, and other data segments.

Each application instance is uniquely mutated, cloaking the application and making application memory unpredictable to attackers. Legitimate application code is updated with the morphed resources while a lightweight skeleton of the original application structure is maintained as a trap.

Malicious code injected into the application targets the original memory structure and gets captured by Morphisec, while the transformed application runs normally using the transformed application memory. Attacks are prevented, trapped, and logged, along with rich forensic data for analysis.

Morphisec’s moving target defense neutralizes advanced attacks and browser-based threats at the earliest stage, independent of threat type, technique, or behavior. Deploying Morphisec provides real-time protection and comprehensive patch gap coverage by preventing exploitation of unpatched vulnerabilities. The Morphisec agent is lightweight, active only at application load time, providing security without impacting performance and requiring no maintenance.



³ Source: ESG Master Survey Results, [Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms](#), October 2018.

ESG Technical Validation

ESG performed evaluation and testing of Morphisec’s moving target defense-based Unified Threat Prevention Platform. Testing was designed to demonstrate how Morphisec’s platform can help organizations efficiently and effectively protect their endpoints.

Operational Efficiency

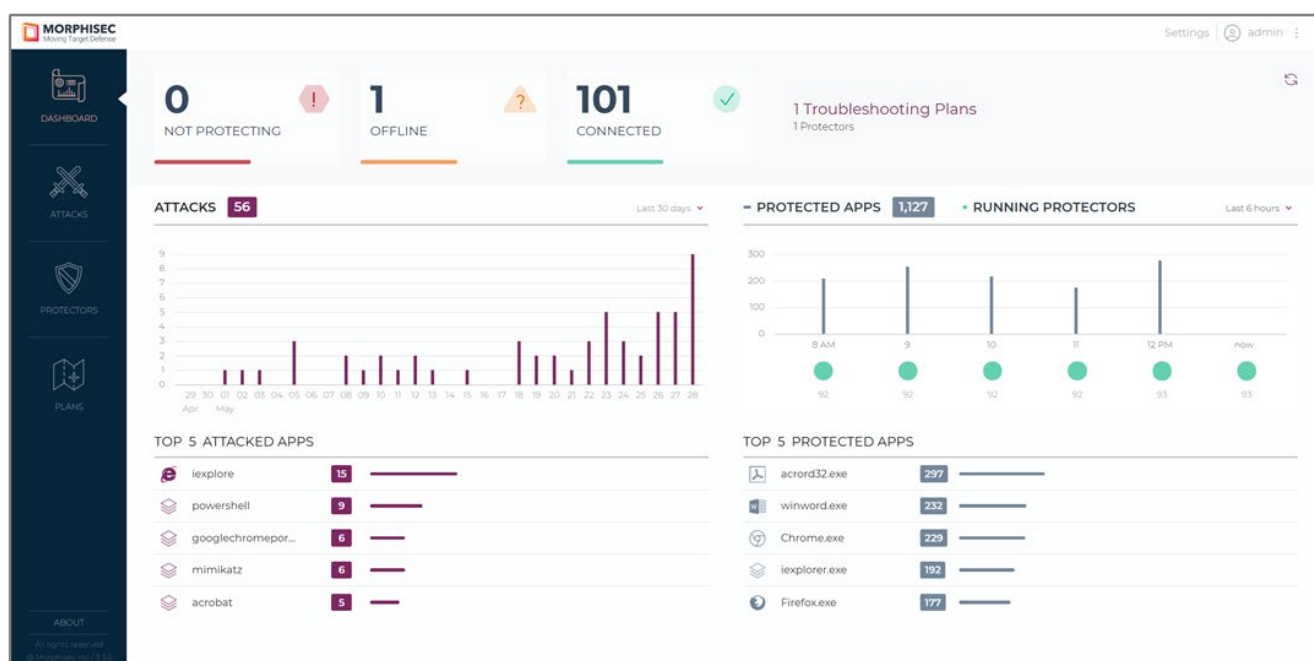
Morphisec’s moving target defense employs decoy technology to prevent threats without the need to first detect. As part of the application load process, Morphisec mutates the application memory, relocating internal application functions and leaving a skeletonized version in the original function locations to act as a trap. When malicious code is inserted and executed, the malicious code will attempt to use the original memory structure and will be trapped.

Thus, alerts generated when an attack is trapped are guaranteed to be the result of malicious activity and there is almost no chance of generating a false positive alert. This frees cybersecurity analysts from the onerous task of determining the veracity of alerts. Instead, cybersecurity teams can focus on root cause analysis—understanding how the malicious activity penetrated defenses to the point at which it was captured by Morphisec. Using this knowledge, cybersecurity practitioners can improve their defenses to avoid future compromise.

ESG Testing

ESG started by launching the Morphisec web-based dashboard. As shown in Figure 2, the dashboard provides easy-to-interpret information about the state of the organization’s endpoint protection. At the top of the dashboard are tallies of the number of endpoints protected or not protected by Morphisec. Two panels provide timelines with bar charts for the number of attacks and number of protected applications (Morphisec can be configured to protect all or just a subset of applications). Two additional panels provide top-five listings for apps being protected and apps under attack.

Figure 2. The Morphisec Dashboard



Source: Enterprise Strategy Group

The dashboard provided us with a comprehensive understanding of the organization's cybersecurity posture and endpoint protection. In this case, we were experiencing anywhere from zero to nine attacks per day, and Internet Explorer was the target of the majority of attacks.

Next, we selected the **Protectors** option from the left-side menu, which brought up the list of endpoints protected by Morphisec, as shown in Figure 3. This list provided the usual and necessary endpoint demographic information, enabling us to understand which systems were more vulnerable or less so, based on OS and the state of Morphisec running on each system. Morphisec's protection service itself is protected and cannot be turned off or disabled without an administrator password. (The Morphisec agent on the systems at the top of the list were manually stopped for ESG's evaluation.)

Figure 3. List of Endpoints Protected by Morphisec

| Last Heartbeat | User | Machine | Org Unit | Plan | Version | OS | License Type |
|-------------------|-------------------|---------|-----------|---------------------------|---------|------------|--------------|
| 28 May 19 1:32 PM | MTD-DOME/BarryW | PC-1038 | VDIPOOL01 | auto default plan (UPD... | 2.7.2 | Windows 7 | |
| 28 May 19 1:32 PM | MTD-DOME/IvankaT | PC-1607 | Computers | auto default plan (UPD... | 2.7.2 | Windows 7 | |
| 28 May 19 1:32 PM | MTD-DOME/AxelRo | PC-236 | VDIPOOL07 | auto default plan (UPD... | 2.7.2 | Windows 10 | |
| 28 May 19 1:32 PM | MTD-DOME/SamBa | PC-1128 | VDIPOOL05 | auto default plan (UPD... | 2.7.2 | Windows 10 | |
| 28 May 19 1:33 PM | MTD-DOME/ShirleyT | PC-1101 | Computers | auto default plan (UPD... | 2.7.2 | Windows 7 | |
| 28 May 19 1:33 PM | MTD-DOME/KarryB | PC-875 | Computers | auto default plan (UPD... | 3.0.0 | Windows 7 | |
| 28 May 19 1:33 PM | MTD-DOME/KarryB | PC-904 | VDIPOOL05 | auto default plan (UPD... | 3.0.0 | Windows 7 | |
| 28 May 19 1:33 PM | MTD-DOME/JoeBidan | PC-1094 | VDIPOOL01 | auto default plan (UPD... | 2.7.2 | Windows 7 | |
| 28 May 19 1:33 PM | MTD-DOME/DavidB | PC-841 | Computers | auto default plan (UPD... | 3.0.0 | Windows 7 | |
| 28 May 19 1:33 PM | MTD-DOME/SamBa | PC-867 | Computers | auto default plan (UPD... | 3.0.0 | Windows 7 | |
| 28 May 19 1:33 PM | MTD-DOME/SamBa | PC-374 | VDIPOOL06 | auto default plan (UPD... | 3.0.2 | Windows 10 | |

Source: Enterprise Strategy Group

Finally, we reviewed the protection plans configured for the environment. Morphisec supports multiple protection plans that can be applied to groups of endpoints, enabling differing levels of protection based on need. By default, Morphisec protects a curated set of applications that are exposed and often threatened by malicious actors, as shown in Figure 4 and Table 1.

Figure 4. Protection Plans

AUTO DEFAULT PLAN

General Settings

Plan Name: auto default plan

Plan Policy

Protect Specific Applications: +Add

Exclude the following applications: +Add

Pop Up Notification Message

Show notification to users when an attack is prevented

Notification Message: The file/url you tried to open contains malicious code. It was blocked and your data is safe.

Advanced

Server IP or Domain: [Text Field]

Server Port: [Text Field]

Protector Zone: [Toggle: OFF]

☒ Protect System Processes

☐ Mini-Dump

☒ Enable 64 Bit Processes

☒ Enable Running Processes

☐ VBScript Blocking

Cancel Save

Source: Enterprise Strategy Group

Table 1. Morphisec Curated List of Applications to be Protected

| | | | |
|-----------|------------|------------|----------------|
| MS Access | PowerPoint | FireFox | Teamviewer |
| Chrome | Skype | IEExplore | Windows Script |
| Excel | Cscript | EQNEDT32 | Rundll32 |
| Outlook | Word | RegSvr32 | Task Scheduler |
| Vic | Autolt | PowerShell | Acrobat Reader |
| Mshta | RegAsm | | |

Source: Enterprise Strategy Group

The list of protected applications is not exclusive—any children or related processes are also protected. Cybersecurity analysts can also configure Morphisec to protect all processes.

Organizations running older applications, such as legacy in-house developed applications, may consider those applications brittle—susceptible to breaking when even minor changes are made—and may wish to avoid having Morphisec manipulate the application’s memory. Thus, Morphisec protection can be configured via include and exclude lists of files and folders.



Why This Matters

The critical lack of cybersecurity skills presents a challenge to organizations: How do they simply and efficiently protect their data and IT resources? A solution focused on easing the management burden is needed to ensure that cybersecurity analysts spend less time on the care and feeding of tools and more time protecting the organization.

ESG validated that Morphisec removes a significant amount of management burden. The lightweight, small-footprint Morphisec agent demonstrated exceptional efficiency, installing quickly and running only at application instance launch, which means no application performance penalty. The dashboard provided at-a-glance state and attack information, and we were quickly able to understand our endpoint cybersecurity posture and the volume and type of threats we faced. Configuring the solution was likewise rapid and simple, and we were easily able to protect the entire fleet of endpoint devices.

Attack Prevention Efficacy

ESG observed Morphisec’s advanced prevention capabilities across detonated attacks and exploits of various threat categories. Our test environment used a C2 server dynamically generating attacks targeted at an up-to-date Windows 10 Enterprise workstation running Microsoft Defender AV and a popular commercial EDR solution.

ESG Testing

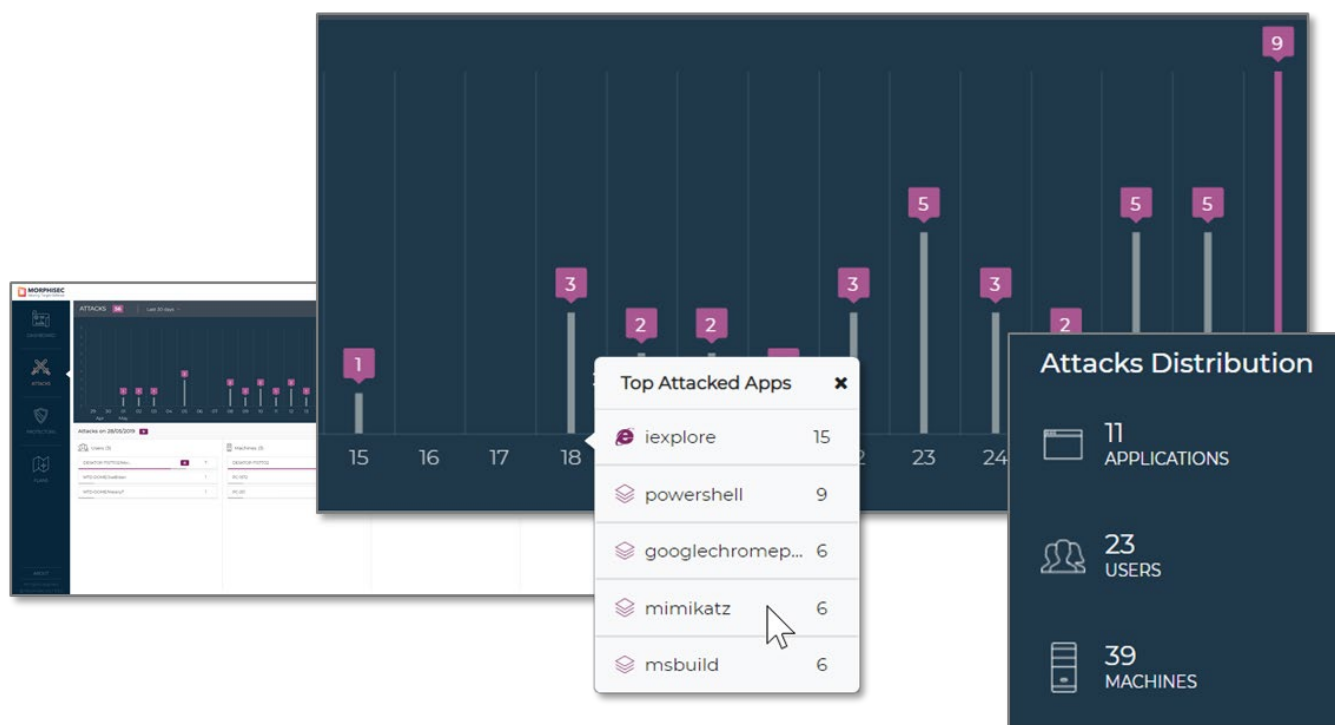
The advanced attack started with a phishing email directing the target user to a website. The site automatically downloaded a VBS script, which passed Defender AV scanning. The script used a variety of TTPs, including dot-net process hollowing to give the attacker a shell running on the target system. Leveraging additional TTPs, the attacker erased all traces of its presence from the system while gaining local administrator privilege, and then moved laterally to attack the domain controller, gaining domain administrator privilege.

After installing Morphisec on the target, we retried the same attack. This time, Morphisec immediately prevented the process hollowing attempt and displayed a Win10 notification. The attack failed benignly, preventing infection or damage to the system, with no interruptions in operations or impact on performance.

We observed that Morphisec’s moving target defense prevented advanced attacks from crucial attack vectors, including email, web, fileless/in-memory, malware, scripts, and kernel. These attacks employed a variety of TTPs, including exploitation, macro, OLE code injection, reflective loading, exploit kits, drive-by campaigns, code injection, process hollowing, self-modifying code, and user-mode code injection from the kernel.

Next, we reviewed the alerts generated by these and other attacks in the Morphisec console by selecting **Attacks** from the left-side menu, as shown in Figure 5.

Figure 5. Morphisec Attack Alerts



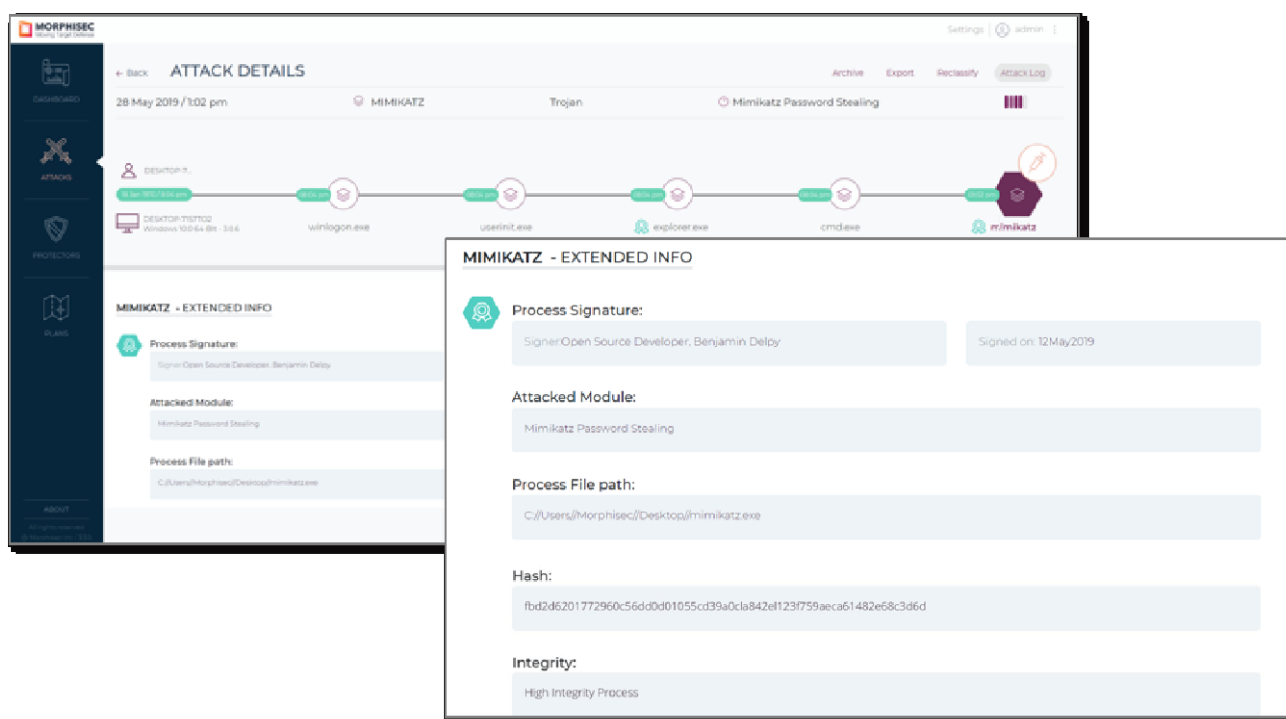
Source: Enterprise Strategy Group

As with the dashboard, the Attack panel displays a timeline bar graph of attacks along with attack distribution statistics. In our environment, we experienced attacks across 39 endpoints, 23 users, and 11 applications. Separate panels listed the top users, endpoints, operating systems, and applications under attack. This enabled us to focus our investigatory efforts appropriately.

From the list of applications, we clicked on *Mimikatz* to get information on the attacked application (in this case, a demo attack using the Mimikatz tools). The Attack Details screen, shown in Figure 6, can be reached by clicking through any of the information panels on the attack dashboard.

The screen displays attack details including name, type, description, and severity of the attack, along with the full attack trajectory, from point of origin through every stage of the attack. Selecting a stage reveals additional critical data points about that attacked process including file path, hash, integrity level, and command line instructions. Analysts can use the information, such as the command line, to understand how the attack entered and penetrated the endpoint defenses.

Figure 6. Attack Details



Source: Enterprise Strategy Group

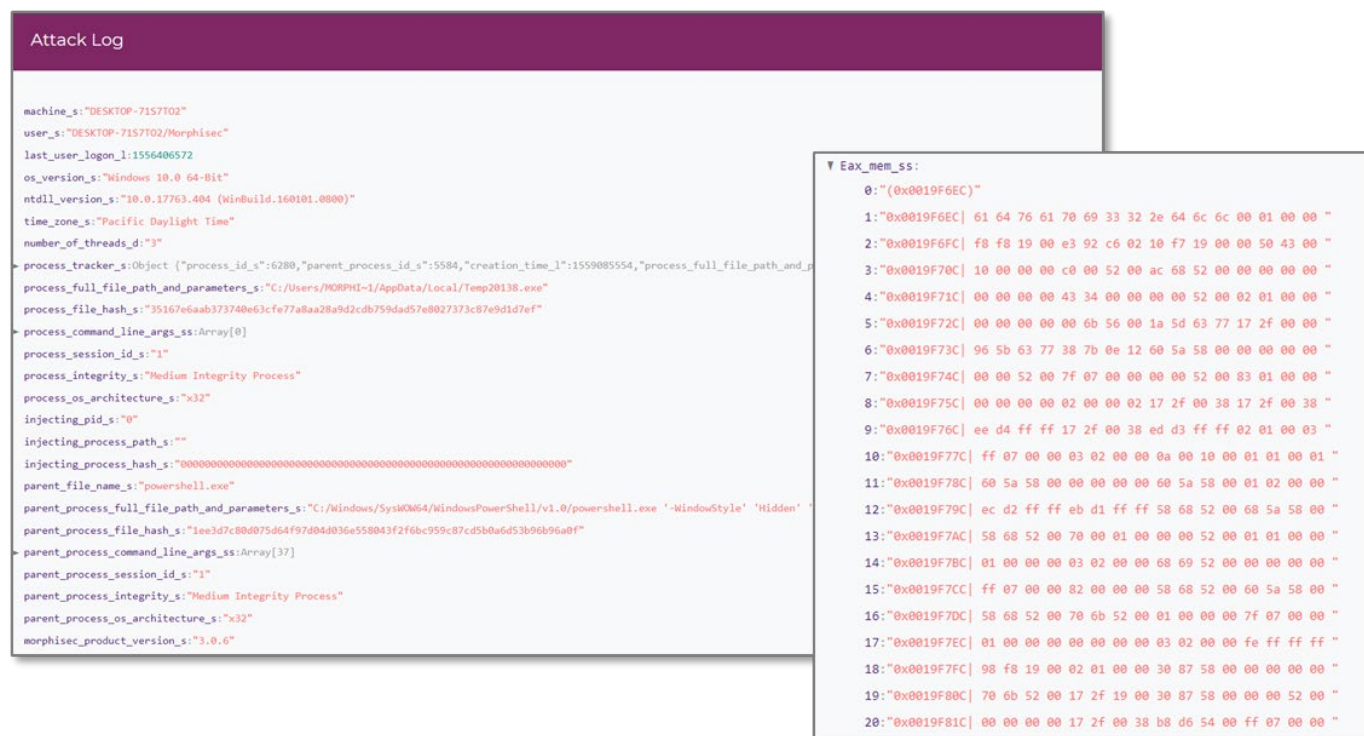
Clicking on the *Show Log* button brought up detailed log information including the process tree, command line, memory and processor register values, and other crucial forensic data, as shown in Figure 7. Critically, because Morphisec traps malicious code at the point of execution, Morphisec captures de-obfuscated malicious code. I.e., the malicious code has been decrypted and decloaked and is ready to be executed by the processor. Investigating this de-obfuscated code enables the analyst to understand exactly what actions the malicious code was about to take.

The process tree information shows the entire tree from initial launch to malicious code execution. For example, we were able to quickly trace malicious code from Power Shell backward to Microsoft Word and then to Microsoft Outlook. This indicated that a user received a malicious email containing a Word doc attachment. The user clicked on the attachment, executing Word, which in turn executed a macro that launched a Power Shell command.

Using this information, the analyst can develop remediation methods for unprotected and infected endpoints, as well as update network, web, email, and other security controls to prevent the malicious code from entering the environment.

Additionally, this information can be used by Morphisec to cross-correlate trends and campaigns across the 3 million endpoints under protection.

Figure 7. Detailed Attack Log



Source: Enterprise Strategy Group

Why This Matters

Malicious actors are becoming more sophisticated and are crafting more devious and evasive attacks. Recent attacks have been specifically designed to evade new artificial intelligence-based methods of detection. Organizations need effective endpoint security controls that can prevent attacks with extremely high rates of success and low probabilities of false positives to avoid alert fatigue.

ESG observed that Morphisec's threat prevention effectiveness reduced or eliminated the need to monitor web and network traffic for threats. Process monitoring could also be eliminated since Morphisec protected processes from buffer, integer, and stack-heap overflow and overrun; type confusion; use-after-free attacks; and other exploitation methods.

While static and runtime detection require known data to classify similar attacks, Morphisec quickly prevented unknown attacks when the attacks tripped over Morphisec traps placed in the original memory structure during the morphing process—attack detection was not necessary for prevention of the attack.

We could see from Morphisec's attack analytics that the system captured extremely detailed forensic intelligence including the full execution stack and memory access, enabling security analysts to forensically investigate how malicious code penetrated their environment. Using this knowledge can help tighten security and prevent future compromise.

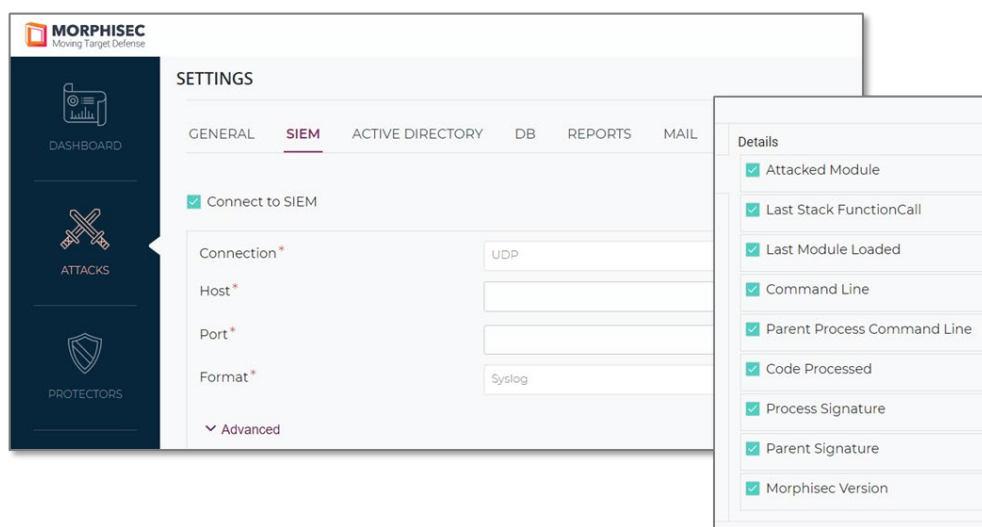
Integrations

Morphisec's Threat Prevention Platform includes the ability to integrate with Active Directory and other cybersecurity tools including SIEMs, Microsoft Defender ATP Security Center, and Microsoft Defender Antivirus.

ESG Testing

From the Morphisec console, ESG clicked on **Settings** on the left-side menu to bring up the configuration section. From the top tabs, we selected **SIEM** to select the SIEM integration configuration settings. As shown in Figure 8, we had the ability to send critical forensic information from Morphisec to the SIEM, including the attacked module, last function call, command line, parent process command line, and signatures. Sending this information to the SIEM enables cross-correlation between Morphisec's threat detection and prevention and other security controls, helping security analysts to quickly understand what malicious code is present, how that code entered the environment, and where future infections could be prevented.

Figure 8. SIEM Integration

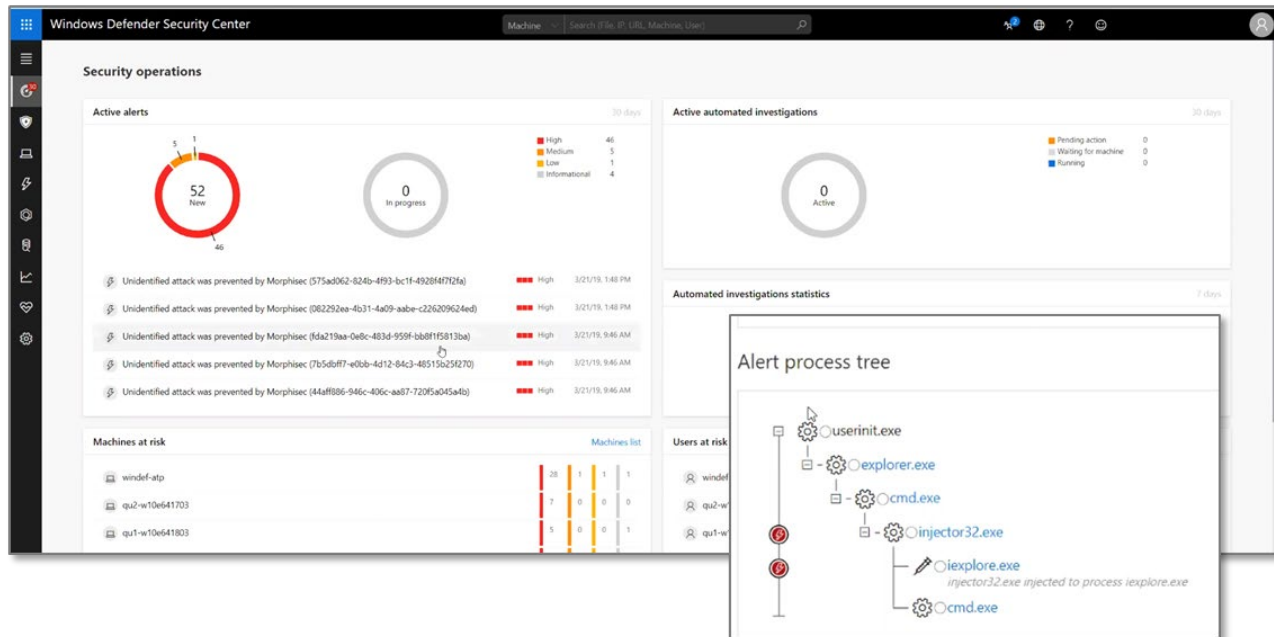


Source: Enterprise Strategy Group

Next, we logged on to Microsoft Defender Security Center to review information Morphisec had previously sent as part of the Defender ATP integration. As shown in Figure 9, Morphisec alerts appear alongside native Microsoft Defender ATP alerts.

Because of Morphisec's high fidelity and extremely low probability of false positives, Microsoft Defender Security Center ranks Morphisec alerts as high priority, marking them in red. Clicking on a Morphisec alert brought up additional information including the full process tree, enabling security analysts using the Security Center console to triage and process these alerts quickly and easily.

Figure 9. Morphisec Integration with Microsoft Defender Security Center

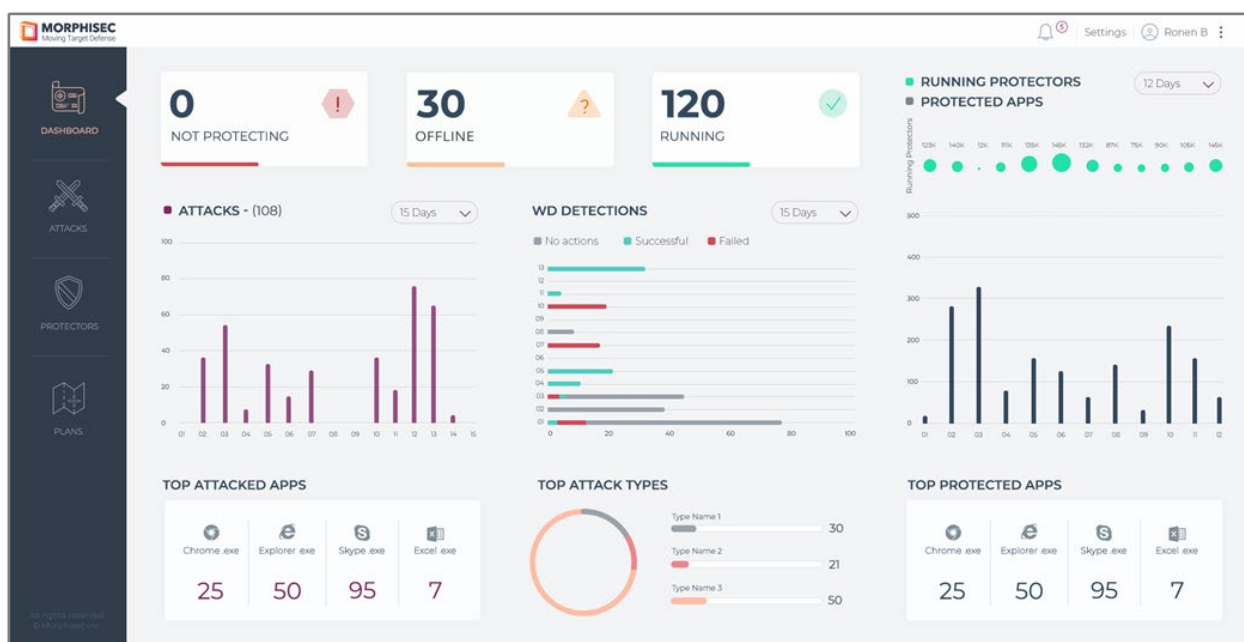


Source: Enterprise Strategy Group

Microsoft Defender AV Integration

Morphisec also integrates with Microsoft Defender AV and consolidates Defender AV threats into the Morphisec Unified Security Center dashboard, displaying Defender AV alerts alongside Morphisec threat data as shown in Figure 10. Using Morphisec, we were able to drill down into Defender AV alerts to get more detailed information, a feature missing from Defender. The integration of Defender AV and Morphisec provides security teams with unified visibility into both known and unknown threats attacking their organization.

Figure 10. Morphisec Integration with Microsoft Defender AV



Source: Enterprise Strategy Group



Why This Matters

Endpoint threat prevention is only one tool in an organization's cybersecurity toolbox, and organizations need to ensure all tools work in concert to both prevent compromise and preserve a record of activities to aid in investigations.

ESG validated that it was quick and easy to integrate Morphisec with commercial SIEM solutions, and that Morphisec provided the requisite forensic data. We also observed that Morphisec integrates with Microsoft Defender ATP. Because Morphisec has high fidelity and a low probability of false positives, Defender ATP gives Morphisec alerts more credence, ranking any alert from Morphisec high priority. Security analysts were able to start their investigation and incident response directly from the Defender console.

We also validated that Integrating Morphisec and Defender AV provides additional data into Defender AV alerts. This can help Windows 10 organizations transition from legacy antivirus solutions to the combination of Morphisec and Defender and thereby gain advanced attack prevention along with end-to-end threat visibility.

The Bigger Truth

The traditional approach to strengthening cybersecurity is to layer on more tools to address perceived or existing weaknesses. This approach fails as it forces organizations to expend more scarce resources—time, money, effort, and, most importantly, staff—and creates an ever-more complicated environment. Instead, organizations need to focus on tools that are effective at preventing threats and have efficient implementations.

ESG's testing showed Morphisec to be both efficient and effective when tested against a range of advanced threats in multi-stage targeted attack campaigns. Tested threat vectors included ransomware, trojans, RATS, malware, downloaders, and others targeted at endpoints, web, and email. Threats were blocked pre-execution, preventing memory infiltration and lateral movement. ESG observed that in all cases, the termination of malicious processes occurred in real time, giving operators an immediate preventative capability against unknown, fileless, and zero-day threats.

The lightweight, small-footprint Morphisec agent demonstrated exceptional efficiency, installing quickly and running only at application instance launch, which means no application performance penalty. Prevented threats were logged with a trove of forensic data. Morphisec's moving target defense deployed decoy code, ensuring that all detections and preventions were valid. This feature avoids false positive alerts and alert fatigue.

Morphisec's management interface proved to be quick, simple, and intuitive. We were able to quickly configure and deploy Morphisec, and the platform logged a great amount of forensic data. This enabled us to investigate incidents, performing root cause analysis of how malicious code entered the environment, and placing controls to prevent future compromise.

Morphisec's moving target defense—randomizing, morphing, and moving memory resources to prevent advanced attacks—obviates the need for separate detection and prevention solutions. Morphisec works in conjunction with any commercial antivirus solution—antivirus tools prevent known, non-evasive malware and Morphisec provides advanced threat prevention. Morphisec can help organizations to maximize the value of their Windows 10 migration, leveraging Microsoft's built-in security tools, including Defender AV, to build an efficient and effective threat prevention stack. No matter your security stack configuration, if you're searching for an efficient and effective advanced threat prevention solution, ESG suggests you consider Morphisec.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.



www.esg-global.com



contact@esg-global.com



P. 508.482.0188