Yet another year, yet another string of security concerns. It seems like each time information security is mentioned in the news, it’s typically related to either a significant data breach or a critical vulnerability that puts thousands, if not millions, of users at risk. In the year 2020 alone, we’ve had critical vulnerabilities impacting both endpoints and networks, quickly followed by attacker exploitation. This creates a scenario in which defenders are forever reacting to incidents, never able to gain a proactive stance.

As defenders continue playing catch-up with detections, they also must keep the organization secure from its own devices, due to users who inadvertently introduce malware or suspicious activity into the environment. If modern defenders find themselves overloaded with all of this, they’re not alone. It’s time defenders—perhaps even at your organization—consider implementing tools that are designed to increase the efficiency of the team and provide the relevant data needed to respond to incidents while simultaneously blocking known bad threats.

We recently spent some time with a platform designed to do exactly that: Morphisec. In this review, we walk through our experience using these products and discuss how they stack up as efficient enterprise security tools. In particular, this whitepaper examines how:

- Morphisec’s unique approach to blocking endpoint threats means prevention is no longer a forgotten topic
- Morphisec provides intuitive endpoint security, meaning analysts can get right to work defending the organization with the data that matters
- Morphisec’s lightweight agent works right out of the box, with defaults that defend against attackers that organizations are experiencing today

After hearing for years that prevention simply doesn’t work, many organizations find themselves unable to afford a dedicated security team, while also not having the resources to outsource to a managed service. This has created a significant gap in the ability to afford capable endpoint solutions. It’s time to reconsider how prevention can be a successful defensive strategy.
Overall, we found Morphisec to be a comprehensive, easy-to-use platform that required minimal intervention from us but provided extensive protection in the form of an extremely lightweight agent. Morphisec reinvigorates the discussion recommending prevention over detection, because it was able to prevent techniques used by today’s threat actors. Morphisec also turned out to be one of our favorite integrations with Microsoft Defender Antivirus and Microsoft Defender ATP, which we explore in subsequent sections.

In many situations, security professionals are encouraged to think about techniques to detect activity. In this product review, we want you to take a different approach: prevention. As you work your way through this review, we encourage you to consider the current state of endpoint monitoring and prevention within your environment. Additionally, consider the complexities behind endpoint monitoring and how often your team finds itself hindered, rather than empowered, to respond to endpoint threats.

Before jumping into Morphisec’s platform, let’s revisit a common myth in endpoint defense and enterprise security that has all but removed the concept of prevention from many analysts’ minds.

**Prevention Doesn’t Work. Right?**

Reviewing Morphisec gave us a moment to pause and reflect on the current state of endpoint security technologies—so much so that after our product review, we found ourselves reconsidering our stance on malware prevention.

For years, organizations were told “It’s not if, but when” or “Prevention doesn’t work,” leading them to believe exactly that: Prevention was a failed attempt at security. This belief led to prolific development of heavy, bloated endpoint agents that consume far too many system resources to achieve their purpose. Furthermore, the deployment, operation and sustainment of these endpoint tools proved to be quite costly for smaller organizations that simply cannot afford managed services. This creates a unique juxtaposition with threat actors—especially financially motivated threat actors—many of whom could not care less about an organization’s size, information security budget or available resources.

For example, consider that in the first half of 2020 there was a surge in ransomware attacks targeting the healthcare industry and local/state governments. Strapped for resources, insecure due to default implementations and overworked because of the COVID-19 pandemic, these organizations were simply unprepared for a cyber incident. Attackers seized on this mayhem, deploying ransomware and holding organizations hostage for sums that were already allocated, and desperately needed, elsewhere.

Security professionals were quick to chastise these victims as ill-prepared, without considering the true cost of a multilayered, detection-first, managed security service. Some organizations simply cannot afford to wait to detect an attack; they need a solution that can prevent one. They need a solution that is lightweight and intuitive to use. Finally, the more integrated or native a solution is, the less impact the organization is likely to experience.
Working with Morphisec gave us a glimpse into a technology that, with the correct implementation and integration, can be an extremely valuable resource with little system overhead. Rather than bulk up with indicators and detections, and then offload analysis to endpoint, Protector (Morphisec’s endpoint software) focuses on running process memory. Protector morphs running programs, such that in-memory code does not resemble the original application. With the knowledge that most malware and attackers will eventually try to access code in memory, Protector deprives malware of memory access. If a process attempts to leverage memory, Morphisec simply blocks that process and thus introduces an effective prevention technique.

If your organization is one that has sworn off of prevention, instead sinking all resources into post-breach detection capabilities, we encourage you to use this examination of Morphisec as an example of success in preventative capabilities.

**Getting Hands-On**

We started by asking how easy Morphisec was to use and whether—in addition to interesting technical concepts—it empowers organizations and analysts. The title of this review, “Intuitive Endpoint Security,” comes directly from the fact that Morphisec is incredibly easy to use, immediately making it applicable for security teams and analysts of all skill levels.

**Initial Access**

The initial setup and deployment of Morphisec is a simple install on a system—virtual or physical—along with a few prerequisites. Once installed, Morphisec’s Protector endpoint agent is also a lightweight install that, with Administrator privileges, links back to the Morphisec server. One nice advantage to this setup is that it allows organizations to scale deployment to their specific needs, on a per-endpoint basis. Furthermore, as organizations fluctuate between in-office and at-home working environments, a flexible agent/server setup means little friction in maintaining endpoint protection. No reboot is required, and securing the system begins immediately.

Once installed, security analysts need simply log in to access relevant threat details. The initial dashboard, shown in Figure 1, provides an excellent, succinct view into the current state of attacks within the organization.

---

**Morphisec was a simple installation with very few prerequisites. We were surprised at how easy the platform was to set up, allowing for applicability to a wide range of organizations, as well as flexibility between virtual and physical hosts.**

---

*Figure 1. Initial Dashboard, Showing Detection Statistics*
As shown in Figure 1 on the previous page, Morphisec brings key details to the forefront for analysts:

- The number of systems unprotected, offline and under active protection.
- Active attacks within the organization, organizable by time frame and operating system.
- The top attacked applications within the organization, as detected by Morphisec and Windows Defender, respectively. **Note: Although we will examine Windows Defender integration shortly, we did not have any active alerts for the screenshot shown in Figure 1.**

The dashboard is straightforward and to the point—in our opinion, providing what we care about right up front. Analysts logging into the platform typically are concerned with the state of infections and incidents within the environment, and Morphisec surfaces this information immediately. In addition, the main Morphisec dashboard includes coverage statistics from an application perspective. Figure 2 provides a screenshot of the other element from the main dashboard, highlighting protection coverage (again, with date filter capabilities).

The simplicity of the Morphisec dashboard highlights the data that analysts need to assess the state of the environment—no more, no less.

**Drilling Down**

It’s worth noting that nearly every element within the main dashboard is clickable for more context. Analysts can click on protector counts to view the endpoints for each category. For example, Figure 3 displays metadata about one agent that is checked into the server, a Windows 10 Desktop.
In addition to basic system metadata, you may also notice that Morphisec displays the Org Unit of a system. If you recognize that as an Active Directory term, you’ve uncovered one of Morphisec’s greatest assets: integration with Windows Active Directory (AD). AD integration has a slew of inherent benefits, the primary being granular control of endpoint plans, which we’ll examine next. The Active Directory integration procedure, shown in Figure 4, is as simple as providing relevant credentials and validating.

It’s just that simple—we felt that Morphisec has spent a lot of time behind the scenes making this platform, and thus consumption of preventative security, easy to use. Once Active Directory has been integrated, we found additional options that enabled us to structure our Morphisec protections. We examine those next.

**Customizing Security**

Many vendors of endpoint products understand that organizations often run proprietary applications and executables, some of which may mimic malicious behavior. (Consider, for example, two security products running side by side.) To allow for customized security, Morphisec has a feature called Plans, also accessible from the main dashboard. As shown in Figure 5, Plans allow an organization to specify which applications to protect and which to exclude.
The Auto Default Plan, which is quite detailed out of the box, is the recommended baseline for any organization. Note that multiple common enterprise applications are protected, including web browsers, communication tools and commonly abused, native Windows applications, such as rundll32, PowerShell, and regsvr32. Excluding an application is as simple as adding it to a list.

One of the nice features of AD integration is that plans can be applied to particular organizational units (OUs) within the domain. As shown in Figure 6, when creating a custom plan, users can specify which OUs the plan should apply to.

![Figure 6. Plan Creation, Allowing for Specific OU Application](image)

Although relatively simple, we found that aligning prevention plans with Active Directory OUs was a very smart decision. Many endpoint protection products will force security analysts to create their own platform-specific host groups, potentially complicating matters when analysts try to understand attacker activity. Morphisec, on the other hand, allows for systems to be grouped in the “natural” way, via Active Directory, and then security to quickly follow up.

Another feature worth mentioning—and one that is extremely critical in today’s modern enterprise environments—is that Morphisec also integrates natively with Microsoft’s Defender Advanced Threat Protection (ATP). Many organizations already take advantage of ATP; however, they may be looking for additional levels of protection, insight and/or preventative coverage. With this native integration, Morphisec can provide a one–two defensive punch for large enterprises currently using ATP without requiring them to replace their security solution.

In an effort to test Morphisec as a standalone tool, and for the purposes of this review, we did not test the Microsoft ATP integration. However, the process is as simple as setting up an API key in Microsoft Azure and providing that to the Morphisec server platform.
Morphisec in Action

Our true test of Morphisec’s capabilities came when we simulated various attacks and put the platform through its paces. Our goal was to test whether Protector could prevent infection by various malware families and to examine the data provided for analysts on the Morphisec server. Our test process was simple: Obtain malware and attempt to run it on one of our test hosts.

The test we’ll walk through was a COVID-19 phishing document that ultimately led to IcedID, a banking trojan, being dropped on the system. As you walk through this test, we encourage you to consider if you’ve had a similar breach or malware infection in your environment. Ask yourself the following:

- Did we prevent or detect the infection?
- If the latter, how quickly did we detect?
- How much damage was done by the time we detected?

Once the malware was on the system, we orchestrated various execution techniques: scheduled tasks, service installation and direct call via Windows utilities. Note that we had no problem placing malware on the system; one feature of Protector is its focus on execution and access to application memory. This prevents Morphisec from bloating its agent with on-disk scanners.

Despite our various attempts to execute pieces of the malware, Morphisec prevented any action from taking place as soon as execution was attempted. Similar to Windows Defender, a small alert informs the user that malicious activity was detected and execution has been blocked. To the user, this is similar to any antivirus or malware alert.

For the security analyst, Morphisec tells a very different story. Navigating to the Attacks section of the dashboard, as shown in Figure 7, allows the user to view activity over a selected time period.

![Figure 7. The Attacks Dashboard, Providing High-Level Details of Observed Malware](image)

When reviewing security tools, platform and implementations, be sure to frequently assess your current tool set. Your security team should be involved in the testing process, from beginning to end. Consider whether what you are reviewing will complement or improve your security posture, and whether it will empower your analysts.

---

1 Thanks to Malware Traffic Analysis for providing a copy of this malware, which can be obtained from [http://malware-traffic-analysis.net/2020/05/27/index.html](http://malware-traffic-analysis.net/2020/05/27/index.html)
Because we were testing only one system, our data represents only one system with five malicious applications. (We attempted to execute one piece of malware twice, which is why Morphisec displays six attacks.) Similar to the main dashboard, most of this dashboard is dynamic and allows for easy visual filtering. Selecting a user or machine, for example, will highlight all entries associated with the selection, as shown in Figure 8. Although it may seem subtle, this is a fantastic way of helping narrow scope when dozens or hundreds of systems are reporting alerts, as in large enterprises. For this test, only one system was involved, and thus filtering is straightforward.

Drilling down into attacks removes the visualizations and instead provides a simple, intuitive way to sort through data. Figure 9, for example, shows a similar dataset of the attacks Morphisec observed. It provides multiple ways to sort through data, including operating system, severity and category (in addition to the previously identified filter options).

It’s worth noting that we enjoyed Morphisec’s visual layouts. While a small number of security analysts pretend they want to view all data in raw hex, most security analysts spend a lot of time sifting through dashboards and organizing alert data. Our compliments to Morphisec for making data consumable, extremely easy to process and intuitive to walk through.

Moving into more technical details, users can examine each and every application blocked by Morphisec within the Attacks dashboard. Starting with Figure 10, we’ll drill down into execution of the file joujkd2.exe.

Keeping with the theme of being intuitive and easy to consume, Morphisec provides a detailed process execution chain. Both processes represented in this alert include granular details such as process signature, file path and, most important, the module that the malware attempted to attack. As shown in Figure 10, this particular file attempted to access kerne132.dll, a key dynamic link library (DLL) in Windows that handles memory management and I/O operations.
Quickly pivoting from simple and intuitive to advanced analysis, note that in the top-right of Figure 10 is an option to view the Attack Log. Selecting Attack Log provides details of malware execution that even the most seasoned reverse engineers would love to see. As shown in Figures 11 and 12, Morphisec captured extremely granular execution details.

Figure 11 provides the first of two screenshots of the Attack Log, as observed by Protector/Morphisec. It’s easy to tell that these screens provide much more technical detail than previous ones, but this data is crucial to understanding what a piece of malware was attempting to do.

Note that the Attack Log provides execution details such as process command line arguments, path, parent relationships and system metadata.

Figure 12 gets down into the technical, in-memory attack details as observed by Protector on the endpoint. The tool provides values for various memory registers along with the specific bytes as observed during malware execution. It’s worth noting that Morphisec expects that this data may be passed off to more senior analysts, and thus provides an easy export of data, including a data anonymizer.

These data points highlight another of our favorite features of Morphisec. From the onset, the dashboard is ridiculously intuitive
and allows users to view attacks across an enterprise on a single screen. However, drilling down into attacks, the information provided quickly scales from simple alert review to detailed malware analysis, including byte strings and memory offsets. The beauty of the data captured by Morphisec is that analysts of all skill levels can utilize the platform to analyze threats to the environment. Seasoned analysts and/or reverse engineers, for example, will likely want to view these granular details first so they can understand the malware intention.

Along with an intuitive interface, the other “feature” we enjoyed regarding Morphisec is its overall simplicity. As mentioned earlier, security analysts are often bogged down by too much or irrelevant data; we didn’t find any of that using this platform. We were able to quickly assess threats to the organization, and knowing they were already prevented meant we didn’t have to jump into a reactive state.

**Closing Thoughts**

Endpoint security can be a tricky topic for many organizations. In many cases, security teams utilize endpoint security products that are bulky and cumbersome, barely effective and only make their jobs more difficult. Furthermore, many security products rely so heavily on detecting an incident *after the fact* that they hardly seem effective in preventing cyber incidents. This leaves the security team constantly chasing alerts through the network, rather than implementing preventative techniques.

In this paper, we spent some time reviewing a platform that is seeking to reverse much of this approach. Morphisec is geared toward the *prevention* of malicious activity through the careful morphing of process memory, which in turn prevents threat actors from accessing sensitive application code. Realizing that the majority of malware—regardless of victim organization size or budget—performs predictable actions allowed Morphisec to craft a prevention mechanism that integrates beautifully with various operating systems.

Morphisec also impressed us with its notable integration with Microsoft’s Windows Defender, Defender ATP, and Active Directory. Through seamless integration with corporate domain environments, Morphisec becomes a multipurpose tool that allows for security applications and monitoring based on the domain, instead of a cumbersome, tool-specific endpoint categorization.

Finally, we also put Morphisec up against malware often seen in common attacks to test its ability to protect a test domain. Despite a lightweight, barely noticeable agent, Morphisec was able to prevent infections with ease, even for previously unknown signatures. Overall, we discovered an easy-to-use, highly scalable tool that integrates well with cloud and on-premises environments. Morphisec proved that security can be effective while being intuitive, ultimately disputing the theory that prevention never works.
About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is also an IR consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper’s sponsor:

MORPHISEC
## Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia, VAUS</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich September 2020</td>
<td>Munich, DE</td>
<td>Sep 14, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Australia Spring 2020</td>
<td>AU</td>
<td>Sep 21, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio Fall 2020</td>
<td>San Antonio, TX</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam October 2020</td>
<td>Amsterdam, NL</td>
<td>Oct 05, 2020 - Oct 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR500 Milan 2020 (In Italian)</td>
<td>Milan, IT</td>
<td>Oct 05, 2020 - Oct 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020</td>
<td>Dallas, TXUS</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Tel Aviv November 2020</td>
<td>Tel Aviv, IL</td>
<td>Nov 01, 2020 - Nov 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain Fall 2020</td>
<td>Denver, COUS</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Sydney 2020</td>
<td>Sydney, AU</td>
<td>Nov 02, 2020 - Nov 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Krakow November 2020</td>
<td>Krakow, PL</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Gulf Region 2020</td>
<td>Dubai, AE</td>
<td>Nov 07, 2020 - Nov 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>APAC ICS Summit &amp; Training 2020</td>
<td>Singapore, SG</td>
<td>Nov 13, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020</td>
<td>San Diego, CAUS</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich November 2020</td>
<td>Munich, DE</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam November 2020</td>
<td>Amsterdam, NL</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>