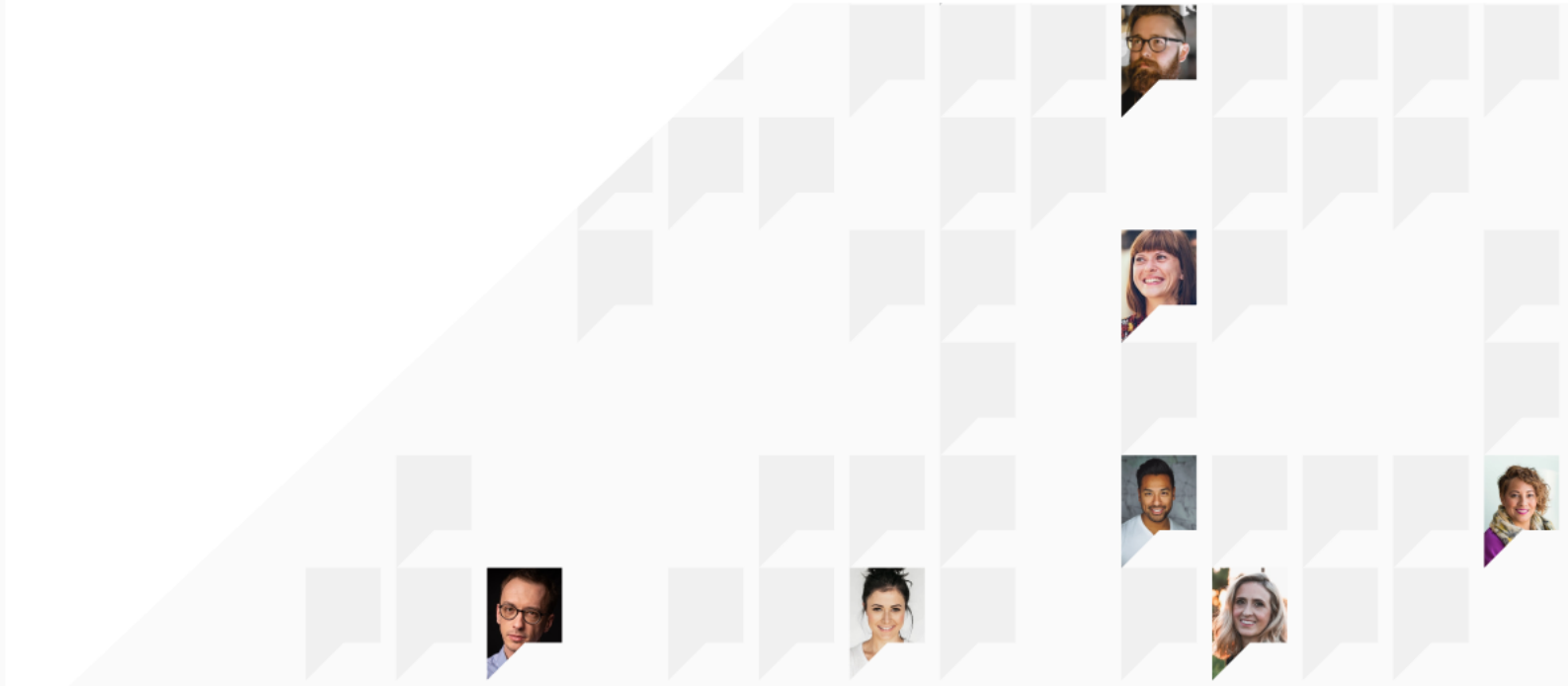
PeerSpot

MORPHISEC

Morphisec for Healthcare Companies

September 2024



Contents

Product Recap

Morphisec Recap

Morphisec's cybersecurity platform is centered around its Moving Target Defense technology. This innovative approach is designed to prevent attacks by making the system environment dynamically unpredictable to attackers, thereby neutralizing zero-day threats, evasive malware, and in-memory exploits without requiring prior knowledge of attack patterns. Unlike traditional security systems that rely on detection and response strategies, Morphisec operates on the principle of attack prevention, reducing the system's attack surface and minimizing security operation efforts.

Morphisec provides cybersecurity defense solutions that protect against advanced threats through proactive and predictive security measures. Key features include Moving Target Defense, which Constantly changes system memory and application structures, making them hard to target. Also, Morphisec enables threat-hunting and visibility by providing detailed forensic data on blocked attacks, enabling advanced threat-hunting capabilities.

Morphisec's key capabilities include:

- Anti-ransomware: Advanced ransomware protection leveraging dedicated AMTD mechanisms for safeguarding against ransomware attacks, from early attack stages to the impact/encryption phase.
- Credential theft protection: Advanced credential theft protection leveraging AMTD for safeguarding against Infostealer/credential stealing attacks
- Enhanced cyber-resilience: Implementing AMTD to efficiently mitigate the costs associated with recovery from advanced, previously unknown evasive threats, thereby bolstering overall cyber defense strategy.
- Prevention-first security: Prevents threats without prior knowledge: signatures, behavioral patterns, or indicators of attacks (IoAs).
- Operational efficiency: Providing simple installation with negligible performance impact and no additional staffing requirements.
- Lower IT and security costs: Significantly reducing security analyst alert triage time and costs due to early prevention, exact threat classification and prioritization of high-risk alerts.

- Risk-based vulnerability prioritization for exposure management: Empowering organizations with continuous business context and risk-driven remediation recommendations, enabling effective prioritization of patching processes and reduced exposure with patchless protection, powered by AMTD.
- Flexible deployment: Offering a SaaS-based, multi-tenant and API-driven platform.
- Incident Response Services: The Morphisec Incident Response Team works collaboratively with client organizations to triage critical security incidents and conduct forensic analysis to solve immediate cyberattacks as well as provide recommendations for reducing the organization's risk exposure. Morphisec's team helps to identify and resolve unknown threats to get organizations' networks restored quickly.

Morphisec is particularly effective in industries such as finance, healthcare, and government, where highly sensitive data is often targeted. Its ability to provide robust protection without the need for extensive updates makes it suitable for environments where system stability and uptime are critical.

In summary, Morphisec offers a proactive cybersecurity solution designed to outsmart modern cyber threats through a strategic, preventative approach, making it an excellent choice for organizations aiming to bolster their defenses against sophisticated attacks.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "I really like the integration with Microsoft Defender. In addition to having third-party endpoint protection, we're also enabling Defender... I like the reporting that we get from Defender, when it comes in. I like that it's one console showing both Morphisec and Defender where it provides me with full visibility into security events from Defender and Morphisec."

Tom Merkle

Chief Information Officer at Houston Eye Associates

- "Morphisec also provides full visibility into security events for Microsoft Defender and Morphisec in one dashboard... in the single pane of glass provided by Morphisec, it's all right there at your fingertips: easy to access and easy to understand. And if you choose to go down further to know everything from the process to the hash behind it, you can."

Billy Sainz

IT Operation Manager at Citizens Medical Center

"The fact that Morphisec uses deterministic attack prevention that does not require human intervention has affected our security team's operations by making things much simpler. We don't have to really track down various alerts anymore, they've just stopped. At that point, we can go in and we can clean up whatever needs to be cleaned up. There are some things that Morphisec detects that we can't really remove, it's parts of Internet Explorer, but it's being blocked anyway. So we're happy with that."

Verified user

Sr. Security Lead at a healthcare company with 10,001+ employees

What users had to say about valuable features:

“The killing of the processes and the alerting are the most valuable features. Where we used to have to wait for either an email to come in and say, "Hey, this has happened," or for a user to call and say, "Hey, this isn't working right," now, the moment it happens, it kicks off an alert to our Microsoft Teams and everybody on my team sees it.

Morphisec also provides full visibility into security events for Microsoft Defender and Morphisec in one dashboard. We purchased that functionality about a year ago. It's important to our organization because we are able to go to one spot to see and follow up on things, and that has been a big help. We're still trying to integrate Windows Defender so that it works with Azure, along with SCCM. If you've worked in SCCM, you know it can be a little bit confusing. When you go into SCCM, you have to do a lot of drill-downs and look for the problem. But in the single pane of glass provided by Morphisec, it's all right there at your fingertips: easy to access and easy to understand. And if you choose to go down further to know everything from the process to the hash behind it, you can.”

Billy Sainz
IT Operation Manager at Citizens Medical Center

Read full review

“I really like the integration with Microsoft Defender. In addition to having third-party endpoint protection, we're also enabling Defender, although we haven't rolled it out fully yet; we have had a test environment. I like the reporting that we get from Defender, when it comes in. I like that it's one console showing both Morphisec and Defender where it provides me with full visibility into security events from Defender and Morphisec. With our help desk situation—where it all comes to me, and I'm responsible to make sure that I am seeing anything that could possibly be a problem—having both of those in one location has been very important for me.

Morphisec stops attacks without needing knowledge of the threat type or investigation of security alerts. It absolutely does do that and that's because of the way it looks at an executable when it starts and when it asks for memory. If it asks for a specific piece of memory, then Morphisec says, "Okay, it's over here," but it's not really, and then it watches what it tries to do with that. It knows whether it did something that it shouldn't and it will kill that process in that scenario. It doesn't require foreknowledge of the application to protect you from threats. I've seen it happen because we have some old software that does some squirrely stuff, and we've had to allow it to run anyway. That old software does stuff that you wouldn't expect from modern software. If modern software were to do what that old software does, it would definitely be a threat. So I've seen it in action, but not with a live vulnerability.”

Tom Merkle
Chief Information Officer at Houston Eye Associates

Read full review

Other Solutions Considered

"The one I remember that we looked at was Carbon Black. The reason we went with Morphisec was that it was well-reviewed at a conference by one of the members of our leadership."

Billy Sainz
IT Operation Manager at Citizens Medical Center

Read full review

"I think there are competing companies now, but I don't think there were when I was first introduced to Morphisec. I was looking for a solution and Morphisec was the one that I found. I didn't find anyone else of consequence advertising they were doing the same kind of process that Morphisec does. And I'm not looking at any competitors right now because I'm happy with Morphisec."

Tom Merkle
Chief Information Officer at Houston Eye Associates

Read full review

“I did not have a previous solution.

During the process of looking into Morphisec, I sent a couple of the details of some of those Zero-day vulnerabilities to the different companies that I was relying on at the time. I said, "Hey, how does your product protect me from this?" and I got them all to basically admit, "Well, we don't." I got back to Morphisec and they were able to explain how their product would protect us from these types of vulnerabilities, because they were memory attacks, and that's what Morphisec does.”

Tom Merkle
Chief Information Officer at Houston Eye Associates

Read full review

“We looked at Bitdefender, Trend Micro, and Microsoft Defender. We are still using Microsoft Defender in conjunction with Morphisec in a small pilot group. We're still evaluating where we want to go for a true antivirus solution. So, we still have a small deployment of Defender.

Deployment was the biggest difference between Morphisec and the other solutions. It was far simpler to deploy Morphisec without having to remove another antivirus, without having to make a large-scale project, or look for compatibility. It works on all supported operating systems. It works in conjunction with other antiviruses. We didn't have to create exceptions and there were no conflicts with the antivirus we were running and Morphisec. So that really helped us make that decision, purchase this, roll it out, and have it supplement our existing technologies. And it gave us an almost immediate return on investment.”

Verified user
Sr. Security Lead at a healthcare company with 10,001+ employees

Read full review

Use Case

“For the most part, it's an install-and-forget until it alerts. When it alerts, if a user has a script or something that runs and that tries to alter a process, a message pops up on the user's device and lets the user know, and then it shuts down the process immediately, preventing further infection.

We recently migrated to their cloud platform, which is hosted on AWS. We had on-prem servers but we're decommissioning them in the next week or so.”

Billy Sainz
IT Operation Manager at Citizens Medical Center

Read full review

“We purchased Morphisec primarily to help mitigate and protect us against Ryuk ransomware back in December when that was running really rampant. The antivirus that we were using at that point was outdated. We were looking to move to a new vendor, and we needed something as a stopgap to supplement our current antivirus. Morphisec fit that bill perfectly. It had features that our antivirus did not. It had an immediate deployment and immediate return on investment that we just would not be able to get if we were to turn around and try to deploy a full-blown antivirus across the entire environment. Morphisec was quick, simple, and did not conflict with anything that we already had. It also did not cause any additional delays in our virtualized environment, which was a huge concern for our infrastructure team. It just fit perfectly.

We've detected things that our antivirus was not picking up. We had no visibility or control over anything that was running in process memory. Morphisec immediately started blocking things that should not have been running in process memory. It also gave us visibility into the Windows Defender antivirus that we did not have without increasing our Microsoft licensing and gave us some basic control over Defender as well. We previously used McAfee.”

Verified user

Sr. Security Lead at a healthcare company with 10,001+ employees

Read full review

“We are in healthcare and when the pandemic started we were really getting hammered with phishing attacks. Thankfully, none of them really got through or were successful, but the uptick in the attacks made me really concerned about the potential for the results of a successful ransomware attack.

The way I've set up our world is as a bunch of different layers, from what I consider to be best-of-breed. We have a gateway with one company, we have endpoint protection with another company, we have firewalls and connectivity to the internet handled by another company. We also have a company that monitors all of our logs. On top of that, the last thing that I saw as a big hole in my defense strategy was all these Zero-day attacks that were getting through some of the other products. They hadn't gotten through to us yet, but I had read that it was more and more of a threat. Morphisec is just another layer on top.

Part of the reason I purchased the product is that we are a very bottom-heavy IT organization, in that we have a really strong help desk group. Anything more complicated than help desk is my problem, and I have a lot of other responsibilities besides IT. I count on being able to bring in vendors that are very useful to me to subsidize that.

They have a new deal where things are controlled by their cloud controller, which is on AWS. I updated to that about two months ago. It used to be on-premises but thankfully it's not anymore.”

Tom Merkle
Chief Information Officer at Houston Eye Associates

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"The initial setup, when it was on-prem, was kind of complex. It took half a day of working with someone from Morphisec to get it set up and then four or five follow-up calls to make sure everything was set up right. When we went to the cloud controller, obviously, I had knowledge of how to run the product by then, and it took about an hour to get set up and we were running. It couldn't have been easier. I was very happy with that.

When we rolled it out, we had about 1,200 PCs and endpoints. I put the product on about 50 of them to make sure that everything was fine. We do application publishing and I put it on the application publishing servers immediately but that was not a great idea. Those are the servers that were running that old software that I mentioned, the software that was getting false positives all the time. We ended up not putting it onto those servers, but after those 50 machines ran for a couple of weeks with no issues, we rolled it out to the rest of the endpoints.

We were fully running within a month."

Tom Merkle

Chief Information Officer at Houston Eye Associates

Read full review

"The initial setup was straightforward and simple. I believe we used a command-line PDQ Deploy and pushed it out across the organization. We were licensed for 1,500 machines in the beginning, 300 servers and 1,200 machines. We didn't go to each individual one. We just pushed it out from one spot to all of them, from a list.

A typical install takes about a minute. It may take three to four minutes if it has to uninstall an old version of Morphisec. Across the organization, it took a day to roll out. We have an inventory of everything we have. Our biggest concern, at the time,

was what would happen on servers. For instance, I recently pushed it out to the servers, but we left it in alert-only mode for this new version. That way, if it did alert on anything, it would not kill any necessary processes for the organization."

Billy Sainz

IT Operation Manager at Citizens Medical Center

Read full review