PeerSpot

Case Study

Morphisec Breach Prevention Platform

Reviewer73463

IT Director at law firm
with 501-1,000 employees

✓ Review by a Real User
✓ Verified by PeerSpot

What is our primary use case?

We are using Morphisec on 100% of our endpoints. The Morphisec protector installation is pretty straightforward, currently using the scripting capabilities of ConnectWise Automate.

How has it helped my organization?

Previously, we had a mix of AV and EDR solutions that required a fair amount of management. Policy management was more complex, and reviewing exception reports was very time-consuming. Even with this extra effort, we still encountered viruses on a somewhat regular basis. At least once or tiwce a month we would have to work on a machine to remediate it. Since we started using Morphisec, that hasn't happened even once.

This alone has definitely reduced our team's workload. I would estimate we save between four and ten hours a month previously spent on remediation.

The attack prevention doesn't require investigation into security alerts, although we do periodically look and see what types of things are taking place. Even so, we don't spend a lot of time doing those investigations because the attack has been prevented and we don't see it occur again.

Another benefit, something that is important to me, is that Morphisec Guard enables us to see at a glance whether users have device control and disk encryption enabled properly. We want to make sure that we're properly secured and following best practices. Prior to that information being made available to us through Morphisec, we didn't really have a great way of confirming whether a machine had an encrypted disk or other security features enabled.

The solution also saves us from paying for a higher-tier license to get visibility into our Defender AV alerts.

What is most valuable?

The primary feature, of course, is the prevention of Zero-day attacks and other related issues.

It also provides full visibility into security events from Microsoft Defender and Morphisec in one dashboard. We've always had that capability with Morphisec. The more recent version appears to do that even a little bit more natively and it's given us visibility that we didn't have otherwise.

What needs improvement?

We are now beginning to use Morphisec Scout, which provides vulnerability information. At this time, it is able to recognize vulnerabilities and reporting them to us, but it's not actually resolving them. There's still a separate manual process to resolve those vulnerabilities, primarily through upgrades, which are done outside of Morphisec. It might be a bit much to ask, but if Morphisec could somehow have that capability, either natively or through interactions with an RMM system, that would be very effective.

For how long have I used the solution?

We have been using the Morphisec Breach Prevention Platform for a little over two years.

What do I think about the stability of the solution?

It's been very stable, both in terms of Morphisec Guard and the administrative console.

What do I think about the scalability of the solution?

We have one primary, default protection plan that applies to all of our machines, and it does the job very well. It's pretty easy to use the administrative console to check on the status of the protectors. For us, it has been very scalable -- we have 1,200 employees, and Morphisec is on every machine.

I can imagine with more complex environments there might be a need for more varied protection plans, and any limitations of the administrative user interface might be exposed. However, that's not something that has impacted us at all.

I know Morphisec is continuing to evolve and to look for additional ways to be of value to its customers, but in our case, the specific items that we are currently using from Morphisec have already provided great value.

How are customer service and support?

We've only had a few instances where it's been necessary to contact their technical support, but when we have engaged them the support has been very good. We've had good responsiveness and the people we've worked with have been very knowledgeable.

How would you rate customer service and support?

Positive

Which solution did I use previously and why did I switch?

We previously used more familiar EDR tools like Carbon Black and Sophos. We still use SentinelOne on a portion of our machines, but we found that Morphisec is so effective that those EDR tools rarely have the opportunity to do the work that they would normally do before Morphisec has already prevented the attack.

Every one of those other solutions required more hands-on management and more direct involvement. With Morphisec, we just make sure it's installed. With the default policies we have in place, things work well without much additional oversight

There were two factors that occurred simultaneously that drove us to make our initial decision about Morphisec. One was that we were in the middle of a transition from Carbon Black to SentinelOne, and I was concerned that we might encounter circumstances during that transition where we were not fully protected. I considered Morphisec to be a good additional layer. We always strive to have layers of security, and in this case, the additional layer did not negatively impact any of the other security processes we had in place. Since that time, it has been a layer that has proved to be very effective at what it does.

The second factor was that we recognized that Morphisec has a different, complementary approach to how secures our endpoints. That approach has been very effective in dealing with unknown vulnerabilities.

How was the initial setup?

The setup was fairly straightforward. We were one of the first to use the hosted cloud instance, so there were some small discrepancies in the documentation that didn't properly recognize our scenario. But I perceive the number of clients using cloud instances has increased dramatically—it may be the norm now for Morphisec customers. The documentation has definitely improved.

Our implementation strategy was to install it on roughly 10 percent of our environment to assess whether there were any unintended consequences, such as performance issues.

Once we validated both the effectiveness and the low impact on performance, we then deployed it across our entire environment.

The deployment didn't take long, and it went very smoothly. The reporting it provides is very good, giving you a sense of the progress. There was nothing of concern.

I would note that there have been two different instances where we've had to manually push out significant version updates. We're now working with a version where the agent, the protector, will update itself. We are interested to see how well this works with the next significant update.

In terms of staff requirements for deployment and maintenance, somebody has to initiate the solution, but it's not a primary role for anybody among our IT employees. We have our basic processes in place to make sure the Morphisec Protector is on every new machine that we deploy. Beyond that, we don't really spend much time looking at any of the incidents that have taken place, or managing the security policies. There is very minimal overhead.

What about the implementation team?

We implemented in-house. The documentation and the onboarding support made the process very easy to manage.

What was our ROI?

It is definitely a tool that has saved us enough time and reduced our risk enough that the cost is well-justified.

That elimination of instances where we had to manually remediate machines that were affected by a virus has saved us time. We also don't feel it's quite as necessary to use more expensive EDR solutions on every single machine, and we're just better protected. We haven't had issues where we've had data loss or exfiltration.

What's my experience with pricing, setup cost, and licensing?

I'm not sure if we were an early adopter or not, but we enjoyed very competitive pricing when we began working with Morphisec a couple of years ago. We've been very happy with the value the service provides.

This is the first year that we've had Morphisec Scout in addition to Morphisec Guard. We are eager to take advantage of the additional capabilities it offers. Of course there is an additional cost associated with Scout, but we feel the value will definitely justify the costs.

Which other solutions did I evaluate?

We evaluated other next-generation EDR

antivirus options, but not any other options like Morphisec. I don't know if there are any security solutions quite like Morphisec.

Defender does well with known vulnerabilities, whereas Morphisec does a job that others can't, with unknown vulnerabilities. The other tools that we have in place, such as our file sharing and email services, do a pretty good job of eliminating the known vulnerabilities from even entering into our environments. But if unknown vulnerabilities are somehow used in an attack, Morphisec has done an excellent job with those attacks.

What other advice do I have?

It just works and it's very easy both to install and manage. I definitely recommend evaluating it. I'm confident that anyone would see the same benefits that we have.

There are two things I've learned from using the solution. One is that their Moving Target Defense is a very unique approach and very effective. It's pretty novel.

The second lesson is the benefit of having that layering. Having Defender and Morphisec has been a really good tandem approach to things. There are a lot of companies out there that may not be comfortable relying on Defender alone, even though it's very effective at managing known attacks. Even in the instances where we're using an EDR, in our case SentinelOne, those Defender and Morphisec layers work really well. We've had good success.

Morphisec does a good job of helping us make sure our endpoints are secure. We've definitely benefited from that. The Morphisec protectors have absolutely done their job. We have not had any instances with viruses, and I would even go so far as to say the EDR tools we have in place have been largely underutilized. They're just sitting there because there really hasn't been much for them to take action on.

Which deployment model are you using for this solution?

Public Cloud

PeerSpot

Validated User Review

Read 13 reviews of Morphisec Breach Prevention Platform

See All Reviews