PeerSpot

Case Study

Morphisec Breach Prevention Platform

Tom Merkle

Chief Information Officer at Houston Eye Associates

✓ Review by a Real User

✓ Verified by PeerSpot

What is our primary use case?

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.

How has it helped my organization?

As far as I can tell, in the year that it's been in, it hasn't stopped a significant attack of any kind. But that's not a negative for me. It is helping me to feel comfortable that all the other layers I've put in place in front of it are doing their jobs. It has definitely increased my comfort level that we are doing the utmost to protect the systems here.

Morphisec saves me from paying for a higher-tier license to get visibility into Defender AV alerts. While it doesn't really save me any money, because I didn't think it was worthwhile to have a product to do that on its own, I love that I get that as a benefit from using Morphisec. But I wouldn't have spent the money on something just to show me the Defender alerts.

What is most valuable?

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.

For how long have I used the solution?

We have been using Morphisec for a little over a year, although we purchased it about 15 months ago.

What do I think about the stability of the solution?

It's been very stable.

Going back to before I had the cloud controller, I probably had to restart the on-premises controller once a month. I would go in and notice that 50 percent of the machines were reporting as offline. I'd restart the web services and they'd all come back. I got into the habit of regularly restarting my machine. That was definitely a stability issue and I was glad to get out of the on-prem solution, to get rid of that.

What do I think about the scalability of the solution?

Scalability wasn't an issue for me because it took very little effort to get it onto our 1,200 machines. I used a third-party software rollout service and it installed, no problem, and worked.

I don't think scalability is an issue, especially now that it's in the cloud. The on-prem server was never overwhelmed from a resource standpoint, so I think it would have scaled just fine as an on-premises solution, but in the cloud it obviously has all the resources it needs.

It's on every endpoint we have, but I don't think the users know they're using it. It's just running. As administrator, when there's an alert, I go investigate it. That's pretty much it. I don't have to do any maintenance because we have gone to the cloud solution.

In terms of increasing our usage, I could potentially put it back on those application servers, but it's not worth the fight because the software is relatively old on some of those machines and it gives false positives all the time. It's just easier to not have it on them.

If Morphisec had an integration with those older technologies, I would be interested in using it on them. I'd rather have it on every server, but not having it on those application servers doesn't concern me too much. The end-users really can't do anything but run that specific application on the server. They don't have the freedom to run other processes there.

How are customer service and technical support?

If anything, tech support might be their weakest link. The process of getting someone involved sometimes takes a little time. It seems to me that they should have all the data they need to let me know whether an alert is legitimate or not, but they tend to need a lot of information from me to get to the bottom of something. It usually takes a little longer than I would expect. The last time they did an investigation, it took about two weeks to decide whether the alert was a false positive or not.

The only thing I was unhappy with was that during the sales process, I thought I was going to be getting a cloud controller. I was very disappointed that I had to build my own controller and operate it. But I don't have to do that anymore. That was the only major issue and they fixed it.

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

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.

How was the initial setup?

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.

What about the implementation team?

The only third party was the reseller, Softchoice, but they didn't do any of the work, they just sold me the product.

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

They charge per endpoint, per year. For 1,200 endpoints and another 60 servers, with the cloud subscription included, it was just under $43,000 for the year.

Which other solutions did I evaluate?

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.

What other advice do I have?

I don't want to think that everything I have put in place is perfect, but we haven't been hacked. I know we are being attacked. I see the logs that show we're probed every day and that we have phishing attacks that come through every day. But we haven't been attacked to a point where Morphisec has been hit as the last line of defense. It's a big deal for me just to have that visibility.

We've had lots of reports of potential threats that Morphisec has handled, but we haven't had a single one, yet, that was a legitimate vulnerability that Morphisec stopped. I don't look at that as a negative at all. I look at it as a positive, that the systems that I have in place are doing their jobs. I really consider Morphisec the last line of defense. That's the way it is set up. Nothing should get to Morphisec if everything else is working. It doesn't bother me at all that we haven't had a significant threat make it to Morphisec. But it's great to know that if one of those was to get through, we have it as an additional line of defense.

When we had it on-premises, it didn't send alerts out, so I would go into it on a regular basis to see if anything needed to be checked out. Now, as of the installation of the cloud version, it actually sends alerts. If I get an alert, I go investigate it.

It also has the potential to save money on my security stack. I'm seriously considering getting rid of our standalone third-party AV scanner, when it's time to renew that next year, and just going with Defender and Morphisec alone. I haven't made that decision yet.

I wouldn't say that Morphisec has reduced the amount of time we spend investigating false positives, because every product I use has the capability of throwing false positives at me. Morphisec does as well and I've had to investigate false positives with it.

I'd be reluctant to give it a 10 out of 10, just because it has never done anything significant. But as far as everything that they've promised and put in place, I would give it a nine. They have followed through on everything they promised. The product is working and supporting me, and like I said, even if it's just proving that everything else I have in front of it is doing its job, that's good enough for me.

If someone has the same kind of systems in place that I had before Morphisec, I would almost say it's a luxury, but it's not really because it helps me sleep at night. If someone has had an attack, that means their current systems aren't cutting it and Morphisec is a great product to have in-house. Morphisec as the last line of defense is as good as you can get. Overall, I'm very happy with the product.

PeerSpot

Validated User Review

Read 16 reviews of Morphisec Breach Prevention Platform

See All Reviews