PeerSpot

Case Study

Morphisec Breach Prevention Platform

reviewer1592379

VP IT at a retailer with 501-1,000 employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We do a multi-layered security approach. Morphisec is really our last layer of defense. It is our insurance policy. So, if a vulnerability gets through the user, network security layer, and antivirus, then Morphisec will then come into the fight.

We have it deployed across all of our workstations and server environments. We have 800 workstation licenses and 75 server licenses.

Right now, we are using 100% on-prem. We have just converted to Office 365. With that, we will be doing cloud hosting as well

How has it helped my organization?

In the last month, we have had two instances that Morphisec stopped, one with Internet Explorer (IE) and the second with another update. We don't know the specific vulnerability that was exploited. We shouldn't be using Internet Explorer here. So, it notified us:

We had a user using IE. It prevented something. I don't know what vulnerability within IE that it was attacking, but it did go to attack a vulnerability, and Morphisec prevented that.

Morphisec makes use of deterministic attack prevention that doesn't require investigation of security alerts. It changes the memory locations of where certain applications run. If you think of Excel, opening a PDF, running an Excel macro, or opening a web page and clicking on a link, all of those actions run in a certain area of memory. Morphisec changes the memory locations of where those run.

If an attack comes in and the hackers are doing a vulnerability on an Excel macro, for example, they know macros are always deployed in a certain area of memory. They write their hacks to that area of memory. Morphisec removes that area of memory and deploys all macros into a different place. When the macro goes to run, it runs in that old area of memory, which no longer is running Excel macros. It basically goes to deploy and blows up, so nothing happens. By morphing the memory location, the hack still gets through, i.e., it doesn't stop the hack from getting through. However, when it goes to run, it doesn't do anything. From that standpoint, it's really looking at: If something happens, it is the last line of defense.

We have a number of other applications that are more forward-thinking where we are looking at logs and training people as well as doing network security. But if a hacker actually gets through all of those different protocols and goes to deploy a vulnerability or malicious piece of code, it will deploy but not do anything. The reason it won't do anything is because Morphisec has moved that process to a different area. So, it is really after the fact.

Morphisec is really good about sending us alerts of security incidents that have happened in the world, saying, "Okay, here is an incident that is happening. It is a zero-day and Morphisec protected it in our labs." They send those out as they come up. I usually get one a week.

We heard there was a company that had deployed Morphisec on most of their servers, but not all of their servers. They actually got hit by a hacker. All of their servers that had Morphisec running were 100% protected. All of the servers that did not have Morphisec got hit. From my standpoint, we have Morphisec across the board. We are acquiring a few other companies, and one of the first things that we are doing is deploying Morpiesec to all the servers and workstations in those other companies.

What is most valuable?

What it does is valuable. A vulnerability might be able to potentially get through and still not be able to run. This is not a question of "If," but a question of "When" someone will get through. If they do get through into our environment, we are comfortable knowing that our last line of defense is Morphisec. A lot of times, without Morphisec, we wouldn't know until we knew. You either get the encryption or it could take a long time to understand. This solution is more of a peace of mind for us.

Morphisec stops attacks without needing knowledge of the threat type or reliance on indicators of compromise. Their development team has developed the security capabilities over a large number of different vulnerabilities, e.g., Adobe Acrobat or Excel macros. We don't have to be experts on any of these. More importantly, the zero-days concern me. All our other security software says that they can stop zero-day threats, but hackers are really good and this is really profitable for them. When the zero-day threats actually get used, it's nice knowing that we have Morphisec.

We don't have false positives with Morphisec.

What needs improvement?

From a company standpoint, a little more interaction with the customers throughout the year might be beneficial. I would like check-ins from the Morphisec account executives about any type of Morphisec news as well as a bit more interaction with customers throughout the year to know if anything new is coming out with Morphisec, e.g., what they are working on in regards to their development roadmap. We tend not to get that up until the time that we go for a yearly renewal. So, we end up talking to people from Morphisec once a year, but it is usually at renewal time.

I tried to sign up for something, but I am still not getting any alerts when Morphisec releases a new version or when our console has been updated. So, I would like to be cognizant when any changes are being made or feature enhancements are added. It would just be helpful to be alerted when that stuff comes out.

Until we migrated to their cloud platform, I wasn't even aware that some of the updates were being pushed out. Then, I came to find out that we were two iterations behind a major release. So, getting those updates or bulletins are very helpful.

If I look at the dashboard, I can see one or two applications hit every once in a while for things like Internet Explorer or some Visual Basic Scripts. I can see that stuff is being prevented, but I don't know exactly if it is securing us in any way that we wouldn't have already had in place. Overall, I don't know 100% if it's increasing our security posture, but it does give us a nice peace of mind.

For how long have I used the solution?

We have been using it for two years.

What do I think about the stability of the solution?

It seems very stable and rock-solid because it is not causing any issues.

I don't require any maintenance on our side.

What do I think about the scalability of the solution?

There haven't been any issues with scalability since we have been on the cloud platform. We do not have to maintain the on-premises servers anymore. It is hosted in an AWS environment, which should be pretty easy to deploy once we add more employees.

Our technical resource is the solo admin at this current time. Two other people have access, but there is not much that we look at or review on it. We just make sure it gets deployed on all our endpoints. That is the only thing we really monitor. As for looking at the console, unless there is something that we need to look at, we are not really reviewing it.

How are customer service and technical support?

We get security bulletins and an email that says, "Hey, this vulnerability just took down whatever company." So, we get technical bulletins that say, "This new zero-day vulnerability just came out, we have tested and stopped it."

The technical support is pretty solid. I did have some issues after we migrated from versions, switching to the cloud version. I ran into a few deployment issues that turned out to be a bad package. They were able to help me with that. They have been pretty good. Anytime I have an issue or question, they are pretty responsive.

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

Before Morphisec, we did not use anything greater than our normal antivirus or malware protection.

How was the initial setup?

The initial deployment was pretty straightforward. It was basically just following the included documentation and working with the admin at the time. We set up a package to push the install out to all our machines. Then, anything that was outside the default library. I added to the protector plan. Certain applications, like Notepad, weren't included in the original deployment. This is stuff that is specific to our environment, like Power BI.

Our deployment took about two weeks.

What about the implementation team?

My technical resource was the one who implemented Morphisec.

What was our ROI?

It has given us peace of mind that we won't be on the news. We do a good job with backups, but if we don't have to use them, that is much better. If the federal government and major corporations who have full-on security teams can get hacked and are vulnerable, then I am not going to say we are not vulnerable. So, for us, it is just a question of when. With Morphisec, at least when it does happen, I feel confident that we have in place solutions that will not only prevent it, but also let us know when something has happened.

Morphisec has 100% enabled our team to focus on other responsibilities or affected productivity. It has reduced our workload by one full-time employee.

Our return on investment is that we haven't needed to have a full-time employee manage it. It hasn't taken away from our other initiatives. Efficiency is really where the savings is. We are getting peace of mind at a decent cost. We can see it working, and it doesn't take full-time resources to manage it.

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

It is priced correctly for what it does. They end up doing a good deal of discounting, but I think it is priced appropriately.

Which other solutions did I evaluate?

Through the years, we looked at Darktrace as well as two or three others. They came with astronomical price tags, while I think Morphisec hit the better price point.

It was not just the initial price tag, but the number of people required to manage the solution. On some of the other solutions, we were able to knock down the pricing considerably, but we needed one to two full-time employees, which we don't have, just to manage the solution. With Morphisec, our technical resource is the main person who works on it. He spends less than two percent of his time managing Morphisec. It is plug and play. It doesn't take a lot of resources, which gives us more time savings as well as being more efficient.

Ease of implementation and ongoing management of the solution were the two top priorities. Our secondary priority would have been cost.

What other advice do I have?

Make sure you implement it on all machines, workstations, and servers. Don't buy it and miss some machines.

Morphisec says they haven't been hacked. From the instances that I have seen when doing research, I find that to be true. Time will tell, but so far it has been working for us.

We will be implementing the Morphisec Guard probably next month. We are just rolling out Microsoft Defender right now. We are evaluating it now. I think we have also started replacing our former antivirus.

Windows Defender and Morphisec go hand in hand, at least from an antivirus standpoint. Morphisec was built to work with Defender, and Defender is a pretty good product. So, that is what we will be using moving forward. From an antivirus standpoint, we just switched our antivirus to Defender within the last month. Between Defender and Morphisec, we don't really have another antivirus need after that.

I would rate this solution as a seven or eight out of 10.

Read 16 reviews of Morphisec Breach Prevention Platform

See All Reviews