PeerSpot

Case Study

Morphisec Breach Prevention Platform

Sean Lewis

Network Administrator at a educational organization with 201-500 employees

✓ Review by a Real User

✓ Verified by PeerSpot

What is our primary use case?

Our primary use case is to protect against ransomware.

We had been hit by ransomware and a couple of our servers went down as a result and some staff computers were affected. We locked everything down very quickly. We were able to restore everything and we didn't lose any data. It took us about eight man-hours to restore the servers, restore services, and get everything back up and running, but it could have been a lot worse than it was. So we looked for a solution that bridged the gap because we have antivirus, we use Microsoft ATP and some other network security measures, but none of them caught it.

We were looking for something that we could layer with security, like what we had preexisting. It turns out it works and integrates very well with Microsoft solutions as well. It bridges that little gap of memory protection that we were looking for to help prevent further ransomware attacks and things like that.

How has it helped my organization?

Morphisec has enabled us to become a lot less paranoid when it comes to staff clicking on things or accessing things that they shouldn't that could infect the whole system. Our original ransomware attack that happened came from someone's Google drive and then just filtered on through that. It has put our minds at ease a lot more in running it. It's also another layer of security that has been proven to be effective for us.

It makes use of deterministic attack prevention that requires the investigation of security alerts. We can always see those and investigate further. It is pretty self-contained and automated. We have not had to really go in to investigate really.

This has made our security team's operations a lot easier. Ransomware has been the biggest threat for us. Of course, we get little attacks here and there on other threat vectors, viruses, and other malware that we have to go in and disinfect. But ransomware has not been an issue and we've even gone through and run a couple of simulated tests for ransomware from other companies. None of them have been successful like Morphisec. It just stopped it dead in its track and it was not able to do anything.

Morphisec has reduced the amount of time we spend investigating false positives. I would say by about 5% to 10%. That typically is how many ransomware-type attacks that we see. It's a low number but it's a very destructive number.

Our team's overall workload has also been reduced by about 5% to 10%. That's just for normal detection, looking for these threats, and trying to find out what it is.

Now, if we were to be infected again, it would then be reduced by a lot, just because depending on how far the infection gets, how many man-hours that would be, we know that would be very significant. We've only been hit once in the past by this. And luckily it was pretty minimal, but it could have been very severe, and then it would have really impacted us on man-hours.

It helps us to save money on our security stacks. It's priceless just because if we were to lose all of our data from an attack like that, there would be no way to get it back without paying massive amounts for ransomware. And there's no guarantee that if you pay for the decryption key from whoever's holding your data ransom, that that's even going to work or that you'll get everything back at the end. Morphisec has been a real lifesaver.

It makes it super easy for IT teams of any size to prevent breaches of critical systems. They have a way to mass deploy it on all of our Morphisec clients. It's very easy to manage, very easy to deploy, and it's also very easy to maintain.

What is most valuable?

The fact that it's able to automatically detect and block ransomware attempts is the most valuable feature.

What needs improvement?

The dashboard is the area that requires the most improvement. We have about, I would say 5,500 computers currently, and searching through all of those takes some time to filter. So as soon as you apply the filter, it takes a few seconds. It crunches, it thinks, and then it brings up the clients that match.

Our computers are named and they have a serial number in front of their name. To be able to see who is signed in or who has a computerbased on their Microsoft account, that part is cut off unless you have a larger screen on a tablet. But on your cell phone, there's no way that I can find a scroll over to see who owns that device because the username is just cut off. Besides that, it's a simple interface. It's a simple product that's easy to maintain and manage. There's not a lot that we have to do with it. It just does what it needs to do.

For how long have I used the solution?

I have been using Morphisec for close to a year.

What do I think about the stability of the solution?

In terms of stability, so far it's worked great. It's been very stable, with no problems, and it continues to be effective so far. If for any reason, we get ransomware infection in the future, we'll know that there's a problem, but so far it's been good. All of the tests that we've run with ransomware simulated software from other vendors have all failed.

What do I think about the scalability of the solution?

Scalability is very easy. It's not a problem. If you have the means to remotely deploy the client to all of your computers, scalability seems so far infinite, it's not a problem. If you can afford the budget for all your computers then you're good.

We are right around 5,000 or 5,500 users and their roles are anywhere from student to staff members, to administrators, and even our board of directors use it. Everyone has it. All of our computers are deployed by us. So everyone gets a computer, whether it's a student or a staff member, it's not on personal devices.

Every one of our computers is using it. All of our servers are using it. It's pretty extensive in how we're using it in that sense. But it's really just toward the ransomware side.

How are customer service and technical support?

We used technical support only for the deployment or the migration from on-prem to the cloud. We've been having to deal with them on what steps we need to take and what we need to do to make it work. They made sure that it's a smooth transition, that we don't leave anything exposed as we're moving from one to the other, but that's it.

Support is pretty good for the most part, once in a while though, just because of their accent, it's kind of hard to understand them. We in particular had one tech that we were speaking to about the migration portion of it. There were three of us sitting in on that meeting and none of us could really understand or comprehend what he was trying to convey. It was not an issue with everyone else that we had dealt with.

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

We were using another solution that wasn't necessarily specific to ransomware. We were using Microsoft ATP in conjunction with Sentinel. We were starting to deploy Sentinel as well, which is also Microsoft's product, and trying to tie everything together, to make it more robust, but they did not have anything that dealt with the memory type encryption that Morphisec uses to help protect against those types of infections that ransomware often exploits. We didn't have anything specific to ransomware other than Microsoft's ATP and it does not catch everything.But we still run ATP anyway. It ties in with Morphisec very well, even within the Defender dashboard, you can punch in your key and it will bring it up and give you some more information about it, making sure that they play well together. It literally bridges a gap that Microsoft ATP has.

How was the initial setup?

The initial setup was very straightforward, especially for self-hosting. One thing to note is that we're currently looking to move to their cloud-hosted system and move away from the on-prem. That is proving to be so far a little more complicated to move from one to the other, at least from on-prem to the cloud. But not impossible. There are a lot more steps and processes to getting everything migrated over. We have to push out a new client to all of our client computers.

The deployment was a matter of a couple of hours once they provisioned the license and everything for us and provided us with everything. We were able to spin up a virtual machine to install everything on, open up the ports that were necessary, which were very easy. Then we just push out the client to all of our devices. We use a combination of Intune and SmartDeploy for remote imaging to push the software out to everybody. Once that was done, we plugged the license key into our Microsoft ATP, just for the integration of that. And that was it. It was up and running and good to go.

We tested it on just a couple of client computers initially, and then one test virtual machine for our servers. Once everything was looking like it was fine, then we just went ahead and pushed out to everything. There were no conflicts, there were no problems. Nothing came up as a red flag. Nothing got blocked that shouldn't have been. It went nice and smooth.

It took two of us to get this done, and that was our systems admin who deals with our servers and a lot of our client computers and then myself, which I handled the networking side, like opening up ports, making sure all the IP addresses were correct.

What about the implementation team?

We went directly through Morphisec. I don't think we had a third party or a vendor for the implementation.

What was our ROI?

We absolutely saw ROI. We did not pay that much for the licensing. It was very affordable. The peace of mind and not having to deal with or worry about as much as we did in the past about ransomware attacks, and just knowing that we're pretty well covered for the most part is ROI.

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

It is a very cost-effective solution. It's very affordable for what we're having to use Morphisec for.

It's extremely affordable for what it does, at least the product that we're using through Morphisec. I know that they have a few others that we're not using, but we don't need it. They did provide us with educational pricing as well. They were very flexible because we deployed it during COVID times and a lot of people were getting hit more and more with ransomware. And so they were also very flexible in what they were able to provide for the price. They understood that our budget was being cut because we had lost a lot of students as a result of COVID. They really worked with us, which was great.

The licensing is also very fair. It's per device. So it was also very easy.

It's just a year-to-year license that we are paying for. There's nothing hidden, no extra charges that were unexpected or anything like that. It was very straightforward.

Which other solutions did I evaluate?

We looked at a couple of solutions and it would have been a full deployment where we would have to install their entire antivirus line on the product. They didn't have anything that just handled what Morphisec does. It would be a full product suite. We'd have to deploy that to everybody. We would have to ditch Microsoft ATP, which, again, we get free because we are Microsoft partners in education so it's included with our licensing of Office 365. And it would have been a lot more expensive to go a different route than what we found in the end.

What other advice do I have?

My advice would be to make sure that if there are a lot of computers, especially if they're remotely distributed, make sure they have some sort of solution to easily push out and deploy it to multiple clients. That's probably the biggest hurdle that I think a lot of people would have. And we had two solutions already in place for us in the past that worked and that were compatible. The nice thing is that they were able to provide a Microsoft MSI Installer so that you can even have it so that it pre deploys it while you're imaging your computers if you're using Microsoft for imaging. It's the same thing if you're using Intune through Microsoft.

We've always been looking for something that would help to protect more against ransomware in our case. And this was it. This is the best solution that we found that worked for us.

I would rate it a ten out of ten. My only complaints are the dashboard and that's not even terrible. It still works. You just have to be a little patient.

Which deployment model are you using for this solution?

On-premises

Read 16 reviews of Morphisec Breach Prevention Platform

See All Reviews