PeerSpot

Case Study

Morphisec Breach Prevention Platform

reviewer1598802

Senior Systems Admin at a transportation company with 501-1,000 employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We've been using Morphisec as a layered defense in our security plan. We have beefy firewalls and another antivirus; Morphisec isn't technically an antivirus. It's a protection agent. It's one of the layers of our security plan. We use it to defend ourselves from any sort of CryptoLocker attacks or ransomware drive-bys, and it should catch auto-executes that come from ads. We haven't been breached, as far as I'm aware.

We started with it on-prem and we had no complaints. It made sense. A cost analysis was done and on-premises cost less than the cloud, which is how things normally are. We used our own network so the cost was cut because they didn't have to use any of the load on their servers or network. It was all on us. But about a year ago they approached us and we were torn away from the on-premises solution. They made such a compelling cost-savings case for us to go to the cloud that it made sense to go to the cloud. We also got another service from them along with the protector, some sort of BI.

We're using it on all of our endpoints, servers and desktops that users touch. For servers that don't get touched by users, we don't have Morphisec on them because we just don't need it.

How has it helped my organization?

I wouldn't be doing Morphisec any favors saying, "Well I can't tell if it's working because the rest of our security posture seems to be taking care of anything else that gets through." Maybe it's not working at all. I can't tell. It would be useful to

set up a virtual machine—and this is something I should bring up with our Morphisec person—and get some triggers that are actually on our dashboard so we can prove to management that Morphisec is doing what they said it was going to do. Worst case scenario, we have an infected virtual machine that I just blow away. The short answer is that we haven't seen it protect us from something yet.

It hasn't taken anything off my plate. It's just a "gun under my pillow at night". It's something that we can tell our cyber-insurance people, "We have this, and this was used." In "Pretend-Land," where we got compromised, we can say, "We have all these layers of security and it managed to get through all of them, so we did our due diligence. Now please pay us for our losses."

What is most valuable?

What's valuable is really the whole kit and caboodle of the Morphisec agent. What it does is genius, in a way, until the bad guys get wise to it. You set it up and then you watch the dashboard. There isn't really much tinkering. As long as you did the install correctly, it should be pointing at your server and it will tell you a bunch of information on each client.

What needs improvement?

We have only had four attacks in the last year, "attacks" being some benign PDF from a vendor that, for some reason, were triggered. There were no actual attacks. They were just four false positives, or something lowly like adware. There have been false positives with both the on-premises solution and the cloud solution.

I'd rather see false positives than not seeing anything. If I see nothing then I literally cannot tell if it's working or not. But there are some false positives that are ambiguous enough to be caught.

For how long have I used the solution?

We have been using Morphisec for about two years.

What do I think about the stability of the solution?

I don't look at the dashboard every day, but the on-premises solution was flawless. If the network was down between the clients and the server in our local area, we would be in trouble. But Morphisec's AWS implementation has been stable as a rock.

What do I think about the scalability of the solution?

I believe it's scalable. I don't know what the upper limit is. Our company is a medium-sized business, with about 100 end-users and 500 employees in total. Morphisec easily holds those

100 users.

All the end-users are using the solution, meaning the solution is attempting to protect them from the silly mistakes that they make. But there are only two of us who actually look at the dashboard.

The business is growing so we do increase the number of clients. Whenever we add a new computer, we add Morphisec to it. Once we get to version 5, we'll revisit the ATP integration.

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

We didn't have a solution before Morphisec for this specific layer of defense, for the CryptoLocker/ransomware niche. We had an antivirus.

The demos worked great. They would open a bad file on a virtual machine and we watched the CryptoLocker being stopped in real time. It's hard to compare with that.

How was the initial setup?

The initial setup was definitely straightforward. It has to go on every computer. There's a different installer for desktops versus servers. You just choose which one is which. We use PDQ Deploy, and a script that the onboarding technician helped us with, and it worked. It ran perfectly. We even have scripts for uninstalling it and installing the newer version, and Morphisec assisted us with that. It was definitely easy to do.

Before I saw the version 5 update and the notes on that, about how it's going to update automatically, I'd say the implementation was a slight pain. It wasn't a huge pain but you can't really get away from how you have to install this on all your computers. However, they actually made that process very easy, and I can do it with just a couple clicks to almost an entire organization, as long as computers are online.

Over the course of a day, it took about two hours to get the script going and select all the computers for each kind of installer. I kept running it over the course of the day because certain computers would be turned off or they were restarting. I had to do a good couple of runs of it, but it was very simple and quick.

Since there was nothing already doing what Morphisec does, on the computers, and Morphisec plays well with the current antivirus that we are using, we just installed on each computer remotely and it started working. We watched the dashboard fill right up in a matter of minutes.

We're not on the latest version but I'm actually excited for the latest version because it will do away with the manual updating process. The clients will start to update themselves. We will have to wait until one of our Morphisec representatives reaches out to us so that we can get the installer for the newest version. Version 5 is where it begins self-updating. Until now, I've had to manually update each time we wanted to do an update. The new one will mean I won't

need to be worrying about updating or if the versions are out of date.

In terms of working with the solution, if Morphisec says, "Hey you're going over the number of licenses," we look to see how many are offline and we look at the versions. We look at it just to make sure that everything is going okay. We have alerts for when there's a threat. We get emailed saying, "Hey, look at this. There's a threat going on on XYZ computer."

What was our ROI?

I haven't seen ROI because I haven't seen a threat that it has protected against, exactly. If you're always wearing a bulletproof vest and you never get shot, was the vest worth it? I'd rather have it than not have it.

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

We looked across the rest of the security field and we spent more money on Morphisec than other solutions that do a similar thing, but the demos that we've seen were impressive enough to sway management. The technology behind it is clever enough for us to think it's cutting edge. It didn't save us money but we spent money on it because we thought it would be a good product.

Which other solutions did I evaluate?

The way that they explained how their solution works was more in-depth than other solutions that we were looking at. It looks cleaner. It has a good UI for the dashboard. It's not overbearing with security tabs and a lot of other stuff. It tells you, "Here's the list of all of your protectors. Here are all the threats. Here's the dashboard that gives you a little bit of everything," but not in an overwhelming way.

What other advice do I have?

It sells itself, honestly. My advice to others looking into implementing Morphisec would be to use PDQ Deploy. The hardest part was getting all of the endpoints protected in a timely manner, but Morphisec assisted us with that. They suggested PDQ Deploy, which is a great tool. Implementation went so smoothly because of that.

Morphisec provides full visibility into security events from Microsoft Defender and Morphisec in one dashboard, although we're not currently utilizing that feature. We're definitely interested in it. The reason we're not using it is because you have to purchase the upgraded version of Defender for Microsoft. We thought it was the regular Defender that each one comes with, but it's actually ATP, Advanced Threat Protection. That's what integrates with Morphisec. We're just waiting for the CFO to say, "All right, who

wants a bigger budget?" and we'll say, "Yes, us, please: ATP." We would do it if we could bend our CFO's arm to get that kind of protection.