PeerSpot

Case Study

Morphisec Breach Prevention Platform

Jeff Magnuson

Sr. IT Architect at Yaskawa Motoman Robotics

Review by a Real User

Verified by PeerSpot

What is our primary use case?

When Morphisec first came out, it was on-prem and we used a group policy to deploy it to the endpoints. Working with them was one of the things I did and then obviously when Covid hit I had a large majority of my workforce that started working remotely. And deploying new endpoints remotely using GPO can be a struggle. I talked to them about that and the next day I got a phone call. We're actually moving to their cloud platform that does automatic updates in the cloud now. So that if I have people working remotely, they get the update automatically. It's not signature updates and whatnot, since it's signatureless, but agent updates. If you're 4.1 to 4.15 or 4.16, those will all get deployed automatically from a cloud server, which really opened up a lot of things for us as well.

That was our request. I went in and they started working on it. I worked with them on the development of the dashboard. They're always looking for customer input about what they can do better. They're constantly asking and getting input from their customers about stuff to improve the product, and there are not a lot of organizations that do that either.

How has it helped my organization?

Morphisec has reduced the amount of time we spend investigating false positives. We can see what's going on in the dashboard. We're a robotics company so we do a lot of in-house development. And so we see false positives on occasion due to whatever reason. When I see that, I contact them, we'll look at the signatures, the hash and the memory affirmation, and stuff

that's provided through the attacks. They analyze that, we look at the application and then they resolve it, or if it's a rare thing, I can just exclude it so that it doesn't get looked at.

It's very quick and easy to do, so it's not like I'm waiting weeks for them to analyze data. We send them the logs or they get the logs automatically, depending on how I have stuff set up, they review them, call me the next day, and tell me what we need to do. And it's over with. It has reduced my team's workload by 30 to 40%.

Morphisec absolutely helps us to save money on our security stack. Budgets were tight during COVID and we had some companies that were jumping. Their prices were going up and up and taking advantage of what was going on in the industry. Morphisec didn't do that. They stuck to their guns and said, "This is the cost of our product and we're not going to take advantage of the customer." That economic side was huge for them as well. Compared to other products, their pricing is very good and very competitive.

The product has absolutely worked flawlessly. We have had basically no issues, either with the product or with any type of virus or zero-day attacks, ransomware, nothing. It has caught everything. And the one thing that's been unique about them is I read a lot and do a lot of research on the products that are out there, and there have been some products that are widely used like CCleaner and such that had been packaged in some of these programs that Morphisec has caught. They've contacted the manufacturers of those programs to say, "This is what we found." And rather than just letting it go on, they're contacting other manufacturers saying, "You just deployed something and it's got some adware." And so they can fix their product and then redeploy the fixed version out to the public. They're looking out for themselves, but they're also looking out for other organizations as well.

What is most valuable?

There are two primary valuable features.

It works without the end-user having to do anything. It just works.

Second, the fact that it's signatureless is valuable. It's very light on the endpoint and does not have any performance hindrance on the endpoint. That is a huge plus as well. We've used some other products in the past that just really bogged down the machine. If we do scans in the background, and I get a request that someone wants to do scans at night, it's fine. You can take your computers home and turn them off in the evening. I don't have any of those kinds of issues with Morphisec.

Morphisec's approach to using deterministic attack prevention is a big deal for us with all the zero-day attacks and ransomware that's going on in the industry. What we've seen is quite a downturn in the virus or signature-based attacks on the endpoints and even malware. The zero-day attacks are really at the forefront industry-wide, whether it be my company or financial companies.

Since using Morphisec we have seen a downturn in attacks because Morphisec protects us versus Defenders and whatnot that are signature-based. I know we have not had any issues with ransomware or other zero-day attacks that we've seen with machines that, all of a sudden, have become before we instituted the product. Now the machine had to be re-imaged and there was a loss of data because something was on the machine. You couldn't really determine what was on the machine because nothing was picking it up. The products we were using weren't picking it up.

What needs improvement?

We're getting ready to deploy the cloud platform. I've already got the cloud portal and everything available to me. There are some nice additional features in there that were some of the things that I had requested previously. Those are some of the features that I was looking for on my on-prem platform that they've already instituted in the cloud and that I'm sure will be instituting on their on-prem platform as well. Having to have an on-prem server required a lot of administration. Being able to push that to the cloud and have it managed up there for us is a real nice addition.

For how long have I used the solution?

We've been using Morphisec since the inception of the product. We were really one of the first commercial organizations in the United States to use it in production. So, we started with a version 1 product, which was several years ago. We were looking to complement our stack of endpoint security products. I then went out and started doing research for primarily zero-day signatureless software that we could utilize on our endpoints. Doing my research, I came across the Morphisec product, placed a call to them, ended up talking to one of their founding members of the product. We also looked at CrowdStrike, Carbon Black, SentinelOne and some of the other similar types of software out there. We decided that Morphisec would definitely be the best solution for us.

What do I think about the scalability of the solution?

As far as scalability, you can put it on a couple of endpoints or you can put it on thousands of endpoints. The initial installation is very fast. It's a minute and a half, two minutes, and you're done. You walk away.

The machine connects to the domain, the application's installed and it shows up in the dashboard and you move on. We put it into the group policy, there's the script, send it out, install it on the endpoint and we don't have to touch it.

Whereas with a lot of the other applications, you have to touch every single machine and make sure that it gets installed correctly, and that it's

loading correctly. We just don't have to do that.

It's so fast that the end-user doesn't even really know that it's happening. For the end user's experience, it's absolutely over the top. We've had other products in the past that we've used and we've had complaints. The CPU could be dragging because their thing is doing some big scan in the background, or the application or agent itself is, for lack of a better term, very heavy so it uses a lot of memory and uses a lot of CPU, and drags down the machines. I have a company of engineers and scientists and they want all the horsepower they can have on their machines and don't want something running in the background that's dragging down what they're trying to, where they're trying to work.

We're doing between six and seven hundred nodes.

I have several people that monitor this stuff but it really takes one person to set it up and let it go. It takes a very small piece of one person's time to do this. I have multiple people because I want them to be able to have experience and understand what's going on in the environment.

To administer it, it takes less than an hour of my time a day. I get reports sent to me. I can review reports. If I need to go into the dashboard, I can pop into the dashboard very quickly, see what's going on, see if there's anything that needs tending to, and then move on about my day.

What was our ROI?

I have absolutely without a doubt seen ROI. It's the cost savings compared to other products, the performance of the product, and the amount of time saved by my team on issues that were happening before we installed Morphisec and utilized their product. I got a return on investment in less than a year.

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

I do not have to pay extra for anything. We're an Office 365 shop but we do not use the MS3 E3. If we would turn around and use that product in the cloud as far as Office 365, then the integration is instantaneous all the way through into Office 365. But that's not dependent on Morphisec. That's a dependence on my licensing with Microsoft.If you don't have that integration, Morphisec integrates with just the Defender on the desktop. It's built-in. You're not paying extra for something to have that feature set.

Which other solutions did I evaluate?

One of the things we looked at was to see how the solutions affect the endpoint performance. Because when you start stacking up products on top of each other, on the endpoints, you can run into performance issues, memory consumption, CPU consumption, and

whatnot. Morphisec was very light and does not consume hardly any CPU or memory. It runs in the background unknown to the user. It doesn't do a bunch of alerts and stuff to the end-user. It just works in the background. Then you have a dashboard and a portal that you can manage and see what's going on. Morphisec was a really good fit for us.In the early days, on a Windows platform especially, you had third-party virus protection applications. McAfee, Kaspersky, Norton Symantec, and those types of things, and we've used several over the course of the years. When we finally migrated fully to Windows 10 platform, Windows Defender was much better at what it did. And one of the things that came up the pipe was Microsoft integration with Morphisec so that I can see what Defender's doing as well as what Morphisec's doing in our dashboard or portal. That was very unique and this worked out very well.

The other solutions at the time did not provide those things, and so that was a big plus for us too. It was nice to be able to see what's going on with Defender endpoints as well. It has been a great product for us. It definitely does what it says. Their support is second to none. If I have an issue with a false positive or something, I can place a service request and they're on it right away. We review it and they resolve it. I really can't say enough about the product and the team that supports the product. They've been great. They've treated me like kid gloves since the very beginning.

What other advice do I have?

I've used their product since its infancy, if they're looking for a product that is reasonably priced, does what it says it's going to do, requires very little administration and deployment effort, then this is the product I would be looking at.

Compared to what I've seen out there right now, I'd rate Morphisec a 10 out of 10. I really can't say enough about the product.

There may be some other products coming out there that are going to compete, and that's fine. And if you look at those other products, you better take a really good, hard look at Morphisec and see what they can do. Look at the whole entire package, the support groups, and what type of support they get that you're getting, that you may not get with other products. That's an important piece for us, if something does go wrong, you know you've got someone you can call, you know you've got a support portal to put in a ticket that you're going to get a very quick response from. You look at the whole package, not just one piece of it.Since the beginning, their deployment strategies and everything has continued to improve and get better and better. You can't do that if you're just sitting in a room, a bunch of engineers and say this is what we're going to do and this is how the customer has to do it.

They treat me with kid gloves and I really can't say enough about the product and how it's performed for us and the support we continue to get, even years later. I get the same amount of

support that I did in the early days.

Read 16 reviews of Morphisec Breach Prevention Platform

See All Reviews