PeerSpot

Case Study

Morphisec Breach Prevention Platform

Brian Lindow

Director, Technical Services and
Information Security at SECURA
Insurance

✓ Review by a Real User
✓ Verified by PeerSpot

What is our primary use case?

Our use case is to augment our antivirus software that's on our endpoints to go in tandem with Microsoft Defender. It's also going on our Windows and Linux servers as well.

How has it helped my organization?

Morphisec has helped us in our deployment strategy of endpoints and keeping a good inventory of our assets. We do that with Defender, but this is another tool to help us know what assets we have deployed, the ones that Defender doesn't always cover.

If Defender is turned off somehow and Morphisec is on then we can investigate. Or the other way around, if Defender's on and Morphisec is not installed, we can have it installed. It does checks and balances on our deployment so we're not left with an endpoint that's unprotected.

What is most valuable?

The ability to stop attacks without having to detect or have a signature for the attack is the most valuable feature. It's just a different way of stopping attacks, by defeating it at the endpoint before any damage is done.

Morphisec provides full visibility into security events from Microsoft Defender and Morphisec in one dashboard. Defender and Morphisec are integrated. It's important because it lowers the total cost of maintenance on the engineer's time. The administrative time is dramatically reduced in maintaining the product and saves an engineer around four to five hours a week.

It's extremely easy to deploy. It functions without needing to talk to a server. It's completely silent once you've installed it. It's been really silent behind the scenes and has not conflicted with other software. It's a real set and forget.

What needs improvement?

We started in the Linux platform and we deployed to Linux. The licensing of that has been confusing between Linux licensing and Windows licensing. The overall simplicity of licensing or offering an enterprise license to cover everything and not needing to count needs improvement.

They've integrated with Defender well, but they should continue maturing that integration so that you can just check boxes with Defender installed to add Morphisec as well. There's licensing and all that, but they should try to make the implementation as easy as possible. It's easy now but they should continue down the path of making it as easy as possible.

For how long have I used the solution?

I have been using Morphisec for two and a half years with a POC before that.

What do I think about the stability of the solution?

From what we've seen it's stable as it can be. If there's such a thing as 100% availability, it's there. I think the architecture of it being deployed and standalone for all desk purposes makes it super stable. The biggest concern was conflicting with the applications on the desktop, and we had not seen that at all. It's been very reliable. We haven't been on the cloud version for very long, but so far it's been very reliable.

What do I think about the scalability of the solution?

It should scale without an issue. It's about the deployment strategy and getting it deployed. Once you have a good deployment strategy, then it can scale to hundreds of thousands of endpoints, if you have them.

We are protecting around 3,000 endpoints. Then when we're all finished, there'll be about five to 6,000.

There is no upgrade that we know of yet, so we're on the latest version. I would anticipate once a year that we would have an upgrade to the endpoints. And it would probably take 10 to 20 hours of information security engineer's time to make that happen.

How are customer service and technical support?

Their technical support is very good, responsive, and has good follow-through on open tickets. We don't have any issues with them.

How was the initial setup?

The initial setup was relatively straightforward. We first installed Morphisec before they had their cloud server, which was a little bit more complicated. But now we've converted to their cloud server, which has made it much, much easier. You don't have the burden of setting up a server and getting the missing libraries and all the issues of setting up a server. Now with the cloud, it's simple.

It took us three weeks to set up with the server.

We did a proof of concept first, and then we tested it to make sure it would catch known malware with no antivirus on the endpoint. Then we started the deployment strategy and our deployment strategy was laptops first, then virtual desktops, and then servers.

What about the implementation team?

We worked with Morphisec and our own engineers for the deployment.

We had a very good experience with their engineers. They were very knowledgeable about the Microsoft stack, easy to work with, and responsive.

What was our ROI?

Our ROI is having another level of control. I can't yet identify breaches that Morphisec stopped directly, but it'll pay for itself once it does that. It's really the extra layer of control that we didn't have before.

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

We've gone through several iterations over renewals. I think it's reasonably priced. I wouldn't say it's cheap, but I also wouldn't say that it's over-the-top pricing. An enterprise agreement would be nice so we don't have to try to count or get an estimate of the number of endpoints. If we go through growth and add 500 laptops, I don't want to have to go back and change our licensing to add that capacity. I'd rather just have that built into the contract.

We haven't seen any additional costs to the standard licensing.

Which other solutions did I evaluate?

The options we looked at were more in the antivirus space. Morphisec as a product does not have direct competitors because of its unique architecture. There are other advanced endpoint protections that I looked at, but this one was by far the most unique architecture. It has a unique way of adding another layer of controls on the endpoints.

What other advice do I have?

Morphisec hasn't added to my team's workload. It hasn't reduced it, but it hasn't added to it.

I didn't buy it to save us money. I bought it to add another level of control at the endpoint beyond antivirus. So it's really adding another layer of defense.

My advice would be to understand how Morphisec works from the Bad Actor's perspective, on how a Bad Actor or malware can compromise Windows or Linux. Morphisec gets to the root of those compromises. Rather than trying to detect the compromise, a design in the operating system issues and defeating those there or rather than trying to respond to changes in malware, they're defeating it right at the exploit level.

I'm part of Morphisec's sales team half the time when I'm trying to educate other IT leaders, my peers, or other CISOs on how it's actually working because it takes a little while to understand it. So my advice would be to really try to ask questions about how the architecture works. Because it doesn't really work like another AV. It works much differently than other endpoint protectors.

I would rate Morphisec a nine out of ten.

Which deployment model are you using for this solution?

Private Cloud

PeerSpot

Validated User Review

Read 16 reviews of Morphisec Breach Prevention Platform

See All Reviews