PeerSpot

Case Study

Morphisec Breach Prevention Platform

Norman Kromberg

VP of Info Security at
SouthernCarlson, Inc.

✓ Review by a Real User
✓ Verified by PeerSpot

What is our primary use case?

We purchased Morphisec to protect our endpoints from anomalous behavior. The biggest use case would be to prevent ransomware, but also to detect other unnecessary programs running on devices. So, the use case has been endpoint protection, both for servers and endpoints, e.g., laptops and desktops.

We do a multi-layered defense in-depth. They are our primary prevention at the endpoints for anomalous behavior. I would classify it as a preventative tool, since Morphisec blocks and prevents execution. So, I would put it at the preventative layer.

We have agents on all of our endpoints and servers pointing to their cloud instance.

How has it helped my organization?

Morphisec makes it very easy for IT teams of any size to prevent breaches of critical systems because of the design of their tool. When we evaluated Morphisec, the CIO and I sat and listened. What attracted us to them is the fact that it stops activity at the point of detection. That saves a lot of time because now we are not investigating and trying to trace down what to turn off. We have already prevented it, which makes it very much safer and more secure.

What is most valuable?

The biggest feature is its ability to prevent. Here is the interesting thing with a tool like Morphisec. You implement it almost as an insurance policy. If it works, nothing happens. If it fails, you have bad things occurring. So far, nothing terrible has happened. It does a good job of reporting when it detects anomalous behavior so we can research it. However, the key is that we can research in a much calmer fashion, since we do not need to uninstall because it blocks the activity.

What needs improvement?

Morphisec is a venture startup. They are still early in their growth stage. They need to get mature on their customer support and on how they interface with system tools. For example, they need to get multifactor in place and an API for the major multi-factor systems, e.g., Okta, Duo, Ping, and Microsoft. They don't have them built in yet. They are working on them. It is just not there yet. Also, their stability, customer support, and processes need improvement, which is just part of maturity.

For how long have I used the solution?

My company has been using Morphisec since mid-December of 2020.

I have been aware of Morphisec since I worked for Optiv and met one of the key sales people back in 2015 or 2016. When I was at that company, I was a consultant helping companies with their roadmaps. So, we connected there and got Morphisec introduced to Optiv, the company I was working with then, who is also a VAR. Therefore, it was getting the product in via another sales route or sales channel.

What do I think about the stability of the solution?

It takes less than one person to deploy and maintain the solution. So far, we have not had to do maintenance. The biggest thing that we are working with Morphisec right now on is the multi-factor interface enhancement.

What do I think about the scalability of the solution?

We have had no issues with scalability. It's worked fine.

We have probably 10 people between our help desk, Tier 2, and executives accessing the system and using the dashboards, which has been pretty straightforward and easy to do.

In the system, our IT people research alerts. We get a daily report of all the events from the prior day. If there was a critical alert, the help desk will go out and research to see if they need to do anything with the endpoint. They have to go into the system to monitor and look at it. If we are running into an issue on a particular server and endpoint, we may go out there to see if there was any indication of an issue or if the actual agent is causing a problem. We have yet to find that the agent is causing a problem, but that is why they potentially would go out there.

It is on every endpoint, e.g., laptops, desktops, and servers, which is pretty extensive. We may expand into their incident response process and a number of other things that we can use them for, but that will be evaluated as we go into our budget cycle at the end of the year.

How are customer service and technical support?

I would rate Morphisec technical support as eight out of 10. They have just been very responsive. They are very strong at follow-up. They won't close tickets until we tell them to. They are very much a customer service focused group. They have been very good at tech support, providing knowledge, information, etc.

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

Morphisec makes use of deterministic attack prevention that doesn’t require investigation of security alerts. We didn't have a protection layer prior to Morphisec, so we added it. The key is the amount of work by the team is minimal. So, it did not increase our workload. We did not have to add staff. It has been a positive benefit that way.

This solution was an additive layer that we didn't have before. So far, it has been successful in the sense that it has not caused us to add resources. So, we have been able to get layer protection without additional expense, in terms of staff. That is a good thing.

How was the initial setup?

The initial setup was very straightforward. It was simple to install the agent. They provided good support. It was just a push, then it just took minutes to get the process rolling. We could monitor how well it rolled out, and they were there to support us. This was one of the easiest that we have ever done.

The deployment took a day or two in total actual work time, so we could confirm it reporting in on the dashboard.

It probably took us a week or two to get it rolled out to all the devices because of our change control windows.

We put it in the most conservative setting that we could for prevention. We did roll through certain applications for the logic of what not to include, but they had a pretty good baseline for what we should reference. We then just pushed the agents with some logic on the change windows. So, we did all the desktops and laptops first, then the servers. It was a pretty straightforward implementation.

What was our ROI?

Morphisec helps us save money on our security stack. We probably would have spent $100,000 more on a different solution. So, it did save us on that expense.

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

It is an annual subscription basis per device. For the devices that we have in scope right now, it is about $25,000 a year.

Which other solutions did I evaluate?

We also evaluated CrowdStrike, Cylance, and SentinelOne. CrowdStrike and Cylance were way too expensive. You could also throw in Sophos and Symantec in there. All those were too expensive and burdensome. SentinelOne was interesting. We were able to get better pricing and better access to the top people at Morphisec, and that is why we went with Morphisec.

We do not use Morphisec for antivirus at this time. We are using another tool for antivirus, but we will look at Morphisec Guard when that license is up.

What other advice do I have?

Don't overthink it. Just do it. Follow the directions of Morphisec and go for it, but make sure you understand what your application stack is before you go full bore, so you don't create false positives. However, they are easy to work with in those terms.

The reality is nobody ever gets to a single pane of glass or a single dashboard. Those claims are made by vendors, even Morphisec will make it. The problem is you have so many layers in your security stack that you will never get to a single pane of glass. So, I never have that as a requirement because I know it is not attainable.

We do not have Microsoft Defender in place, but so far it is providing visibility for what it is installed on.

While I have known of the company since 2016, they are still a startup. They are still equity-backed. I don't know where they are going to end up, but right now I am confident that they have good backing and financial resources. They got a new round of funding just after the first of the year. That is always a good sign.

Biggest lesson is the amount of discipline required in our company to stay current. Morphisec highlights breakdowns that we have in process and procedure, which is a good thing, but it's highlighted to us that we need to be a little bit more disciplined.

I would rate Morphisec as nine out of 10.

Which deployment model are you using for this solution?

Public Cloud

If public cloud, private cloud, or hybrid cloud, which cloud provider do you use?

Amazon Web Services (AWS)

Read 16 reviews of Morphisec Breach Prevention Platform

See All Reviews