PeerSpot

Case Study

Morphisec Breach Prevention Platform

reviewer1633446

Director, DevOps at a tech services company with 51-200 employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We use version 4. It's not the absolute leading edge, but it was the first version that they supported with Linux.

We use both environments to protect our corporate Windows assets and we also use them to protect our production Linux servers. We're using an on-prem option where we installed the Morphisec server on one of our own pieces.

Our primary use case of Morphisec is to prevent in-memory attacks that would be conducted from ransomware. It's used for frontline and back-end protection. We have it installed on our front-facing web servers and on the backend database servers as well.

How has it helped my organization?

Morphisec has given me a lot more visibility into if my employees are actually encountering ransomware. Luckily, to date, we have not actually had any positives come through. We have had false positives, but at least it has given me the peace of mind that upon the investigation that we have not been exploited or have had ransomware, for that matter.

In the future, it'll help me with ensuring that viruses are not inundating our machines as well. Right now I have to go through a separate interface for that.

Morphisec makes use of deterministic attack prevention that doesn't require the investigation of security alerts. Anything that's suspected gets blocked immediately on the machine, which is

nice. It allowed us to go back and see what was going on in that situation. And if it was in fact a false positive, then either we figure out a different way to execute whatever the person was trying to do or we can whitelist the event.

Morphisec does not save us at this point from paying for a higher-tier license to get visibility into Defender AV alerts. I'm sure once we get upgraded, absolutely it will, from what I've seen.

It reduced the amount of time we spend investigating false positives. In the past, we haven't had any legitimate ransomware attacks, all we have had is a false positives pop-up. But knowing that ransomware, once it's on a machine, pretty much tanks it, I'd say it saves me hours upon hours of having to recover individual machines, and of course, it could become exponential requirements if there was more than one machine affected. At the very least when it could be one server, it would definitely save me hours of labor up the scale if I had 80 machines that I had to fix. But, that would be a serious time issue. The protection itself saves me potentially an exponential number of hours trying to recover the organization.

Morphisec reduced our team's workload. Instead of having to go to multiple UIs, or instead of having to do manual investigations, I should say rather. It's at least put stuff to the forefront. More so, after we do the upgrade.

Morphisec has absolutely helped save money on our security stack. The ransomware at the end of the day can cost organizations millions upon millions of dollars. Investing in tools like Morphisec is a great reduction in that cost. If I can spend $10,000 in a year to protect assets that could be ransomed for $20,000,000, that's definitely a bet that one should pursue. Morphisec absolutely it's worth the investment.

It gives us 99% peace of mind in terms of knowing our systems are not being ransomwared. Once we get the upgrade, I'm sure it'll give me much more peace of mind in terms of the antivirus functionalities, knowing that there are no viruses on our machines, as well. But, for now, the only thing I can definitively say is that it gives me confidence that in terms of ransomware attacks, we are not going to be susceptible.

What is most valuable?

The in-memory attack features have been the most valuable. As we transition to a newer version, I'm excited to see the antivirus reporting functionality search come into effect. We are planning on updating and renewing our contract with them.

My company offers online and mobile banking services. Much like your own bank or credit union, the company has apps and a web interface and provides that to various credit unions and banks. As such, we have direct connections into the various financial institutions' banking courses. We see our environment as a prime area, or vector of attack against this course. We've installed Morphisec over two different production data centers, and

it's hooked into our workstations.

Morphisec's new version provides full visibility into security events from Microsoft Defender and Morphisec in one dashboard. The version that we're on right now does not. That's one of the things I'm excited about getting in the upgrade.

This is extremely important to my work. My team is very small. We have four guys across two data centers. Our data centers are through Rackspace, but we are the primary people that interface it. We have a team of four people that own those two data centers and make sure services are functional. We have a small team and having as much information in one basic user interface is critical.

The ease of use is great. It's a basic UI. It clearly tells us how many of our agents are checked in and how many are not. It gives us a very simple UI to be able to see attacks over time-series data, and to be able to drill down very quickly to see which assets or computers are affected. We can see what user was on there and what application was at play. So, in terms of being able to drill down really quickly, they're great.

What needs improvement?

It would be useful for them if they had some kind of network discovery. That kind of functionality I think would give IT administrators a little bit more confidence that they have 100 percent coverage, and it gives them something to audit against. Network discovery would be one area I would definitely suggest that they put some effort into.

For how long have I used the solution?

I have been using Morphisec for around a year and a half.

What do I think about the stability of the solution?

So far it's been extremely stable. Their UI has never crashed once. The agents do check in regularly. Overall, I have not had a single issue with them which is the way it should be.

What do I think about the scalability of the solution?

We have the Ansible playbook for doing the automated install on Linux. At this point, we tell it what server to install to and it does it. In terms of scalability, it's really easy. It's pretty straightforward.

There are four users using this solution including the director of DevOps, the director of Software Engineering, and we have a DevOps Engineer and a Corporate IT Engineer.

The DevOps side folks and the software engineering guy are focused mainly on what our production systems are saying through the UI here, while the corporate IT guy is focusing

much more on the Windows workstations. That said, if we do notice an attack, all four of us come together to analyze what we're seeing there.

We don't require any staff for deployment and maintenance.

At this point, we have to do the installations of any updates to the Morphisec server, or the Morphisec clients. But for that one person is enough to handle that. It's either me or the IT administrator, but it's really not that painful.

The Windows corporate machine is the weakest spot because we don't have automation configuration managers for the Windows side. But, on the Linux side, as far as running updates, it's very straightforward. A couple of commands and run through the Samson playbook and off it all goes.

We do have plans to increase usage. So, as we transitioned to AWS, we're planning on having them with us right off the bat. It's critical to our security portfolio.

How are customer service and technical support?

We contacted technical support a couple of times towards the start, and just had to do with installation. When we first started working with them, it was using a release candidate of their latest stuff. So, it was just a couple of back and forth exchanges, but they were very attentive and forthcoming.

How was the initial setup?

The setup was straightforward. With our Linux environment, our production Linux environments, we were able to deploy using Ansible playbooks to automate, and then on the windows side, they have a number of options available to us. However, because we don't have, on the corporate side, any kind of configuration management tool or whatever, I did have to have my IT admins go in and run a PowerShell script that made the appropriate calls for set up scripts so that they're set up. In terms of our own windows deployment, it was more of a manual process. But, I can tell you from experience with larger organizations and all as well, that the packages that were provided to us could have easily been loaded into a configuration management tool and pushed out much more automatedly.

Once we had things going, I mean, we had everything installed I think, in a total of 10 minutes. That's running these installations concurrently of course, or in parallel. And on the windows side, I'd say over the course of a week, we are able to manually go into all of our workstations and get this installed. Being the COVID environment that it is right now, a lot of our employees are working remotely. A lot of that overhead in that week was simply negotiating when we can actually have the employee make their machine available, remotely.

Our first and foremost deployment was on our Linux front-end servers. We're thinking, get our

production environment for a layer of protection right off the bat. So, we protected our web front end as most attackers would be coming through the front door, essentially, aka those web boxes. So, we figured that if we deployed there first that we'd get a nice level of protection.From there, we did the installations of the windows front end or the endpoints of the window on the corporate side, just to make sure that employees that would be interfacing our source code, or our production environments, would have protection in place, not only to protect their own assets but to also protect the rest of the network that they'd be interfacing with. From there, we went back and upgraded or installed the backend Morphisec agents.

What about the implementation team?

We did our own deployment.

What was our ROI?

If there was a valid attack one could easily say that they could have tried to ransom us 20 million dollars.

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

We pay per year, and per endpoint. So, if it's a Windows server, it has its own skew. Versus, a Linux server has its own skew. Pricing is a little bit different between those.

To cover 100 Windows endpoints we're at $5,699. It all comes with the annual maintenance and support crew.

Which other solutions did I evaluate?

We had looked at a couple of options, but none of them actually seemed to be really what we were looking for because Morphisec handles everything in-memory as things are going. Whereas it seems like a lot of those other tools out there, like Kaspersky and the like seem to be more reactive.

What other advice do I have?

My advice would be to really consider the reality. It's not a question of if you're going to get attacked by ransomware, it's a question of when. And while this seems like something that would be easy to kick down the road, in terms of evaluating the overall battlefield if you will, a ransomware attack will take down your organization. There's no doubt about it.I would advise you to realize that with that inevitability and how much of your environment it can takedown or render useless. This would probably be one of the higher, first choices, and first endeavors you should make as you go into your source of security portfolio.

The biggest takeaway from this that I've had is, never underestimate would-be attackers. You have something on the internet, they're going to go for it. The other lesson I've learned is that sometimes users of computers do weird things, or do things differently than others would normally. That leaves the door open for would-be attackers of having tools like this in place. It will help you avoid headaches down the road.I would rate Morphisec a nine out of ten.