PeerSpot

Case Study

Morphisec Breach Prevention Platform

reviewer1594032

Sr. Security Lead at a healthcare company with 10,001+ employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We purchased Morphisec primarily to help mitigate and protect us against Ryuk ransomware back in December when that was running really rampant. The antivirus that we were using at that point was outdated. We were looking to move to a new vendor, and we needed something as a stopgap to supplement our current antivirus. Morphisec fit that bill perfectly. It had features that our antivirus did not. It had an immediate deployment and immediate return on investment that we just would not be able to get if we were to turn around and try to deploy a full-blown antivirus across the entire environment. Morphisec was quick, simple, and did not conflict with anything that we already had. It also did not cause any additional delays in our virtualized environment, which was a huge concern for our infrastructure team. It just fit perfectly.

We've detected things that our antivirus was not picking up. We had no visibility or control over anything that was running in process memory. Morphisec immediately started blocking things that should not have been running in process memory. It also gave us visibility into the Windows Defender antivirus that we did not have without increasing our Microsoft licensing and gave us some basic control over Defender as well. We previously used McAfee.

How has it helped my organization?

The fact that Morphisec uses deterministic attack prevention that does not require human intervention has affected our security team's operations by making things much simpler. We

don't have to really track down various alerts anymore, they've just stopped. At that point, we can go in and we can clean up whatever needs to be cleaned up. There are some things that Morphisec detects that we can't really remove, it's parts of Internet Explorer, but it's being blocked anyway. So we're happy with that.

It's very important to us that it offers visibility into and control over Windows 10, native device control, disc encryption, and personal firewall. We're actually in the process now of deploying the control over the firewall so that we can consolidate to a single pane of glass for our antivirus and controls. It will help us through leveraging group policy, which can fail, especially if the machine drops off of the domain, we have a significantly larger remote than we did a year ago. We have machines that don't necessarily get the policies they need to get when they need to get them. Morphisec fixed that.

The level of control from Morphisec Guard compared to Windows 10 Native Security tools is a bit more basic than the Windows 10 Native Controls. You basically enable the firewall or you disable it, based on the various profiles. I have not yet seen a way to create exceptions in the firewall or rules and things like that but those can be pushed through group policy, regardless. As long as the firewall is enabled, it's functioning and it's doing better than if there was no policy applied at all.

Morphisec Guard enabled us to see at a glance whether our users have device control and disk encryption enabled properly. It is especially important with our remote workforce. Disc encryption is an absolute must. And the device control, USB devices, is also an absolute must.

It has reduced the amount of time we spend investigating false positives. It reduced our amount of chasing antivirus alerts by about 80% a week.

Our team's overall workload has also been reduced by about 30% on a weekly basis of our workload, we would spend a lot of time tracking alerts.

It has enabled us to take Morphisec and leverage one product where we would have had to have had at least two previously. I don't really have numbers for what that would look like. We didn't really investigate too many other vendors in that space, but it's probably at least 50% savings over what we would have needed. So it has helped us to save money on our security stack.

What needs improvement?

Some of the filters for the console need improvement. There are alerts that show up and just being able to acknowledge that we've seen those and not turn them off, but dismiss them, would be a huge benefit.

For how long have I used the solution?

We've been using Morphisec for about six months now. It is installed on our endpoints and servers. We have a SaaS version of the console.

What do I think about the stability of the solution?

I've had 100% availability anytime I've needed to go look. I have not had any issues in any of our environments with the agents.

What do I think about the scalability of the solution?

Scalability is very easy. We can just call and say that we need more licenses and they give us more licenses and we can push that agent out. It's the same executable file we have on our file shares. We just expand however many we need, to as large as we want to go.We have about 8,000 endpoints, 2,500 servers, and 4,000 virtualized desktops.Our next step would be to purchase the Linux agent and get that on the few Linux servers and appliances that we have.

How are customer service and technical support?

The technical support has been fantastic. Any feature requests I've had, any issues I've run into, which have been very minimal, they've had an immediate response. Turnaround for feature requests is really, really fast. I've seen it within the next update which they do monthly. They provide great technical support.

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

We looked at Bitdefender, Trend Micro, and Microsoft Defender. We are still using Microsoft Defender in conjunction with Morphisec in a small pilot group. We're still evaluating where we want to go for a true antivirus solution. So, we still have a small deployment of Defender.

Deployment was the biggest difference between Morphisec and the other solutions. It was far simpler to deploy Morphisec without having to remove another antivirus, without having to make a large-scale project, or look for compatibility. It works on all supported operating systems. It works in conjunction with other antiviruses. We didn't have to create exceptions and there were no conflicts with the antivirus we were running and Morphisec. So that really helped us make that decision, purchase this, roll it out, and have it supplement our existing technologies. And it gave us an almost immediate return on investment.

How was the initial setup?

The initial setup was very straightforward. We deployed it via group policy. We had it deployed

across the entire environment in about three days.

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

There are no additional costs to standard licensing. We've had full support. I get biweekly calls with my technical account manager and we purchased the licenses for everything we needed for a single cost.

What other advice do I have?

If you have the ability to get Morphisec into their environment, it's going to be a hundred percent return on investment. I would recommend it every time.

If you can, get it and run with it, because it's great. It's been eye-opening, the things that other antiviruses were missing, and we've seen it protect against zero days. We've seen it protect against ransomware that other antiviruses have not even seen.

I would rate Morphisec a ten out of ten.

Read 16 reviews of Morphisec Breach Prevention Platform

See All Reviews