PeerSpot

Case Study

Morphisec Breach Prevention Platform

Dominic Parke

Information Technology Manager at a financial services firm with 11-50 employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

I use it mainly as an additional layer of security since we have quite a lot of servers. I have unblocked a couple of things that got filtered out, and it worked great. We are a small company, not a really large firm.

We were on-prem before, but now we are on a SaaS service that they provide, which is hosted through AWS. This makes it easier for me to access from any location. I can also have Morphisec lock it down to a specific IP for allowing me to get into the system. I would need to be on a computer within the network in order to access the AWS site.

How has it helped my organization?

They provide some information about security events from Microsoft Defender. I know recently when there was that Print Nightmare issue, they did release an email saying, "We are aware of this, and Morphisec is basically on it as well." So, they don't release just random little Microsoft stuff. They would release any major breaches and ransomware. This is where they would notify clients that Morphisec has been updated already to block these things. This is definitely important to us. I am usually up-to-date on all these things. However, if I don't hear from my software vendor, I would be a little bit worried, "Are they blocking it? Is this something that will be blocked? Are they looking into it?" So, it is good to be informed on these things.

Morphisec stops attacks without needing to

know what type of threat it is, just that it is foreign. It is based on injections, so it would know when a software launches. If a software launches and something else also launches, then it would count that as anomalous and block it. Because the software looks at the code, and if it executes something else that is not related, then Morphisec would block it. That is how it works.

Most of the alerts that we have gotten are for legitimate stuff. They have typically been for logins and stuff that users might try to install, e.g., WebEx or some background Google update, so we block them. We have been working internally to block the use of plugins and stuff. It's not that they are fake; they are real notifications. It is just that we have to restrict certain access to certain browsers.

It reduces two alerts every month. It is not so much. We have locked down a lot of things, like our internal group policies. In this way, we don't have to run into any random alerts developed in other people's software for a lot of little things, which we noticed that we can immediately remediate. We have Morphisec doing its real job versus just blocking tiny little programs that don't matter to it. We just have it there as a layer of security on top of our layer of security policies that we already have. I don't think it's going to really catch a lot of stuff, but if something were to happen, it is the backup. That is why we have it.

Every month we get a security report, which tells us, "These are all the things that it scanned, and these are the things that it blocked." 99% of the time, there won't be a lot of stuff, but it gives us an executive report at the end of the month. I usually review it just to make sure that things are okay, e.g., any machines that we might have replaced, need to get rid of, or archive. That is really all I would really look at the security report for. Because if I were to get something like a threat, I won't see it at the end of the month. I see it right away.

Morphisec makes it super easy for our IT team to prevent breaches of critical systems. It is a one-click install, then it takes care of the rest. If we have to evaluate anything, they will notify us. After it has been prevented, we can jump in and release it or create a new rule. Then, if it gets deployed, it gets deployed to all our endpoints. It is really simple for the amount of stuff that they actually do.

What is most valuable?

As far as threat prevention goes, it does great. There have been a couple of preventions that it blocked from browsers and stuff. From time to time, Google may try to install something through the use of a plugin and it blocks that out.

The dashboard is really easy to use. It is not super convoluted, which is great.

Like any other threat prevention platform, this one is mostly specific to memory attacks. That is what I really like about it. I get emails if there are any threats.

What needs improvement?

Right now, it's just their auto-update feature. I know they are currently working on that. When they release a new version of the threat prevention platform, I do have to update that, rolling out to every computer. They have said, "From version 5, you would be able to do an auto-update." While this is very minor, that is the only thing that I would say needs to be upgraded. It would just make life a lot easier for other IT teams. However, I have simplified the process, so all I need to do is just download one file.

For how long have I used the solution?

At my company, we have been using Morphisec for about three years.

I have been using it since last November, which is when I took over from the previous IT manager and was introduced to Morphisec.

What do I think about the stability of the solution?

The stability seems great. There is literally no downtime that I have ever noticed.

There is no maintenance. Morphisec does everything. As long as the endpoint is connected to the dashboard, which is hosted online, then there is nothing that I need to do besides just making sure that it has Internet access on my side, which is how it gets updates.

What do I think about the scalability of the solution?

Scaling is very simple. We just have to add a new computer, then install Morphisec. There is really nothing else to do.

There's only two users who have access to it: a backup admin and me. In the event that something were to happen to me, the backup admin could still get into it, but I am the most active admin on the account. I usually make sure everything is up and the devices are checking in. I just check it from time to time to make sure that all the devices are cleaned up and archived. Since we have been replacing computers, I want to make sure that they are not going to be showing up in our list as offline devices if they were replaced. I just have to remove them and archive it.

How are customer service and technical support?

I contacted their tech support once, when I was deploying the software. I just had to update an IP, and that was it. It was pretty fast. I have a direct contact with their support tech, and even our account manager. I can send issues to them, then they will forward them to their tech support team. They get back to you within an hour, and they are in different time zones. Time-wise, in terms of getting back to you, it is pretty

fast.

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

We previously used Carbon Black. We switched to Morphisec because Carbon Black had a lot of false positives. Based on my knowledge, it was really noisy for stuff that really didn't matter. So, Carbon Black was not the best choice.

How was the initial setup?

When I came in, my company was on an older version, so I had to roll out a newer version. It was literally a migration. We moved from the on-prem server to the cloud. I had to do that from scratch. It really was just Morphisec saying, "This is your new link. There is an installer. You can either install it on all your computers one by one or you can script it out." They provide all the information. Therefore, whenever a computer signs in, it would just install the program and point it to the new server.

The migration took a few seconds. Once I have set it up, all I have to do is wait for people to turn their computers on. Then, I can see them start populating inside of the new dashboard. It was just a waiting game for whenever the CPAs would turn their computers on and log in.

We are in a domain, so all our computers are managed by user accounts. We can set specific rules, e.g., when a user logs in, this happens. So, I set up a rule that would install the new version of Morphisec when a user logs in. Then, I just have to wait for them to log in from wherever they are.

Before, we had to manually install it. However, I am a believer in automating things and doing things a lot faster. So, I was able to roll it out to every computer, even making sure that we had it on all our computers by using their built-in, automatic deployment.

I get emails if I have to set up anything.

What about the implementation team?

I met the guys from the support team and also used a program to deploy it.

Deployment was done in-house. My main thing was that I didn't want to have any computers being missed. It was all done on a one-to-one basis, where the guy would go to every computer and install it. So, installing it would be policy. I know Morphisec would reach out to every single computer, as long as it is joined to the domain. That was my main strategy when rolling it out to everybody. Once it popped up, I made sure the numbers matched up to know whether Morphisec was on every computer on the domain.

What was our ROI?

It is more of a peace of mind. We know that we have an additional layer of security that is

protecting our endpoints, since we are working remotely for certain things. We have the threat prevention platform. 80% of our stuff is based on security materials, because of the data that we work with day-to-day. Having Morphisec made us a little bit more comfortable knowing that our servers are not going to get hacked by any random stuff. However, if it does get hacked, then Morphisec will prevent it.

Morphisec has reduced the amount of time that we spend investigating false positives. It gives me the breakdown of where things originated from. It is easy for me to identify whether it is a false positive or not. Most of the stuff is legitimate. So, I have never had to deal with a false positive block.

The solution has reduced our team's workload. We don't have to really go in, look at stuff, and monitor a dashboard. There is something we set that will notify us. We just have it getting sent to our mailbox. Therefore, if we get an email, we would know (at that stage) that something is going on.

I know my organization was paying a lot more for the previous software that they used through an MSP. It was charged per user and cost quite a bit to use per endpoint.

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

I don't have to purchase any additional licenses, unless I go over. I have a license limit of 80. Whenever we renew our contract, if we have gone over that amount, then we will get billed for that amount.

Our licensing is tied into our contract. Because we have a long-term contract, our pricing is a little bit lower. It is per year, so we don't get charged per endpoint, but we do have a cap. Our cap is 80 endpoints. If we were to go over 80, when we renewed our contract, which is not until three years are over. Then, they would reevaluate, and say, "Well, you have more than 80 devices active right now. This is going to be the price change." They know that we are installing and replacing computers, so the numbers will be all over the place depending on whether you archive or don't archive, which is the reason why we just have to keep up on that stuff.

Which other solutions did I evaluate?

The two main contenders were Carbon Black and Morphisec. We made a decision between those two. We had two trials, where they were trialed them on different machines. Morphisec was more detailed. Morphisec was detecting stuff that was correct versus Carbon Black, which mostly just protecting literally every little thing that you do but not really malicious at all nor causing a memory issue. Morphisec was a little bit more real-time with real stuff versus just a bunch of anomalous stuff. Though, I think

Carbon Black learns as it goes.

Morphisec has helped us to save money on our security stack. Considering other platforms that we have gotten quotes from and other platforms that I have looked into, based on our initial investment into it, it has saved us quite a lot of money on external and internal devices that we would have needed to purchase from other vendors. Right now, it is saving us anywhere between the range of $9,000 to $20,000 per year, because we put a lot of money on security. We house a lot of sensitive information, so we can't afford to go around something. That would put all our clients' information at risk.

We use Morphisec as one of our security artillery platforms. We have other software that we use for security threats, so Morphisec is not the only one. Morphisec is probably around the second stack. We have our main threat prevention software that we rolled out, and after that is Morphisec. After Morphisec is our DNS filtering.

What other advice do I have?

Read the instructions. They literally tell you everything you need to do. Just make sure that you know what Morphisec is before getting into it, because it is not an antivirus. They have a feature that binds with Windows Defender. Windows Defender is an antivirus and Morphisec is more of unified threat prevention for memory attacks. So, you still need to have an antivirus.

Morphisec is a security platform. The things that it does are better for companies who have sensitive information that they don't want to risk getting out. If they have Morphisec, they can feel safe that their stuff is protected.

I would rate it 10 out of 10. It is a great program. We will definitely be renewing it when our renewal period is closer.

Read 15 reviews of Morphisec Breach Prevention Platform

See All Reviews