PeerSpot

# Case Study

## Morphisec Breach Prevention Platform

**Billy Sainz**

IT Operation Manager at Citizens Medical Center

Review by a Real User

Verified by PeerSpot

## What is our primary use case?

For the most part, it's an install-and-forget until it alerts. When it alerts, if a user has a script or something that runs and that tries to alter a process, a message pops up on the user's device and lets the user know, and then it shuts down the process immediately, preventing further infection.

We recently migrated to their cloud platform, which is hosted on AWS. We had on-prem servers but we're decommissioning them in the next week or so.

## How has it helped my organization?

We've seen it work successfully in a couple of areas where it helped us stop a problem before it became a problem. A user clicked on something they shouldn't have clicked on, and it was going to do something. Morphisec will kill Internet Explorer, for instance. That's one of the most popular scenarios.

Morphisec has also reduced the amount of time we spend investigating false positives. Before we got it, it would take a couple of hours whenever we did have an alert, to identify the machine. Now it's really fast and simple because Morphisec provides a full report. We can then jump in there and see exactly what process or script kicked off the alert. We can go directly to it to see if it's legitimate or not. Usually, now, it takes a few minutes.

It helps us save money because of the reduced man-hours when it comes to hunting down something that happens. We also haven't looked at adding any other security software to

our environment because we've been very happy with Morphisec.

It has also reduced workload. When I first started here, we had to remove the computers from a large section of a department to hunt down a problem. Now, it's just automatically shut down and we get an alert and we can go directly to the problem.

## What is most valuable?

The killing of the processes and the alerting are the most valuable features. Where we used to have to wait for either an email to come in and say, "Hey, this has happened," or for a user to call and say, "Hey, this isn't working right," now, the moment it happens, it kicks off an alert to our Microsoft Teams and everybody on my team sees it.

Morphisec also provides full visibility into security events for Microsoft Defender and Morphisec in one dashboard. We purchased that functionality about a year ago. It's important to our organization because we are able to go to one spot to see and follow up on things, and that has been a big help. We're still trying to integrate Windows Defender so that it works with Azure, along with SCCM. If you've worked in SCCM, you know it can be a little bit confusing. When you go into SCCM, you have to do a lot of drill-downs and look for the problem. But in the single pane of glass provided by Morphisec, it's all right there at your fingertips: easy to access and easy to understand. And if you choose to go down further to know everything from the process to the hash behind it, you can.

## What needs improvement?

In the Windows Defender integration, they have put in a report of computers that need Windows Defender updates. If those updates could be kicked off directly from the dashboard, instead of having to go to another system entirely, that would be good. It reports on it, but it doesn't let you take any action from there.

Also, as opposed to when users are on the cloud where it will automatically update the correct agents when they check in, it cannot do that for a VDI client.

## For how long have I used the solution?

I've been using Morphisec for three to four years.

## What do I think about the stability of the solution?

I've had no complaints or concerns about the stability of Morphisec.

## What do I think about the scalability of the solution?

Scalability is not an issue. The way it is designed is that it gets installed and pulls up the necessary plan from the server. Even if you shut down the server, it would stay running to push out more. You just need the licenses for it.

Our entire organization is using it, they just don't realize it. At any one time we have between 500 and 600 people using it. There are only two administrators of the solution right now. Up until now, as one of the administrators, I have done all of the maintenance, but now with the move to the cloud, Morphisec is going to handle that. My role will continue to include ensuring that clients are pushed out to the devices and to follow up on any alerts that come up.

We don't have plans to increase usage. Usage is based on the number of devices we have and we don't intend on expanding that at this time. But the goal is to have it on every desktop that exists in the hospital.

## How are customer service and technical support?

Their support has been good. The only problem is that their support lives in Israel, so the time zones are a bit off, but I've never had any complaint beyond that.

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

We did not have a previous solution for Zero-day protection.

## How was the initial setup?

The initial setup was straightforward and simple. I believe we used a command-line PDQ Deploy and pushed it out across the organization. We were licensed for 1,500 machines in the beginning, 300 servers and 1,200 machines. We didn't go to each individual one. We just pushed it out from one spot to all of them, from a list.

A typical install takes about a minute. It may take three to four minutes if it has to uninstall an old version of Morphisec. Across the organization, it took a day to roll out. We have an inventory of everything we have. Our biggest concern, at the time, was what would happen on servers. For instance, I recently pushed it out to the servers, but we left it in alert-only mode for this new version. That way, if it did alert on anything, it would not kill any necessary processes for the organization.

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

There are two major plans for Windows Defender, and we've chosen plan one. We haven't considered plan two yet because it was

more of a cost-savings when we were looking at Microsoft. Going with Morphisec was more for the Zero-day protection that they offer.

Licenses are per endpoint, and that's true for the cloud version as well. The only difference is that there is a little extra charge for the cloud version.

The only cost, in addition to the standard licensing fees, is if you want the Windows Defender platform, the integration. That one was between $2,000 and $3,000. It's an add-on feature.

## Which other solutions did I evaluate?

The one I remember that we looked at was Carbon Black. The reason we went with Morphisec was that it was well-reviewed at a conference by one of the members of our leadership.

## What other advice do I have?

It's simple, it's easy, and it works. It's a product that actually does what it says it's going to do.

The biggest lesson I've learned from using it is that there are a lot more things in your environment than you want.

Read 16 reviews of Morphisec Breach Prevention Platform

**See All Reviews**