PeerSpot

Case Study

Morphisec Breach Prevention Platform

Barry Bastiaansen

CISO at a logistics company with 1,001-5,000 employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We use it for ransomware protection.

How has it helped my organization?

It is the first product that we are using globally. Beside that, it is a good security solution. It is good for centralizing our IT, the way we think about security, people, and processes.

Morphisec Guard enables us to see at a glance whether our users have device control and disk encryption enabled properly. This is important because we are a global company operating with multiple entities. Previously, we didn't have that visibility. Now, we have visibility so we can pinpoint some locations where there are machines that are not really protected, offline, etc. It gives us visibility, which is good.

It easily prevents breaches of critical systems. It stops them before you detect them, then you don't have to delve into an attack since it was stopped.

What is most valuable?

There is no performance degradation on remote working. We work on PDIs at home without any performance degradation, which is great.

The solution provides full visibility into security events from Microsoft Defender and Morphisec in one dashboard. This is important because it is always good to have less dashboards and panes of glass. If it is all in one, then it is so easy to manage, see, and report on it. This makes the world a much easier place. We use this in our South African entity. However, at our HQ and

other entities, we do not use Windows Defender. We have another antivirus or endpoint security tool, so that is not in one dashboard, though we are probably going to move to Windows Defender. The single dashboard is a factor in our consideration for moving to Microsoft Defender as well as cost.

We use Morphisec Guard for antivirus first. It offers visibility into and control over Windows 10-native device control, disk encryption, and personal firewalls. It is one of the key features for why we are using it since we are all Windows 10 users. Morphisec Guard is very important.

What needs improvement?

We wanted to have multi-tenants in their cloud platform, so every entity can look into their own systems and not see other systems in other entities. I have a beta version on that now. I would like them to incorporate that in the cloud solution.

For how long have I used the solution?

I have been using Morphisec for a year.

What do I think about the stability of the solution?

It has been very stable.

There are two dedicated IT maintenance, and that's it. We also have other people who are now engaged with the implementation of Morphisec. We also train them on administration tasks, e.g., how to look at the dashboard and see if there are any problems.

Not much maintenance is required. Upgrading and pushing the upgrades to the endpoints is done by Morphisec. We only have to look to see if it works on all our machines. If not, then we contact Morphisec.

What do I think about the scalability of the solution?

It is very scalable.

My company has multiple entities, i.e., multiple suborganizations and locations. One entity can be a location or a geographically dispersed organization.

There are about 3,000 end users who have their own endpoints. We have a large number of servers and are a logistics company. Administrators, operations staff, and clerks all do the same types of tasks.

Morphisec is used for every system in the organization. It is on every system, server, and endpoint. Everybody is using it, not actively, but they have it on their machines.

How are customer service and support?

Every week. I speak with someone from Morphisec. If there is something wrong, I can immediately tell them. Then, in the next meeting, they will provide me with a solution.

Their tech support is very good, understanding, and flexible. They know exactly how to work with different people and cultures.

How would you rate customer service and support?

Positive

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

There wasn't a solution like this one, previously. We only had the endpoint security, endpoint protection platforms, EDRs, XDRs, and MDRs, but they don't really have the stuff that Morphisec is doing.

Previously, we didn't investigate false positives. Our company was security immature. If something happened, we didn't investigate it deeply. We just reacted to the fact that something didn't work, then we recovered it and it worked again. Now, we are seeing less false positives using Morphisec.

How was the initial setup?

Our organization is complex and the network is complex, so the initial setup was complex. There was some friction with GPO. We technically implemented it the right way, but it didn't go in automatically. They had to rewrite and recode some parts of it before it could be done automatically.

We are still deploying it. In the end, it has taken more than a year.

We started at HQ and another entity (South Africa), then we wanted to move forward to entities who were in the same network domain as the HQ. We are now in phrase three. It is a global program. We are now implementing, during phase three, in the entities who have their own network structure.

What about the implementation team?

We worked with Morphisec for deployment and implementation. We worked side by side with Morphisec for many of the problems that we encountered during implementation.

What was our ROI?

Morphisec has given our security team's operations peace of mind and more time for patching.

In the end, it saves us money on our security stack because we use a very expensive

endpoint protection platform. We are planning on moving towards Office 365, then having Windows Defender integrated into that so we can save money on our endpoint protection.

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

We are paying per endpoint/machine. We have a two-year contract with Morphisec.

We have had some additional costs because of their cloud. We have needed to make some changes within the cloud environment of the Morphisec tooling, which have added some additional costs.

It does not have multi-tenants. If South Africa wants to show only the machines that they have, they need their own cloud incidence. It is not possible to have that in a single cloud incidence with multiple tenants in it, instead you need to have multiple cloud incidences. Then, if you have that, it will be more expensive. However, they are going to change that, which is good.

Which other solutions did I evaluate?

We evaluated other solutions, but they were quite expensive nor did they do what Morphisec does.

Morphisec Guard has more control than Windows 10-native security tools. For example, with Windows Defender, you can configure it, but you don't have a dashboard. Monitoring with it is a bit difficult. It is better with Morphisec Guard. However, Morphisec combines well with Windows Defender.

What other advice do I have?

I am quite happy with the way they perform, providing us with information, new possibilities, and new features. My advice, "Just do it," if you are looking at implementing this solution.

Morphisec makes use of deterministic attack prevention that doesn’t require investigation of security alerts. If you want, you can deep dive into an attack, but you don't need to. In the future, we may have more security personnel and want to deep dive into an attack to see where it happened, what happened, and learn from it. Then, maybe we can have some other controls in place in other areas of our IP environments. Because of the deep dive and benefit analysis, it is good. However, we don't do that now.

The solution has added some workload because there previously wasn't a security team in place. Now, with the focus on security getting higher, the board of directors wanted to have some more security in place. One of the first tools that we bought was Morphisec, besides endpoint protection, antivirus, and firewalls. Our dedicated security tooling was Morphisec. It added focus in the company on security. Also, some people are busy with security now,

besides their normal jobs.

If we have more machines, then we will definitely increase usage. Also, Linux is now out of scope because they don't have it in their suite yet. If this is added into their suite, then we could have Linux protection as well.

Biggest lesson learnt: It is quite difficult to have an organization with a lot of complexity in their networking as well as differences in the way the network is architectured. It is always more difficult than you think.

I would rate this solution 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)