

Bupa Latin America Fortifies its Security Posture While Optimizing and Enriching Threat Investigations

Seamless Morphisec Automated Moving Target Defense (AMTD) and Microsoft Defender Antivirus for Endpoint integration provides improved visibility and a prevention-first approach to security

Customer

Bupa is an international healthcare company offering health insurance and healthcare services to more than 38 million customers worldwide. While headquartered in the United Kingdom, the company operates in 190 countries across multiple business units. The Bupa Latin America Information Security team provides security services to operations at multiple locations across Latin America.

Challenge

Latin American (LATAM) operations are supported by a single network and shared IT department. Its data center and servers are located in Miami and provide service to all LATAM locations through Microsoft 365. Head of security and risk for Bupa LATAM Alexander Realpe and his team had confidence in the solutions already in place, including Microsoft Defender for Endpoint and Microsoft Defender Antivirus for frontline threat defense, and Tanium to reduce exposure and manage vulnerabilities.

“Morphisec came in, ran a test on one of our computers with all controls in place, and showed how easy it is to create a back door.”

Industry

 Health Insurance

Headquarters

London, United Kingdom

Company size

- 85,000 employees
- 38 million customers worldwide
- \$17B in annual revenue

Challenges

-  Unidentified and unknown security stack gaps
-  Inability to defend against in-memory attacks
-  Technology compatibility and integration

Solution

-  Morphisec AMTD deployed on all endpoints and servers in concert with Microsoft Defender for Endpoint

Results

-  Improved threat protection against complex threats like ransomware and fileless attacks
-  Improved mean time to respond
-  Greater visibility to technology performance
-  Reduction in false positive alert volumes

Challenge cont.

The team frequently applies a variety of tests (including a ransomware simulator) to ensure resiliency against new and emerging threats. Upon learning about Morphisec AMTD, the team commissioned a proof of concept (POC) on a prepared computer loaded with existing security controls.

“We have a very robust set of security controls implemented including Extended Detection and Response (XDR) with Microsoft Defender, and our tests indicated they were producing excellent results,” said Alexander. “But then Morphisec came in, ran a test on one of our computers with all controls in place, and showed how easy it is to create a back door.”

The POC demonstrated how easily the team’s endpoint detection and response solutions could be successfully bypassed. Bupa LATAM Cybersecurity Specialist Erick Vargas ran the POC and observed that “Morphisec proved that it’s able to protect against ransomware and fileless attacks.”

While Microsoft Defender offers comprehensive coverage against a wide range of cyber threats, like many solutions it struggles with the evolving threat complexity like ransomware attacks. For companies relying primarily on Microsoft Defender for endpoint security, the absence of a critical ransomware defense layer means that the organization is not fully equipped to stop advanced ransomware attacks.

Solution

Morphisec now protects all Bupa LATAM endpoints (more than 1,000) and Windows servers (more than 400), in complement to the existing tools and controls already in place. “In the simplest terms, traditional security tools are like doors and locks,” said Alexander. “Morphisec takes protection further. It hides the door, hides the lock, and then moves them all around so threat actors don’t know where to attack.”

The deployment and onboarding process was simple with Erick noting that: “Installing Morphisec was a great experience. We were able to put it in production in a really short time.” Morphisec’s seamless integration with Microsoft Defender yielded immediate insights into technology performance. This identified opportunities for optimization, and allowed the team to configure and fine tune the Microsoft Defender console to monitor and efficiently act on triggers and alerts.

According to Alexander: “The Morphisec and Defender EDR integration helps us to understand which solution reacted to an incident first. It helps us to see what things were caught by Defender versus Morphisec – having that level of visibility provides better security to all our endpoints. Morphisec acts as a fail safe for attacks that bypass the EDR – it’s the last line of defense.”



The Morphisec and Defender EDR integration helps us to understand which solution reacted to an incident first. It helps us to see what things were caught by Defender versus Morphisec – having that level of visibility provides better security to all our endpoints.

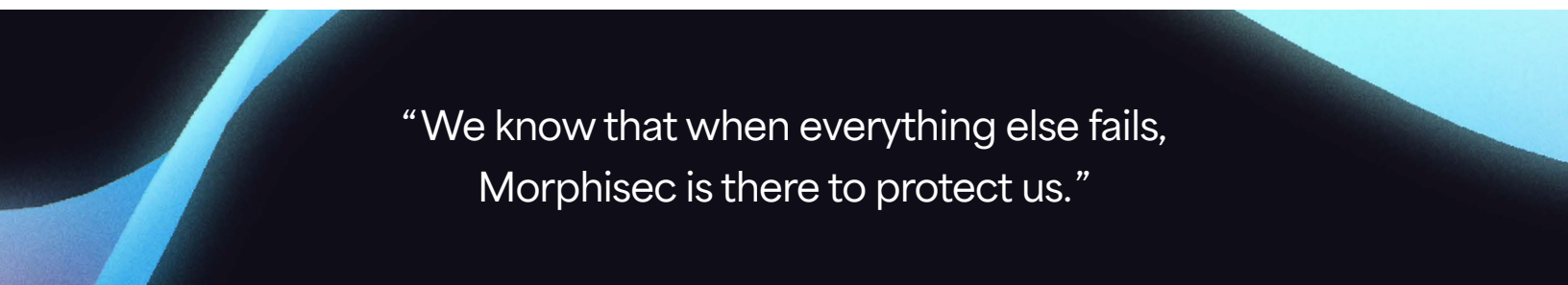
Results

Operationally, Alexander and Erick work with Morphisec's implementation team on an ongoing basis for continued system optimization. Morphisec's incident response team provides invaluable context, flagging and identifying prevented or isolated threats, which helps the Bupa LATAM team improve and optimize mean time to respond. "As a part of the blue team here, I can say first-hand that Morphisec helps us to reduce time gaps that we might have when reacting to an incident," said Erick. "As an Incident Responder, it reduces time to investigate."

Morphisec integrates seamlessly with Microsoft Defender for Endpoint, providing full visibility into the attack chain. High priority alerts are delivered directly into the Microsoft Defender for Endpoint console to assist security analysts with event prioritization.

One such example occurred in late 2023, when Morphisec prevented Mispadu loader (a banking trojan used for monetary and credential theft) that had bypassed Microsoft Defender – Mispadu loader is a highly active and [extremely evasive threat](#). "One cool feature is the fact that Morphisec doesn't rely on normal EDR detection patterns," said Erick. "It doesn't analyze behaviors. Instead, it sees something accessing an application and blocks it right off the bat. Having this effectiveness at the impact phase greatly impacts reaction time."

Morphisec's AMTD stops attacks like Mispadu and other banking trojans and Infostealers across the attack chain, detecting malicious installers, scripts and the payload itself. It prevents such attacks at the earliest stage, preemptively blocking attacks on memory and applications, which effectively remediates the need for response.



"We know that when everything else fails,
Morphisec is there to protect us."

Morphisec AMTD prevents ransomware, as well as supply chain, zero-day, fileless, in-memory attacks and other advanced threats using system polymorphism in memory to hide operating system and application targets from adversaries in an unpredictable manner. The platform has negligible performance impact and does not require additional staffing.

According to Alexander, "Morphisec is set it and forget it. It's that simple. It produces a minimal number of false positives and doesn't impact our business and applications. Deployment, implementation and configuration was a very smooth experience. Morphisec is easy to implement and doesn't require maintenance."

The team appreciates the prevention-first approach that Morphisec AMTD offers with Alexander noting: "Morphisec's unique value is having additional protection against ransomware with decoys deployed - we don't have that with any other tool. If anyone touches those files it generates an alert and Morphisec kicks in. The decoy files and system recovery protection are fantastic."

“Morphisec is the last line of defense.
The amount of detections where Morphisec
has kicked in is really low – and that’s a good thing.
We know that when everything else fails,
Morphisec is there to protect us.”

- Erick Vargas,
IT Security Specialist, Bupa LATAM

*“A layered defense consisting of AMTD obstacles and deceptions
significantly elevates an organization’s security posture.”*

Gartner

Tech Innovators in Automated Moving Target Defense



See Morphisec in action

Stop ransomware with our
Preemptive Cyber Defense Platform

Get a demo

About Morphisec

Founded in 2014, Morphisec, a pioneer in blast radius resiliency, keeps your business safe by intelligently anticipating and neutralizing threats - minimizing the impact and blast radius of cyber incidents and ensuring uninterrupted business operations without the need for constant tech team intervention or impact to performance.

Powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity, Morphisec protects over 7,000 organizations across nine million Windows and Linux endpoints, servers and workloads. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Cipla, Citizens Medical Center, and many more. Learn more at www.morphisec.com

To learn more, visit morphisec.com/demo