

MANUFACTURING CASE STUDY

Morphisec Empowers Global Manufacturer with Better Security at Lower TCO

Customer

Morphisec's customer is a global manufacturer of motion control and power transmission systems for multiple industries through its four main reporting segments and seven operating companies. With numerous brands, 10,000 employees, and over 50 manufacturing facilities.

Challenge

The company's CIO leads the IT team. As the company does not have a formal information security chief, the CIO also serves as the default CISO in the organization. His combined role took on new importance in 2018 as the company completed a major merger.

The merger included the adoption of a Managed Detection and Response (MDR) solution that essentially outsourced the management and reporting of a leading Endpoint Detection and Response (EDR) vendor. Despite the high cost, the combined company decided to continue with the MDR vendor because they lacked the internal resources required to manage the EDR tool themselves.






INDUSTRY

Manufacturing



ENVIRONMENT

- All endpoints running on Windows 10
- 10,000 employees operating at multiple locations worldwide.
- Distributed environment across 50 manufacturing facilities.

CHALLENGES

-  Gaps across security stack.
-  Securing an IT environment that doubled in size after a major merger with another manufacturer.
-  Operating without a CISO.
-  Justifying a significant security spend despite an underwhelming return on investment.
-  Picking up the slack for magic-quadrant EDR vendors who routinely failed to detect or remediate threats.

SOLUTION

-  Utilize an existing solution like Microsoft Defender combined with the preventative cybersecurity of Morphisec.
-  Quarantine and neutralize known and unknown threats alike while the security team redeploys resources where they have the biggest impact.

Challenge cont.

Given how they were using a market-leading endpoint security tool, the team felt confident they were safe from an attack under the watch of the MDR service. That perception all changed when the company experienced an incident where the MDR service failed to show value.

Instead of pinpointing the attack and deploying swift remediation, the attack evaded the MDR vendor's detection, escalated privileges, and turned off the ability to report back subsequent events. As a result, mass confusion ensued among the team. Meanwhile, the MDR solution contributed nothing to remediation efforts and did little more than create reports with inaccurate data.

Frustrated by the experience and realizing they had relied on a false sense of security by one of the top quadrant leaders in EDR, the CIO turned his attention towards finding a solution focused on prevention, where the incident would have automatically locked down the attack before it had a chance to cause damage.

Solution

The CIO chose Morphisec paired with Windows Defender AV to secure the company's critical infrastructure. A long-time Microsoft customer, the CIO started his process to improve security by examining what the company already owned and could quickly deploy.

"The high spend on the EDR product and services required to gain value from it didn't reflect the value provided," said the CIO. "In fact, we weren't using these products on all of our machines, and it was only those machines that were not affected by the incident. We later learned that it was because we took free steps such as proper configuration, hardening, and patch management to ensure to account for the fact that those machines weren't being monitored by the MSSP. It turns out, that was giving us a false sense of security."

They already had Windows 10 on their machines, which made it easy to transition to Windows Defender AV. After seeing a demo at a tradeshow of Morphisec's platform, the CIO decided to deploy the Morphisec agent on top of Windows Defender AV to increase visibility into Defender alerts and gain the prevention capabilities of the Morphisec agent.

"Dollars spent doesn't correlate to security value. We spent a lot of money on our MDR provider, and yet we still were breached and had to do a lot of work ourselves. After bringing on Morphisec, we were able to protect twice the endpoints at half the cost of our MDR platform."

Results

“Dollars spent doesn’t correlate to security value,” the CIO said. “We spent a lot of money on our MDR provider, and yet we still were breached and had to do a lot of work ourselves. After bringing on Morphisec, we were able to protect twice the endpoints at half the cost of our MDR platform.”

With the Morphisec agent added to Windows Defender AV, the CIO also gained full visibility throughout the entire attack chain.

This allowed the company to secure all its endpoints and servers without needing to hire a chief security officer or any dedicated security resources to manage systems that are incredibly easy to misconfigure.

Thanks to the preventative capabilities of the Morphisec agent, the CIO and his team adopted an entirely new security posture. “We don’t spend much time on detection and response because we don’t need to.” Instead, they focus on training people, improving processes, and planning for emerging threats: high-level initiatives they have the resources for now that Morphisec blocks attacks they used to detect, and prevents damage they used to remediate.

*“A layered defense consisting of AMTD obstacles and deceptions significantly elevates an organization’s security posture”
Get your complimentary report [here](#).*

Gartner

Tech Innovators in Automated Moving Target Defense

About Morphisec

Morphisec provides prevention-first security against the most advanced threats to stop the attacks that others don’t, from endpoint to the cloud. Morphisec’s software is powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity. AMTD stops ransomware, supply chain attacks, zero-days, and other advanced attacks. AMTD provides an ultra-lightweight, Defense-in-Depth security layer to augment solutions like NGAV, EPP and EDR/XDR. We close their runtime memory security gap against the undetectable cyberattacks with no performance impact or extra staff needed. Over 5,000 organizations trust Morphisec to protect nine million Windows and Linux servers, workloads, and endpoints. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Covenant Health, Citizens Medical Center, and many more.

Schedule a demo now: morphisec.com/demo