

MANUFACTURING CASE STUDY

Morphisec Protects Fortune 500 Manufacturer From Advanced Threats

Customer

A global, Fortune 500 heavy equipment manufacturer which also has a financial services arm that conducts full service leasing operations for its equipment.

Challenge

The company had a well-developed network and endpoint protection structure in place, but still was concerned about threats from advanced attacks that could bypass its security systems.

Their CISO, a prominent thought leader in the security space, did not believe in just addressing the current security situation, but anticipating the future. He wanted to invest in a solution that would prevent emerging and as yet unknown threats, including APTs, zero-days and fileless malware. With a highly technical background, he sought new approaches which could prove their effectiveness in the field, not just on paper. The solution also needed to work with their existing security tools, including integrating with their SIEM system.

The company security team is strong but lean – any solution that required additional staff or introduced system complexity was out of the question. Alert fatigue and false positives were a particular concern. The team also couldn't afford to waste time on configuration and deployment, both from a resource point of view and the need to limit the company's security exposure fast.

The company has won numerous awards for efficient practices and operational excellence. It is of high priority that nothing disrupts work, introduces system latency or clogs up endpoints.




INDUSTRY

Manufacturing




ENVIRONMENT

- 18,000 endpoints
- Multiple locations worldwide
- Morphisec management console residing on two sites
- Requirement to comply with European privacy regulations

CHALLENGES

-  Exposure to advanced threats that can bypass standard security solutions
-  Integration into existing security environment
-  Reinforce lean security strategy

SOLUTION

-  Build an effective, cost-efficient prevention stack with signature-based AV for known malware and Morphisec for advanced threats
-  Stop attacks before the kill chain starts, with no false telemetry, reducing time spent on detection and remediation
-  Focus on early prevention to cut detection and response times and risk to operations

“Morphisec gives me the effectiveness against advanced attacks and the operational simplicity that are imperatives to safeguarding our company and customers and running a lean, efficient enterprise.”

— CISO at a Fortune 500 US Manufacturing Company

Solution

The company conducted a rigorous test of several products, including an extensive pilot of Morphisec Endpoint Threat Prevention. Morphisec’s ease of deployment, operational simplicity and minimal CPU usage immediately won points. But the solution really proved itself when it prevented a live attack during the pilot period.

With this clear demonstration of Morphisec’s effectiveness and efficiency, the company CISO selected Morphisec to be their new advanced threat layer and began deployment across the enterprise.

His choice was justified sooner than expected. About 25% into initial deployment, Morphisec blocked several advanced threats, including a virulent Kovter variant that injects malicious code into PowerShell scripts and registry keys to evade detection and analysis. These sophisticated attacks went undetected by the company’s other solutions and could have caused considerable damage had Morphisec not prevented them.

Realizing the company’s exposure, the CISO instructed his team to accelerate deployment across the enterprise. Full rollout to all 18,000 endpoints took a couple of weeks, with no disruption to employees or company operations in any of its various locations.

“I was amazed that we could roll out an entire new crucial defense layer that quickly and smoothly,” says the company CISO. “I credit not just the ingenious simplicity of the software but also the high level of cooperation between my teams and Morphisec support and engineers.”

Results

With the entire enterprise now protected by Morphisec, the company CISO and board are breathing much easier. Since the deployment, numerous attacks have been prevented. The security team appreciates its ease of use and that they don't have to spend time updating rules and investigating false alerts.

For the CISO, Morphisec's minimal administration and resource demands have been crucial to the continued success of his lean security strategy.

"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