

MANUFACTURING CASE STUDY

Morphisec Lets Radwell International Focus on Its Customers



Customer Profile

Radwell is a privately owned enterprise and the world's largest provider of new and used surplus, industrial electrical and electronic control equipment. Radwell maintains specialized industrial electronic equipment to many manufacturing companies including automakers, chemical plants, food processing facilities, municipalities, government agencies, power plants, exporters, plastic molding, steel plants and a long list of other business sectors.



Challenge

John Janthor, vice president of information technology at Radwell, said that the company paid close attention to the major cyberattacks that made the news. The company's founders and board fixated on the risk of a breach by fileless and evasive threats, and turned security into a key component of their business continuity planning and risk management process.

Janthor also noted that Radwell, as a global company, needed to comply with GDPR and PCI standards when it came to data security and privacy. These requirements forced Radwell to think closely about their markets and how to protect customers under a magnifying glass. Combined with their concerns about fileless threats, these privacy regulations created a strong need for Radwell to seek out a performant cybersecurity solution.

"For us security is all about business continuity, and our risk assessment showed there was a hole in our security posture in protecting against unknown attacks going after memory and using fileless techniques," Janthor said. "We also needed to have immediate visibility and streamlined actions."

Ultimately, Janthor said, Radwell wanted to be proactive with their cyber defense to mitigate the risk of fileless, evasive threats. They had evaluated the cost of downtime and irreparable damage from a cyberattack, and realized that those costs dwarfed the cost of any cybersecurity solution.

Solution

Radwell had recently adopted Microsoft's holistic security strategy, and sought a solution that had tight integration with their existing Microsoft Defender for Endpoint license. As part of the evaluation process, Janthor said they tested all the major endpoint protection vendors for protection against fileless attacks, evasive malware, and in-memory exploits.

INDUSTRY

Manufacturing

ENVIRONMENT

- 900 employees across North America and Europe
- Microsoft Defender for Endpoint user for EDR
- Windows 10 on endpoints

CHALLENGES

- Prevent fileless attacks, evasive malware, and in-memory exploits.
- Zero tolerance for breaches or disruptions.
- Proactive strategy on mitigating cyber attack risk.

SOLUTION

- Integrated Morphisec and Microsoft Defender for Endpoint
- Proactive approach to cybersecurity with complete visibility and insight via Microsoft Defender for Endpoint Security Center.



“Security is a journey for us that is never done. The moment you rest on your laurels, the bad guys are looking for new innovative ways to get around what you’ve implemented. Plugging in Morphisec to Microsoft Defender for Endpoint was an important milestone in our security journey. For the first time, we have high confidence that extreme advanced threats in zero days are going to be prevented by Morphisec, and flow seamless into Defender for Endpoint for full visibility, reporting and in remediation steps.”

— John Janthor, VP of Information Technology, Radwell International

Morphisec was chosen following the rigorous evaluation period for its facility at blocking the threats Radwell was concerned about, as well as its tight integration with Microsoft. Janthor said that Morphisec integrated so well that it appeared like they were using one solution from a single vendor.

“We became really focused on stopping a sophisticated in-memory attacks and fileless attacks before the actual crime happens,” Janthor said. “Only Morphisec was able to prevent the unknown in-memory attacks that we see becoming more prevalent. The fact that Morphisec was partnering with Microsoft and integrated into Microsoft Defender for Endpoint made our decision even easier. Now we could report on our risk score in preventing unknowns, make decisions faster and do so through a single dashboard from Microsoft Defender for Endpoint. For us it was best of both world and felt like it was designed and implemented as a single package.”

Results

With Morphisec and Microsoft Defender for Endpoint, Radwell now has protection against unknown fileless attacks and in-memory threats as well as full visibility within the Microsoft Defender for Endpoint Security Center. Morphisec’s zero trust runtime solution, powered by moving target defense, makes the memory environment unknown to attackers and quickly surfaces threats in the Microsoft Defender for Endpoint Security Center. This enables analysts to quickly identify and remediate threats that Morphisec has blocked.

“Security is a journey for us that is never done,” Janthor said. “The moment you rest on your laurels, the bad guys are looking for new innovative ways to get around what you’ve implemented. Plugging in Morphisec to Microsoft Defender for Endpoint was an important milestone in our security journey. For the first time, we have high confidence that extreme advanced threats in zero days are going to be prevented by Morphisec, and flow seamless into Defender for Endpoint for full visibility, reporting and in remediation steps.”

Because attacks are confirmed prevented by Morphisec, Radwell can now rest assured that their business continues uninterrupted. Janthor said the Radwell security team further gained the ability to focus on the highest-level threats through Morphisec’s seamless integration with Microsoft Defender for Endpoint.

Schedule a demo now: demo@morphisec.com



www.morphisec.com

