MORPHISEC

YASKAWA

INDUSTRIAL ROBOTICS CASE STUDY

Yaskawa Motoman Takes On Advanced Threats

Customer

Yaskawa Motoman, a leading industrial robotics, provides automation products and solutions for virtually every industry and robotic application. The company is known worldwide for its high quality, innovative robotic solutions. Motoman's reputation for innovation extends to its IT and cybersecurity, with a team known for creative thinking, a best-of-breed approach, and early adoption of new technologies.

Challenge

Motoman employs an agile development environment where more than 90 percent of the users are engineers and scientists with administrative rights on their PCs. In order to meet business requirements with tight deadlines, they need to download and install software and utilities and it was important to enable individual flexibility without compromising security. At the same time, the company was confronted with increasingly more sophisticated targeted attacks capable of bypassing its antivirus, putting intellectual property at risk, creating the potential for business disruption, and forcing the IT team to commit resources responding to incidents.

Jeff Magnuson, Senior IT Architect at Yaskawa Motoman, led the search for a security solution that could stop these attacks but did not impede end users in their work. "If security interfered with the applications our developers need or the installation of new systems then we'd be trading one problem for another."

Magnuson also didn't want to waste IT resources on false alerts, remediation tasks or an endless cycle of case management.

INDUSTRY

Industrial Robotic Automation

ENVIRONMENT

- Sites across United States, Canada, Mexico and Brazil
- Agile development environment with complex applications
- Most users are engineers and scientists with administrator access to download apps or utilities as needed

CHALLENGES

- Protect without restricting user access privileges
- Decided to replace AV with Malwarebytes but still needed protection against advanced threats, particularly fileless in-memory attacks
- Solution must use minimal CPU resources and operate invisibly to the end user

SOLUTION

- Strengthen endpoint stack with Morphisec for advanced threat prevention
- Protect the enterprise from both commodity threats and advanced, targeted attacks without creating overhead or interfering with IT automation

> “ Morphisec simplifies and automates prevention. It prevents advanced attacks that would otherwise breach us, takes essentially no care and feeding and stays out of the way of my end users.”
>
> — Jeff Magnuson, Senior IT Architect, Yaskawa Motoman

Solution

Magnuson assessed the risk from the growth in fileless and other stealth attack techniques and saw they left Motoman increasingly exposed. He needed to combat attacks on two fronts: conventional malware plus in-memory attacks designed to evade AV and malware detection.

After investigating numerous solutions, Magnuson decided a best-of-breed security stack was the best protection against the advanced attack technology he was facing. It would give Motoman better security performance than an all-in-one platform and simplify security operations in the bargain. He chose Malwarebytes for known malware but this still left Motoman exposed to unknown threats and evasive, in-memory attacks that most tools are blind to. Many advanced threat products on the market proved unsuitable for Motoman’s agile development environment – they slowed down the endpoint, interfered with users and were hard to manage. On top of that, most were simply not effective enough against in-memory attacks. Then Magnuson found Morphisec Endpoint Threat Prevention.

“Morphisec simplifies and automates prevention. It prevents advanced attacks that would otherwise breach us, takes essentially no care and feeding, and stays out of the way of my end users. It is exactly what we need for protection from advanced threats and in-memory attacks,” says Magnuson. “We especially appreciate the fact that it prevents new attacks with no updates.”

Once the choice was made, implementation went quickly and coverage across the enterprise was immediate. All prevention functionality kicked in the moment of installation, with no configuring, learning, database connections, tuning or rule setting.

Results

Right away, Morphisec stopped targeted, advanced attacks that bypassed Motoman's other solutions. The company is now protected from both conventional threats and advanced attacks like fileless and browser-based attacks, evasive malware, and malicious code embedded in legitimate applications. And by eliminating process steps like managing alerts, setting up rules, and remediating compromised systems, it allows Magnuson's team to focus on higher value IT and security activity.

"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