RunSafe Enhances Security and ROI for an Industrial Automation Leader Deploying HMI Products

Overview

A leader in industrial automation deployed around the world sought to transition its Human-Machine Interface (HMI) products to embedded Linux to improve security. By partnering with RunSafe, they aimed to reduce the attack surface of 850 identified vulnerabilities without altering product functionality.

Since HMI products are the most commonly attacked OT network devices and because the company's new models contained a new operating system, RunSafe deployed code protection to dramatically reduce the attack surface by 70% protecting software in very difficult to update facilities within critical infrastructure. This transition not only provided future-proofing but also increased the resilience of customer infrastructure.

Challenge

This industrial automation leader had significant security challenges with their existing HMI products. The transition to embedded Linux revealed many vulnerabilities that needed addressing. It was crucial to enhance security without changing the functionality of the HMI products. Ensuring long-term security and resilience against emerging threats was paramount, as was achieving significant ROI and operational savings while improving security.

Industry

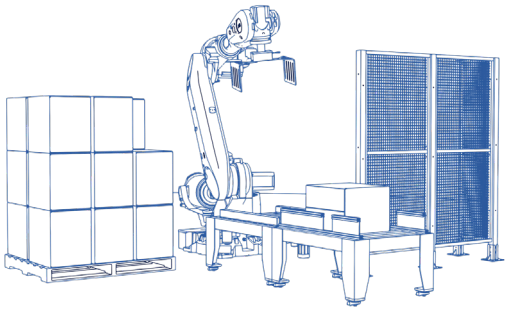
Industrial Automation

Key features

- Automated mitigation
- Reduced attack surface
- Seamless integration with an embedded Linux environment
- Future proof from zero day

Solution

This industrial automation leader integrated RunSafe's software into their HMI products built on embedded Linux. RunSafe automated the hardening process, mitigating identified vulnerabilities and significantly reducing the attack surface without altering product functionality. This seamless integration provided robust protection and future-proofing against zero-day vulnerabilities.



About the Customer

This company is a global leader in energy management and automation, offering solutions that drive digital transformation in homes, buildings, data centers, infrastructure, and industries. With a focus on sustainability and efficiency, they empower customers to make the most of their energy and resources.

RUNSAFE SECURITY

About RunSafe

RunSafe Security is the pioneer of a unique cyberhardening technology designed to disrupt attackers and protect vulnerable embedded systems and devices. With the ability to make each device functionally identical but logically unique, RunSafe Security renders threats inert by eliminating attack vectors, significantly reducing vulnerabilities, and denying malware the uniformity required to propagate. Based in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the Industrial Internet of Things (IIoT), critical infrastructure, automotive, and national security industries.

Results

The implementation of RunSafe yielded remarkable outcomes for:

Enhanced security:

Automated mitigation of 850 vulnerabilities significantly improved the security of HMI products.

Operational savings:

Calculated significant ROI and operational savings.

Resilience and future-proofing:

Increased resilience of customer infrastructure with robust protection against zero-day vulnerabilities.

Preserved functionality:

Security enhancements were applied without any change in product functionality, ensuring seamless operation.