Aerospace & Defense Leader Ensures Mission Success with RunSafe's Cyberhardening Technology

Overview

A leader in the Aerospace and Defense industry was looking for a solution to protect critical systems without risking mission assurance or requiring extensive developer resources. The company integrated RunSafe's technology, increasing visibility into vulnerabilities, eliminating the need for manual SBOM creation, and protecting legacy apps without having to rewrite a single line of code.

Challenge

The Aerospace and Defense provider approached RunSafe with three key challenges:

- **Legacy Applications Exposed to Cyberattack:** With dozens of legacy applications running on major customer programs, there was a real risk for a cyberattack to cripple critical systems and undermine mission success.
- **Complex Software Supply Chain:** A complex software supply chain made it difficult for the company to understand the software composition of its programs, limiting visibility into vulnerabilities and the ability to take steps to remediate them.
- **Risking Mission Assurance:** The company needed to integrate a security solution that would meet their needs while preserving their ability to execute on mission.

Industry

Aerospace and Defense

Key features

- **Automation:** Automated cyberhardening and SBOM generation across legacy apps
- **Visibility:** Increased visibility into vulnerabilities to boost overall security posture
- **Integration:** Seamless integration into existing software development infrastructure

Solution

The Aerospace and Defense provider adopted the RunSafe Security Platform to address their challenges. Using Identify, RunSafe's C/C++ SBOM generator, the company eliminated the need for development teams to manually create SBOMs. Instead, the company was able to generate SBOMs automatically across multiple code repositories within the software supply chain.

Additionally, by implementing RunSafe's Protect solution, the company automated security protections for their embedded systems, including legacy apps written in C/C++, without having to consume developer resources to rewrite code and without risking mission assurance. RunSafe's patented technology protects systems from build time to runtime, reducing risk and the attack surface.

About the Customer

The company is a leader in aerospace and defense, providing cutting-edge solutions to the market with a focus on creating advanced technology that keeps companies ahead of emerging threats.

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

After implementing the RunSafe Security Platform, the Aerospace and Defense leader preserved their ability to execute on mission while enhancing their overall security posture and protecting legacy apps without rewriting code.

Increased Resilience:

RunSafe's runtime memory protections enhanced the resilience of critical systems, shielding from both known and unknown memory-based vulnerabilities.

Improved Visibility:

C/C++ SBOM generation saved developer resources and provided complete visibility into software components, allowing for vulnerability identification and remediation.

Operational Efficiency:

The seamless integration of RunSafe into existing toolchains allowed for continuous delivery of cyberhardened software without disrupting development workflows.