Vertiv Enhances Critical Infrastructure Security for Embedded Systems with RunSafe Integration

> “From our perspective, adding RunSafe to Avocent Core Insight means we have more opportunity to shrink the attack surface and reduce overall risks for our customers since security is now already built into our product.”
>
> **- Donnie Sturgeon, Senior Director of Avocent Business and Product Development**

Overview

Vertiv, a leading global provider of digital infrastructure and continuity solutions, turned to RunSafe to secure the embedded management system code produced by its Avocent Core Insight (ACI) family of embedded Linux packages. By centralizing vulnerability identification and applying code protections across its GitLab environment, Vertiv aimed to increase the ROI on their GitLab investment and differentiate their offerings by protecting the firmware and SDKs shipped to computer manufacturers.

Industry

Critical Infrastructure

Key features

- Automated mitigation
- Reduced attack surfaces
- Seamless integration with CI/CD pipelines
- Proactive protection against zero day threats

Challenge

Vertiv faced significant security challenges. OpenBMC, the base layer of open source code for ACI, is a major target for cyber attacks. They also had an urgent need to secure embedded management system code without adding significant overhead or disrupting workflows. Deputy CISO Jeremy Block aimed to standardize security across development teams using GitLab and RunSafe.

Solution

Vertiv integrated RunSafe's software as a layer into their Yocto builds, ensuring every module built with ACI is self-protected against memory-based attacks. RunSafe's integration into Vertiv's GitLab environment automated the identification and mitigation of vulnerabilities, enhancing security without impacting performance or functionality. This comprehensive approach protected the firmware and SDKs shipped to computer manufacturers, centralizing vulnerability management and applying robust code protections.

VERTIV™

About Vertiv

Vertiv is a global leader in designing, building, and servicing critical infrastructure that enables vital applications for data centers, communication networks, and commercial and industrial facilities. With a focus on innovation and reliability, Vertiv provides comprehensive solutions to ensure the continuous operation and optimization of essential digital infrastructure.

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

By adopting RunSafe, Vertiv achieved remarkable results:

- **Enhanced security:** Automated mitigation and reduced attack surfaces significantly improved the security of Vertiv's embedded systems.
- **Increased ROI:** By maximizing their GitLab investment, Vertiv enhanced security with minimal additional resource allocation.
- **Market differentiation:** Protecting firmware and SDKs differentiated Vertiv's products, offering customers enhanced security built into their systems.
- **Operational efficiency:** Seamless integration allowed security teams to focus on strategic initiatives, optimizing resource use.
- **Long-term protection:** RunSafe's protection against zero-day vulnerabilities provided robust, future-proof security.

Vertiv's experience with RunSafe's software highlights how automated, integrated security solutions can enhance software protection, improve ROI, and maintain seamless development workflows, safeguarding critical digital infrastructure against emerging threats.