

Ship Secure Embedded Devices Faster with RunSafe Security

Speed up software delivery with RunSafe Security. Integrate SBOM creation into your CI/CD pipeline, identify vulnerabilities, and protect embedded software without interrupting your development workflows.

THE CHALLENGES DEVELOPERS FACE

Developers are increasingly bogged down by:

- **Time-consuming security patches and fixes** that take attention away from new releases
- **Legacy device maintenance**, which is labor-intensive and resource-heavy
- **Compliance requirements for SBOM** generation and maintenance

RunSafe Security directly addresses these challenges with code protections that reduce the need for patching and tools that provide complete visibility into your software components, dependencies, and vulnerabilities.

THE RUNSAFE SOLUTION

RunSafe Security mitigates cyber exploits through Load-time Function Randomization (LFR), preventing attackers from exploiting both known and unknown vulnerabilities in embedded software. LFR is embedded directly into your build process to protect software at runtime, even before a patch or fix is available.



50%

increase in automated mitigation with RunSafe applied, reducing the need for patches and fixes

Additionally, RunSafe provides build-time SBOM generation to identify vulnerabilities early in the software lifecycle and to meet compliance standards.

BENEFITS

- **Deliver secure releases on time** without draining developer resources
- **Reduce the time you spend on vulnerability mitigation by 50%**
- **Protect code at runtime** with minimal performance impact
- **Integrate into your existing CI/CD environment** in as little as 5 minutes

SMOOTH OUT YOUR PATCHING SCHEDULE

No more rushing to patch vulnerabilities. With RunSafe's automated code protection, embedded software can **defend itself while waiting for updates**.



AUTOMATE SBOM GENERATION & IDENTIFY VULNERABILITIES

Get complete visibility into your software components with build-time SBOMs. Upload manually or connect to GitLab/GitHub to **generate an SBOM for every commit**.



DEFEND AGAINST 70% OF CYBER EXPLOITS AT DEPLOYMENT

By integrating our memory protection technology into every software release prior to deployment, RunSafe can **prevent up to at least 70% of the exploits** being used in cyber kill chains today.



INTEGRATE SEAMLESSLY WITH LITTLE OVERHEAD

Integrate with your CI/CD pipeline for continuous security throughout development. **RunSafe adds minimal performance overhead** to successfully run on resource-constrained systems.



ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: RunSafeSecurity.com.