

RunSafe Moves to Lead Operational Software Assurance as U.S. Elevates Cybersecurity Across National Security

New research and White House strategy spotlight the need to protect fielded software in defense and critical infrastructure from supply chain through runtime.

MCLEAN, VA, UNITED STATES, September 8, 2026 /EINPresswire.com/ -- [RunSafe Security](#) today announced its strategy to lead the emerging Operational Software Assurance (OSA) market, a new cybersecurity category focused on protecting the fielded software that powers U.S. defense, critical infrastructure, and other mission-critical systems throughout their operational lifecycle.

The move comes as the White House's new National Security Science and Technology Strategy (NSSTS) elevates cybersecurity across U.S. technology and homeland defense priorities, and new independent research identifies a critical gap in protecting software already operating across defense and critical infrastructure.

Research from former Gartner analysts Brad LaPorte and Rob Smith of Lionfish Tech Advisors defines Operational Software Assurance as the next evolution of software security, extending assurance beyond development and the software supply chain to software already deployed in weapons systems, critical infrastructure, vehicles, medical devices, and industrial equipment.

The report, *The Call for a Digital Golden Dome*, defines OSA around three capabilities: Identify, Protect, and Comply. RunSafe delivers those capabilities through a platform that:

- Identifies what is present in compiled software and firmware, including vulnerabilities, dependencies, and whether vulnerabilities are reachable.
- Protects deployed binaries and firmware against exploitation through runtime protection without requiring source code changes or waiting for a patch.
- Demonstrates compliance through continuous assurance evidence and artifacts supporting cybersecurity, regulatory, and mission requirements.

"Cybersecurity has spent decades getting better at finding vulnerabilities, but finding more vulnerabilities doesn't protect the software already operating our aircraft, weapons platforms, energy systems, factories, and other critical infrastructure," said Joseph M. Saunders, Founder and CEO of RunSafe Security. "AI is making that gap impossible to ignore. Operational Software Assurance is about knowing what's actually in your software, protecting it while it runs, and

continuously proving that protection."

A National Security Strategy Built on Cybersecurity

The White House's NSSTS, released August 18, reinforces the timing of the emerging OSA market. The strategy places the maintenance of a next-generation missile defense shield under a Golden Dome for America alongside the protection of critical data, networks, assets, and infrastructure against cyberattacks and espionage as priorities for countering strategic threats to the homeland.

The strategy also maps critical and emerging technologies against priority national security needs. Information security and cybersecurity span every mission represented, including battlefield advantage, undersea superiority, national-security AI and autonomy, border security, nuclear deterrence and missile defense, cyber defense, and biological weapons defense.

Those missions increasingly depend on software that may remain operational for years or decades.

"The White House strategy makes clear that cybersecurity isn't a separate technology problem. Instead, it underpins nearly every major national security mission," Saunders said. "Golden Dome itself will ultimately depend on software. So will autonomous systems, C5ISR, undersea platforms, critical infrastructure, and advanced weapons. Protecting those missions means protecting the software they depend on, including software already in the field."

AI Is Changing the Economics of Software Security

Artificial intelligence is making that challenge more urgent. AI-assisted systems can analyze enormous code bases and discover vulnerabilities at machine speed, while attackers can use the same capabilities to accelerate exploit development. Remediation of fielded software, however, remains constrained by testing, certification, operational availability, and lengthy patch cycles.

The result is a widening gap between machine-speed discovery and human-speed remediation.

"While AI didn't create the problem of vulnerable legacy software, it did change the economics of attacking it," said Shane Fry, CTO of RunSafe Security. "We cannot assume defenders will find, patch, test, and recertify every vulnerability before an adversary can exploit it. For software that must remain operational, we need defenses that prevent attackers from exploiting software faster than AI can discover and exploit them."

Building a Digital Golden Dome for Software

The Lionfish report describes that additional layer as Embedded Runtime Security, the Protect component of Operational Software Assurance.

Its Digital Golden Dome framework applies a missile-defense principle to software: rather than assuming every threat can be eliminated beforehand, prevent threats that reach their target from succeeding. For deployed software, that means making successful exploitation materially more difficult without waiting for the underlying vulnerability to be eliminated.

This approach complements secure development, vulnerability management, SBOMs, Zero Trust, and the transition toward memory-safe languages by addressing the enormous installed base of compiled software that cannot immediately be rewritten or patched.

RunSafe's runtime protection technology originated in DARPA-funded research and protects compiled binaries and firmware without requiring source code changes. RunSafe technology is available through the Department of War's Iron Bank and is used across defense, aerospace, and critical infrastructure environments.

Independent Research Points to a Growing Market

The Lionfish research maps more than 140 funded U.S. defense programs across 19 DoW components whose fielded software falls within the scope of runtime protection, representing approximately \$87 billion in FY2026 procurement and \$159.5 billion in the FY2027 request. The researchers characterize the figures as measures of software exposure, not estimates of serviceable market revenue.

RunSafe sees OSA extending beyond defense into industrial control systems, energy, automotive, medical devices, telecom, rail, robotics, and space, sectors where software is long-lived, difficult to patch, and increasingly tied to physical and mission outcomes.

"We need to build new software securely, but we also need to protect what is already deployed," Saunders said. "Operational Software Assurance closes that gap. That's the market RunSafe was built to address."

Learn more about RunSafe's approach to Operational Software Assurance [here](#).

About the Research

The Call for a Digital Golden Dome was independently initiated and funded by Brad LaPorte and Rob Smith of Lionfish Tech Advisors. RunSafe did not commission or fund the research. LaPorte serves as a board advisor to RunSafe, and RunSafe contributed technical data, research assistance, and peer review. RunSafe held no approval rights over the report's category definition, economic model, or recommendations.

About RunSafe Security

RunSafe Security is pioneering Operational Software Assurance for software powering critical infrastructure, defense systems, and connected devices. RunSafe helps organizations identify software risk, protect deployed code from exploitation, and comply with cybersecurity and regulatory requirements across the operational lifecycle.

Kari Walker
RedIron PR
+1 703-928-9996
kari@redironpr.com

This press release can be viewed online at: <https://www.einpresswire.com/article/940429153>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.