RunSafe Security's Doug Britton to Present on AI-Accelerated Memory Exploits at Emerging Technologies for Defense

The session will show how AI-accelerated exploit development has outpaced patching and how Load-time Function Randomization takes memory attacks off the table.

WASHINGTON, DC, UNITED STATES, September 1, 2026 /EINPresswire.com/ -- RunSafe Security, the pioneer in embedded runtime security, today announced that EVP and Chief Strategy Officer Doug Britton will present a technical session at the Emerging Technologies for Defense Conference and Exhibition on how defense programs can eliminate memory exploits at a time when AI is finding and weaponizing software flaws faster than any patch pipeline can respond.

Doug will lead a session that examines why memory corruption vulnerabilities remain one of the most dangerous and persistent attack vectors in modern defense software and why the rise of AI-enabled exploit generation makes the problem far more urgent. Doug will show why traditional, reactive cybersecurity cannot keep pace with machine-speed attacks, and how defense programs can eliminate the exploit rather than endlessly chase vulnerabilities after disclosure.

What / Scheduled Sessions:

- Technical Session: “Taking Memory Exploits Off the Table in the Age of AI-Accelerated Cyber Warfare”

- Context: Doug will discuss how traditional cybersecurity approaches remain overwhelmingly reactive (discover, patch, deploy, repeat). For mission-critical defense systems operating across distributed, contested, and disconnected environments, patching alone cannot keep pace with AI-driven attack velocity.

Who:
- Doug Britton, EVP and Chief Strategy Officer, RunSafe Security

- Federal and defense industry leaders and program stakeholders

When: September 8-10, 2026

Where: Walter E. Washington Convention Center, 801 Allen Y. Lew Place NW, Washington, DC

Why It Matters to Federal and Defense Organizations

Artificial intelligence is changing the cyber threat landscape. AI dramatically accelerates the speed at which attackers can identify, weaponize, and operationalize software vulnerabilities, particularly memory-safety flaws that proliferate in exploit chains across critical infrastructure and defense systems.
Attendees of Doug Britton's session "Taking Memory Exploits Off the Table in the Age of AI-Accelerated Cyber Warfare" will learn how RunSafe Security's Load-time Function Randomization (LFR) technology transforms software binaries at load time to prevent attackers from reliably exploiting memory safety vulnerabilities even when flaws remain present in the code. LFR requires no source code changes, no recompilation, and no recertification, which makes it deployable on legacy and already-certified defense platforms without operational disruption while extending their service life. Recent modeling puts the payoff for defense at roughly $1.4 billion a year in avoided patching, sustainment, and recertification costs at 25% adoption across more than 140 in-scope programs, and LFR is Iron Bank approved.

Media Opportunities:
Doug Britton will be available for brief one-on-one interviews, technical deep dives, and on-camera commentary regarding the global impact of AI-Accelerated Cyber Warfare. Press credentials can be coordinated via the contact below.

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