Rampart AI™ SECURING CRITICAL INFRASTRUCTURE

Today's Challenges

Critical Infrastructure is under constant threat, and existing threat detection approaches fall short in providing robust security. The Rampart approach revolutionizes application protection of Industrial Control Systems (ICS) and IoT devices.
Our innovative solution ensures self-protection without code changes or constant updates to your ICS.

Backdoor Prevention:	Rampart identifies and stops threat actors from using backdoors and vulnerabilities in ICS systems, even without prior knowledge or heuristics.
Seamless Integration:	Weave security directly into existing ICS applications, making them self-protecting.
Threat Intelligence:	Rampart provides detailed telemetry and attack reports, enhancing existing threat detection tools.
Proven Technology:	Developed under the Small Business Innovative Research program, Rampart has undergone rigorous red team testing and supports Navy Aviation Red Team.

Cyber Lab Validation

Our dedicated cyber lab continuously validates Rampart's effectiveness, ensuring scalability and reliability.

Emergent Artificial Intelligence-Generated Threats

The use of Artificial Intelligence by nation-states and criminal gangs to rapidly identify vulnerabilities and develop exploits against critical infrastructure requires a new approach. Enabling ICS to be self-protecting represents a critical layer in improving the nation's cyber defense.

Lee Krause, CEO of Rampart AI™
lkrause@rampart-ai.com
www.Rampart-AI.com