Rampart AI™

EMPOWERING SECURE, RELIABLE APPLICATIONS

Rampart AI™ is the industry-leading Application Security technology that continuously monitors software applications to ensure seamless operation. Our innovative architecture comprises a robust server framework and language-specific agents.

KEY FEATURES

- **Behavior Model:** Automated Machine Learning leveraged to defend your business operations
- **Behavior Detection:** Detect and block suspicious behaviors
- **Zero-Trust Security:** Ensure applications remain secure even when interacted with untrustworthy clients

DETECTS VULNERABILITIES

Prevents issues like Remote Code Execution (RCE), SQL injection attacks, and logic bombs

PROVEN SECURITY

Successfully tested against "rogue programmer" scenarios, including the SolarWinds exploit and more

- 30+ examples highlighting Rampart™ alerting and blocking attacks

INDUSTRY-VALIDATED

- Independent Red Team Tested
- DoD Use Cases
- Commercial Users

WHY RAMPART?

- Leverage a behavior model to quickly identify abnormal operations at runtime
- Behavior model is automatically developed as part of the deployment process
- Ensure business continuity at the application level at runtime
- Enhance Threat Detection for both known and unknown vulnerabilities at runtime
- Improve application reliability and resiliency

GET RAMPART AI™ FOR YOUR BUSINESS TODAY!

Contact us to learn how Rampart AI™ can fortify your applications against threats and ensure operational integrity.

www.rampart-ai.com contact@rampart-ai.com