Rampart AI™

SAFEGUARD YOUR APPLICATIONS FROM EMERGING THREATS

Rampart AI™ is an advanced Application Security technology designed to fortify your software applications against malicious threats. By employing a cutting-edge architecture comprising a robust server framework and language-specific agents, Rampart-AI ensures the continuous monitoring of your applications, enabling seamless operation while mitigating security risks.

KEY FEATURES

- **Behavior Model:** Leveraging Automated Machine Learning, Rampart-AI establishes a dynamic behavior model that defends against emerging threats.
- **Behavior Detection:** Rampart-AI actively detects and blocks suspicious behaviors in real-time
- **Zero-Trust Security:** Rampart-AI ensures the security of applications even when accessed by untrustworthy clients.

COMBATTING SYSTEM THREATS:

- **Emerging AI-generated threats:** Rampart-AI's proactive defense strategy anticipates and catches potential exploits that remain undetected within your system, ensuring comprehensive protection against evolving threats.
- 2024- **XZ Utils Backdoor:** Rampart-AI's zero-trust security architecture ensures the resilience of your applications, preventing unauthorized access and thwarting backdoor exploits.
- 2023- **Atlassian Confluence RCE Flaw**: By leveraging its behavior model, Rampart AI detects and mitigates risks posed by Remote Code Execution (RCE) flaws, shielding your applications from exploitation.
- 2022- **Spring4Shell**: Through continuous monitoring and behavior detection, Rampart-AI detects and neutralizes threats like Spring4Shell, fortifying your application ecosystem.
- 2022- **Zimbra Collaboration Suite Bugs:** Rampart-AI's proactive defense mechanism guards against vulnerabilities within collaboration suites, maintaining the security of your collaborative platforms.
- 2021- **Log4Shell:** Rampart-AI's behavior model identifies and prevents exploits targeting vulnerabilities like Log4shell, ensuring the integrity of your applications.
- 2020 - **SolarWinds:** Rampart-AI has been successfully tested against sophisticated attacks like the SolarWinds exploit, demonstrating its capability to mitigate high-profile security breaches.

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