Rampart AI™

When your applications are down, your business suffers.
That's why at Rampart AI™ we are working to forge a new frontier in application resiliency.
Rampart's behavior-based approach blocks exploits the first time they occur and every time thereafter.

Resiliency Built For Your Business Applications:

1. Understand Your Application

Rampart™ provides a complete, detailed review of how an application will behave in production. Rampart™ provides a resilient solution that is focused on ensuring your application runs as expected. Rampart™ supports monitoring of containers and fortifies applications built in .NET, Java, and Python.

Complete visibility into your applications behavior

2. Identify Security Risks That Exist in the Application

Rampart™ will deliver an assessment of your application, identifying the risks beyond vulnerabilities that exist in your application, including open source and software supply chain risks that can be exploited.
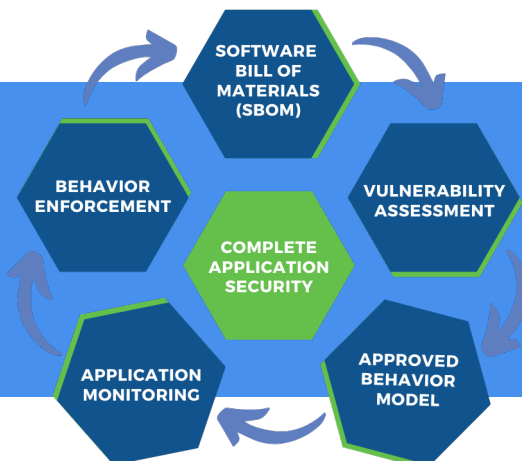
Protection against software supply chain attacks

3. Delivers Zero-Trust Applications to Production

Rampart™ automatically integrates application resiliency directly into the build and test process, monitoring and alerting on all anomalous behaviors. Rampart™ protects against zero-day attacks.

True application protection against zero-day attacks

SOFTWARE BILL OF MATERIALS (SBOM)

BEHAVIOR ENFORCEMENT

VULNERABILITY ASSESSMENT

COMPLETE APPLICATION SECURITY

APPLICATION MONITORING

APPROVED BEHAVIOR MODEL

Protection Across the Application Lifecycle:

Over two years of engagements, Rampart™ has proven its value in detecting and blocking exploits leveraged by professional application pentesters. Witness the power of Rampart™ to protect your application with a live demo.

www.rampart-ai.com