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 for containers provides notifications for exploits the first time they occur and every time thereafter.

Resiliency Built For Your Containerized Business Applications:

1. Understand Your Application

Rampart provides a resilient solution that is focused on ensuring your application runs as expected using dynamic generated rules based on your container. With that dynamic knowledge Rampart flags anomalous behavior happening in your containers environment.

Complete visibility into your applications behavior

2. Identify Security Risks That Exist in the Application

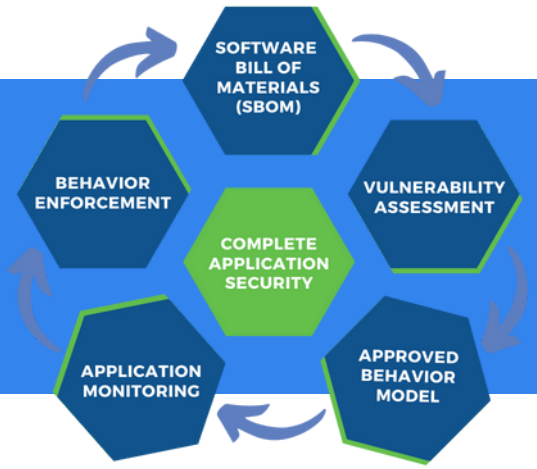
Rampart delivers an assessment of your application, identifying the risks beyond vulnerabilities that exist , including open source and software supply chain risks that can be exploited. Rampart supports monitoring of containers and fortifies applications built in .NET, Java, and Python.

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.

True application protection against zero-day attacks



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.