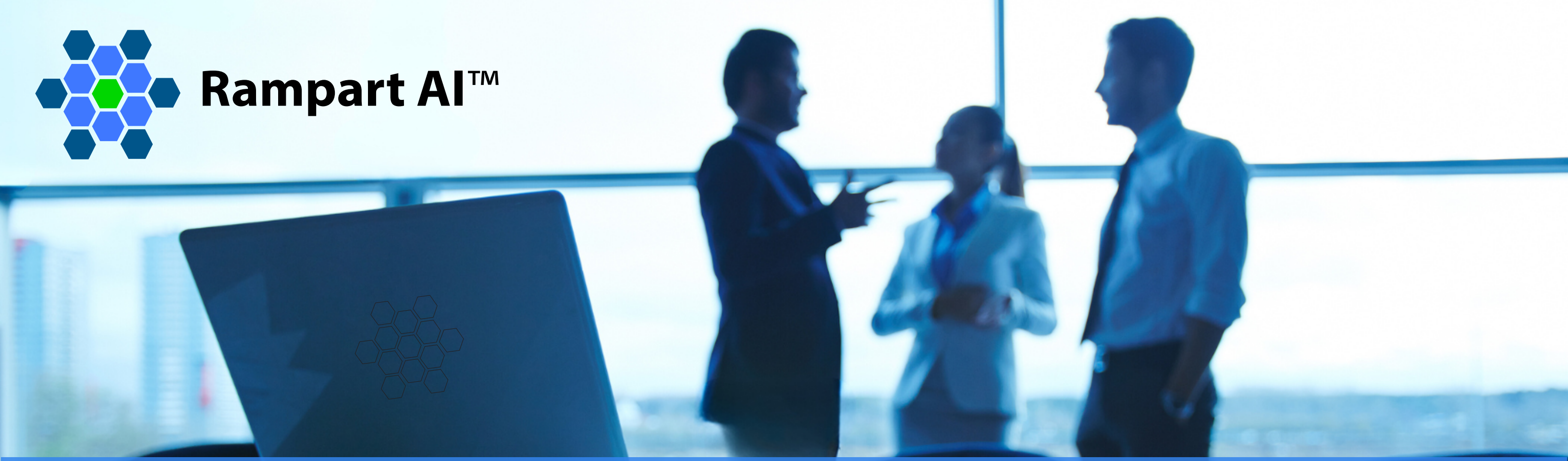
Rampart AI™



Rampart AI™ is the only approach that allows your application to keep up with the mutation of known vulnerabilities

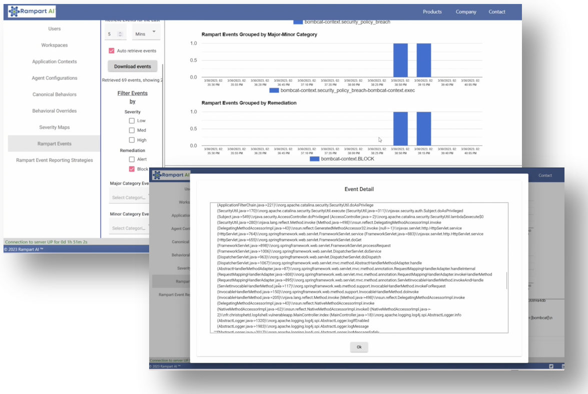
Three Easy Steps For A Resilient Application:

1. **Hardened Sensors Deployed To Monitor For Activity**
   Rampart™ makes sure your application environment is not compromised.

2. **An Agent Learns The Behavior Of Your Application**
   Rampart™ using its sophisicated training model to learns more and more about your application over time.

3. **Rampart™ continues to monitor and protect your application by enforcing the approved behavior model**
   Rampart's™ model, which using AI, improves over time. This means your application protection is constantly updating further protecting your application.

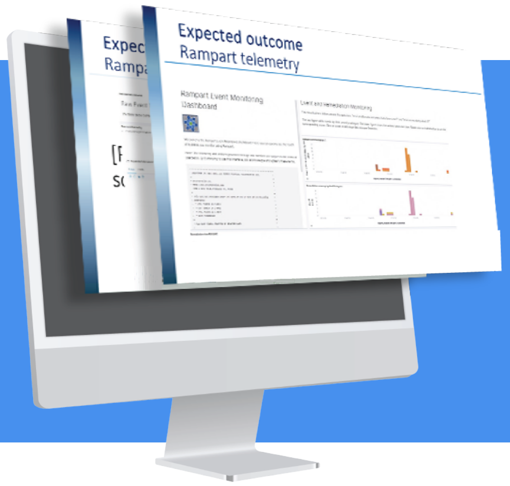
Easy To Use Dashboard



```
(ApplicationFilterChain.java->221)\\norg.apache.catalina.security.SecurityUtil.doAsPrivilege
(SecurityUtil.java->170)\\norg.apache.catalina.security.SecurityUtil.execute (SecurityUtil.java->311)\\njavax.security.auth.Subject.doAsPrivileged
(Subject.java->549)\\njava.security.AccessController.doPrivileged (AccessController.java->-2)\\norg.apache.catalina.security.SecurityUtil.lambda$execute$0
(SecurityUtil.java->280)\\njava.lang.reflect.Method.invoke (Method.java->498)\\nsun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java->43)\\nsun.reflect.GeneratedMethodAccessor32.invoke (null->-1)\\njavax.servlet.http.HttpServlet.service
(HttpServlet.java->764)\\norg.springframework.web.servlet.FrameworkServlet.service (FrameworkServlet.java->883)\\njavax.servlet.http.HttpServlet.service
(HttpServlet.java->655)\\norg.springframework.web.servlet.FrameworkServlet.doGet
(FrameworkServlet.java->898)\\norg.springframework.web.servlet.FrameworkServlet.processRequest
(FrameworkServlet.java->1006)\\norg.springframework.web.servlet.DispatcherServlet.doService
(DispatcherServlet.java->963)\\norg.springframework.web.servlet.DispatcherServlet.doDispatch
(DispatcherServlet.java->1067)\\norg.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle
(AbstractHandlerMethodAdapter.java->87)\\norg.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal
(RequestMappingHandlerAdapter.java->808)\\norg.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod
(RequestMappingHandlerAdapter.java->895)\\norg.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle
(ServletInvocableHandlerMethod.java->117)\\norg.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest
(InvocableHandlerMethod.java->150)\\norg.springframework.web.method.support.InvocableHandlerMethod.doInvoke
(InvocableHandlerMethod.java->205)\\njava.lang.reflect.Method.invoke (Method.java->498)\\nsun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java->43)\\nsun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java->62)\\nsun.reflect.NativeMethodAccessorImpl.invoke0 (NativeMethodAccessorImpl.java->-
2)\\nfr.christophetd.log4shell.vulnerableapp.MainController.index (MainController.java->18)\\norg.apache.logging.log4j.spi.AbstractLogger.info
(AbstractLogger.java->1320)\\norg.apache.logging.log4j.spi.AbstractLogger.logIfEnabled
(AbstractLogger.java->1983)\\norg.apache.logging.log4j.spi.AbstractLogger.logMessage
```

Full Stack Trace

- When deploying Rampart™ our code is instantly drop into your enterprise for immediate insight into your application. In addition to building the applications behavior model.
- Rampart™ is added into an applications CI/CD Pipeline either before or after depoyment.
- Rampart™is used for all containerized applications in addition to Java .Net, and Python based applications.



Rampart™ is the true zero-trust protection that defends applications.

Current signature- and vulnerability-based tools are inadequate to stop advanced cyber operations, and the sheer number of vulnerabilities make it difficult to keep up with a changing environment. Rampart™ requires no prior knowledge to stop a cyber attack, true zero-day protection.

www.rampart-ai.com