

Waratek Solves the **Application Security** Problems That No One Else Can

Application Security with No Code Changes for Java and .NET

Point. Click. Protect.



Virtual Patching

There is more than one way to win the cybersecurity race

Each security patch issued by Oracle, Microsoft, IBM, Apache or any software developer starts a relay race. One team is the malicious hackers who exploit new flaws to steal valuable data or take control of an important process. The other runners are application security and development teams who need weeks, months, or years – if ever – to fully patch known software flaws across an enterprise. Losing the race is not an option.

Waratek Patch is a lightweight runtime plugin agent for Java and .NET-based applications. Using “virtual” patches, teams can instantly protect applications from known flaws - including long-term unpatched vulnerabilities - without any code changes or taking an application out of production.

Virtual patches function just like a physical binary, but dramatically reduce the time to patch and the risk of being breached while waiting to apply a critical update. A virtual patch can be applied within hours of the release of a routine or emergency patch without the risk of breaking an application.

Benefits	Traditional approach	Waratek
Create custom patches from scanner outputs	✗	✓
Patch without downtime or code changes	✗	✓
Instantly apply functional equivalent patches	✗	✓
Improve compliance with patch requirements	✗	✓
Automatically deploy patches across all apps	✗	✓
Reduce patching costs	✗	✓

Point. Click. Patch.

Always on Security

The US National Vulnerability Database currently includes more than 99,900 known software flaws, including approximately 40,000 CVEs of the highest severity. Nearly 15,000 new vulnerabilities were added in 2017.

Each software vulnerability represents a point of attack – most often against a web application. In a software driven world under siege from malicious hackers, securing applications is a requirement for all businesses and government agencies.

Waratek Secure offers “always on” security protections that ensure 100% accuracy detecting code injection attacks. A lightweight runtime plugin agent for Java and .NET-based applications, Waratek Secure instantly protects against OWASP Top Ten, SANS Top 25, and other common attacks that exploit known software flaws.

Waratek Secure installs in minutes and instantly protects applications without requiring code changes or routine tuning. Best of all, Waratek Secure has an ultra-low performance impact on an application and it produces no false positives. Waratek Secure is backed by a rules subscription that allows you to select out-of-the box protections as well as apply custom rules without downtime.

Benefits	Traditional approach	Waratek
No false positives	✗	✓
Ultra-low performance overhead	✗	✓
Installs in minutes; instant protection	✗	✓
No code changes required	✗	✓
No tuning; no white or black list maintenance	✗	✓
Seamless integration with Waratek Patch agent	✗	✓
Write and deploy custom rules with no restart	✗	✓

Point. Click. Secure.





Complete Application Security Platform

After 22 years and nine major versions, Java remains the most used programming language in the world. Ask an IT leader which Java version they use for web applications and the likely answer is a variation of “all of them - except the current one.”

Company policies, industry standards and government regulations often require applications to be based on the most current version of the Java Virtual Machine. Yet, upgrading older Java-based enterprise applications is a binary choice: continue to run the app as is; or, invest a significant amount of time, money, and people to rewrite the code.

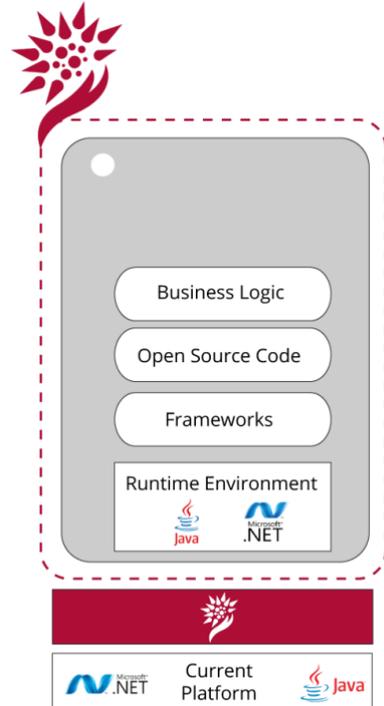
Instant platform upgrade. No code changes or magic required.

Waratek Enterprise utilizes the full power of virtualization to upgrade out-of-support Java applications to the most current version of the Java Virtual Machine (JVM).

Waratek wraps the entire application stack – including the original Java Runtime Environment (JRE) - in a virtual “guest” container on top of the most current JVM that acts as the “host.”

This unique, patented approach to application protection has been in production worldwide for more than two years without generating a single false positive.

This virtualization-based guest / host architecture allows the application to continue to run using its original business logic, but protected by virtual patches and the most current version of the JVM without the time, risks, or costs of rewriting the application. This arrangement also serves as a compensating control¹ for purposes of compliance, further reducing costs and the pressure to immediately rewrite older applications.



Simple Solutions for Complex Problems

Along with the benefits of a virtual Java upgrade, Waratek Enterprise solves security and performance issues not available from traditional application security approaches, including:

- Full application stack protection from 0-Day Attacks and the OWASP Top Ten - without heuristics, code changes, or routine tuning – for Java and .NET-based applications. The performance impact is <3% under attack and *improves* app performance under normal operating conditions.
- Waratek’s unique “always on” application protection ensures 100% accuracy when detecting code injection attacks – backed by a No False Positives financial guarantee – for Java and .NET applications.
- Instantly and automatically patch Java and .NET applications with a code equivalent “virtual” patch without downtime, code changes or tuning. App Sec and Development Teams can also create and deploy custom patches to fix code flaws reported by scanning tools.

Point. Click. Protect.



Waratek Features:

Features	Waratek Patch	Waratek Secure	Waratek Enterprise
Lightweight Agent <i>(requires subscription)</i>	Standard	Standard	
Full Agent			Standard
Rules Engine	Standard	Standard	Standard
Management Console	Standard	Standard	Standard
Virtualization Layer			Standard
Always-on Protection		Standard	Standard
No Code Changes Required	Standard	Standard	Standard
No Profiling or Tuning	Standard	Standard	Standard
Full Stack Protection			Standard
Virtual Upgrade for Java			Standard
Ultra-low Performance Overhead	Standard	Standard	Standard
CPU Subscription	Paid Option		Standard
Custom Patch Service	Paid Option		Paid Option
Patch Library	Paid Option		Paid Option
A` la Carte Patches/CPU	Paid Option		Paid Option
OWASP/SANS Rules Subscription	N/A	Paid Option	Standard
Custom Rules Service	N/A	Paid Option	Paid Option
A` la Carte OWASP/Sans Rules	N/A	Paid Option	Paid Option
No False Positives	N/A	Standard	Standard
Virtual Patch Will Not Break an App	Standard	N/A	Standard
No Successful Attack against Virtually Patched App	Standard	N/A	Standard

Summary

Waratek is a pioneer in the next generation of application security solutions. Using patented virtualization technology, Waratek makes it easy for security teams to instantly patch known flaws, virtually upgrade out-of-support applications, and protect 100% of their application code – all without time consuming and expensive code changes or unacceptable performance overhead.

Waratek is one of [CSO Online's Best Security Software](#) solutions of 2017, a winner of the RSA Innovation Sandbox Award, and more than a dozen other awards and recognitions.