WARATEK SECURE

DATASHEET

Instantly remediate Java vulnerabilities with immutable control through policy

Ensure desired security behavior is applied consistently in the runtime with fully-automated patch management and validation that finds and fixes known and unknown vulnerabilities alike.

Overview

In 2022 a new CVE is released nearly every 4 hours, with 32% of those vulnerabilities classified as critical. While you may not be at risk for every vulnerability published, with an MTTR of 205 days, even a handful of critical vulnerabilities can consume your roadmap for the next year and a half.

The effect of this velocity means security teams will need to adjust their approach to the application layer of security according to the OSI model. Waratek Secure provides application security automation with Security-as-Code for defining, applying, and managing control through policy to be executed in the runtime.

Security-as-Code allows security teams to scale with modern software development. New rules deploy into production without waiting for a deployment window or restarting your servers. This streamlined approach reduces human error and false positives while maintaining lockstep with the rapid rate of code changes.

Benefits

- Ultra-low performance overhead
- Full protection against OWASP Top 10, Sans 25, and many others
- Protection against Zero-Day attacks
- No code changes Required
- No tuning or list maintenance
- Rapid response to new threats

Solve Security at Scale

Achieve economics to deploy, scale, and maintain security throughout every application using automation.

Don't Fret Code Changes

Eliminate vulnerability regressions with immutable security that overrides any changes to the codebase in the future.

Instantly & Effortlessly Patch

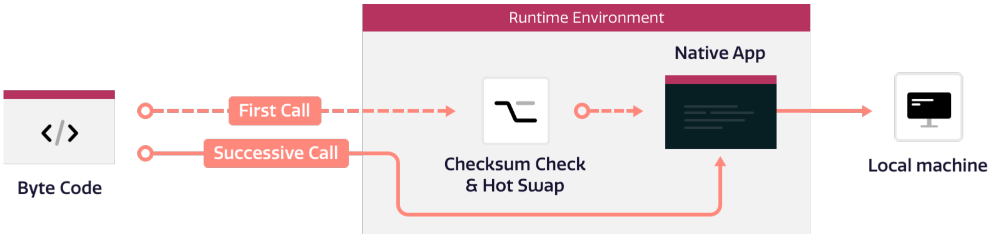
Apply patches in live executing code rather than the next available deployment window in your CI/CD pipeline.

> Waratek not only found the cryptominer we knew we had, but securely removed it within 48 hours, stopping us from having to rebuild our solution from scratch.
>
> – SEBASTIEN ROCHE, CISO

How it Works

When an action is performed on your applications for the first time, and an attempt is made to execute vulnerable code, Waratek Secure performs a checksum check and tells your application to ignore the code.

A healthy version of the code is returned in real-time as defined in your Policy Config file or the Waratek Portal. Only the healthy version will be made available on any additional call to that same piece of code, resulting in even faster execution.



Technical Requirements

Requirement	Notes
Java Vendors	• Oracle Hotspot • OpenJDK • IBM J9 • Amazon Corretto • JRockit
Java Versions	5, 6, 7, 8, 11, 16

Technical Specs

Feature	Notes
Agent Size	3MB
CPU Utilization	< 5%
Memory Utilization	25MB
Network Utilization	Negligible at scale

See first hand how Waratek can help you

Immutable Security
Say goodbye to regressions after deployments. Once your policy is defined, no code added to the codebase can supersede the policy.

Deployment Agnostic
Securing your runtime instead of your codebase or CI/CD pipeline enables critical patches to be applied instantly instead of during the next deployment window.

Economically Scalable
Remove the toil of false positives and long feedback loops between security and engineering to transform the economics of AppSec.

sales@waratek.com

waratek.com

linkedin.com/company/waratek-ltd