WARATEK SECURE

DATASHEET

Autonomous Java Application Protection Against Known Vulnerabilities and Zero-Days

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 ever 4 hours, with 32% of those vulnerabilities being classified as critical. While you may not be at risk for every vulnerability that's published, with a 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 the desired final state of security behavior for your applications to be executed in the runtime.

Security-as-Code allows security teams to manage security behavior the same way application developers build applications: codify, validate, test, and deploy into production without restarting your servers, to reduce human error, false positives, and maintain 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

Protect whole-of-enterprise apps by preventing false positives, removing depedency on DevOps, and decreasing Time-to-Protection to seconds

Don't Fret Code Changes

Automatically apply appropriate security behavior in real-time as new or changed code is deployed without fear of security regression

No-Code Patching

Patch security vulnerabilities such as Zero-Day exploiits without DevOps intervention and deploy security behavior with no downtime

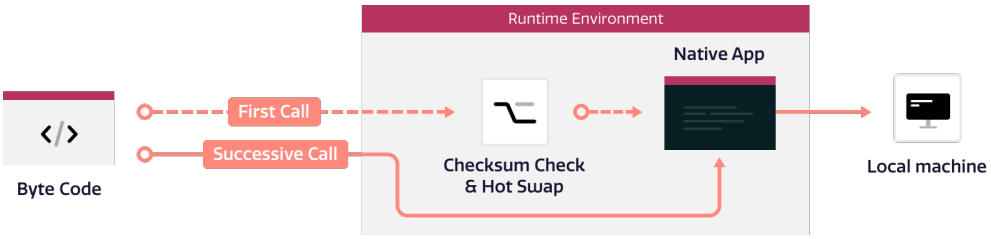
> **Waratek not only found the cryptominer we knew we had, but securely removed it within 48 hours, stopping us from having to rebuild our solution from scratch.**

– 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 ingore the code.

A healthy version of the code is returned instead in real-time as defined either in your Policy Config file or the Waratek Portal. On any additional call to that same piece of code only the healthy version will be made available, 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

Let us show you first hand how Waratek can help you with:

Autonomous Protection
Fix known and unknown vulnerabilities in real-time without a single code change

Virtual Patches
Virtually upgrade applications without code changes, vendor patches, or downtime

Removing Security Gaps
Engrain protection within the DNA of your apps instead of relying on protection that sits on top allowing attacks to slip through

sales@waratek.com

waratek.com

linkedin.com/company/waratek-ltd