WARATEK

DATASHEET

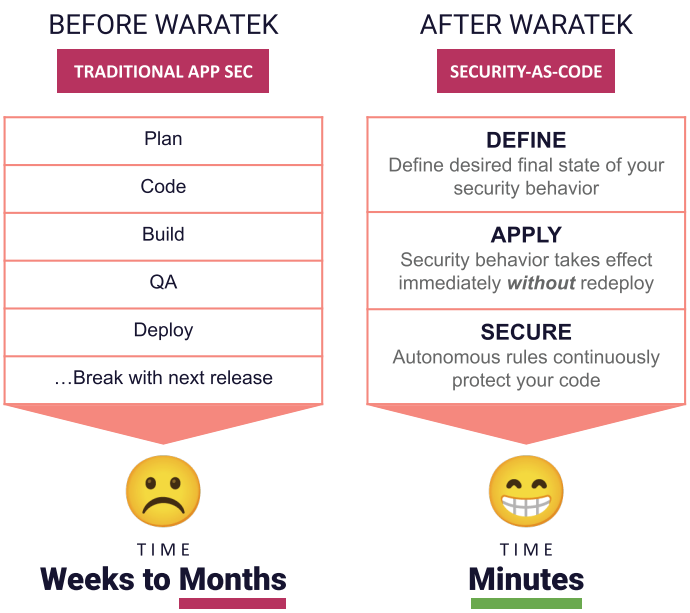
Introduction to Security-as-Code

Shifting security left shortens feedback loops through the development lifecycle, but doesn't solve for scalability. Security-as-Code enable security to scale with modern software development by providing security professionals control through policy. The result is immutable security, release-after-release.

Overview

Security-as-Code is the practice of leveraging machine-readable definition files that use high-level descriptive coding language to automate security behavior in the runtime.

This approach drastically reduces reliance on human intervention and grants security teams autonomy while allowing engineers to focus on development rather than vulnerability remediation.



Instead of trying to keep pace with development and the rate of deployments only to miss the majority of releases or hold up business-critical features from hitting production, Security-as-Code uses a Policy Config file to declaratively or imperatively define the desired security outcome for your applications allowing an agent to apply the protection in real-time.

Simplifying the security process to properly integrate into the DevOps pipeline will help you maintain parity with development velocity and make time-to-protection instantaneous.

This means you're able to secure every application on every environment, release-after-release, diminishing your risk profile, resulting in happier security teams.

Immutable Security

Remove the risk of reintroducing previously fixed vulnerabilities back into your apps

No-Code

Define and execute your desired security outcomes in a single file or portal without engineering help

Scalable Enterprise Security

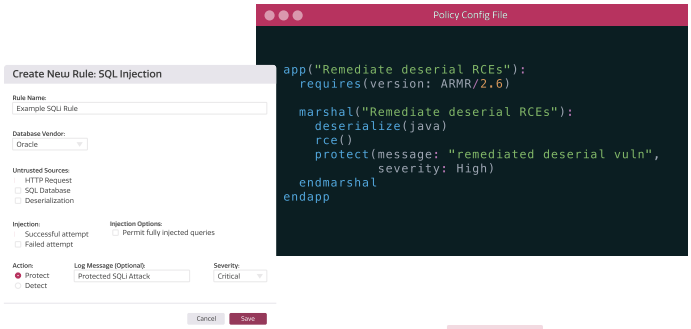
Achieve the economics to deploy and maintain security in every app in your enterprise

> **Utilizing security as code enables organizations to scale with modern software development by codifying security and policy into development processes and workflows.**
>
> – Melinda Marks, Senior Analyst, ESG

How it Works

1. Define Your Desired Security Behavior

Tell your applications how you want them secured declaratively or in-app. Remove the dependency on developers and DevOps to scale your entire team's impact.

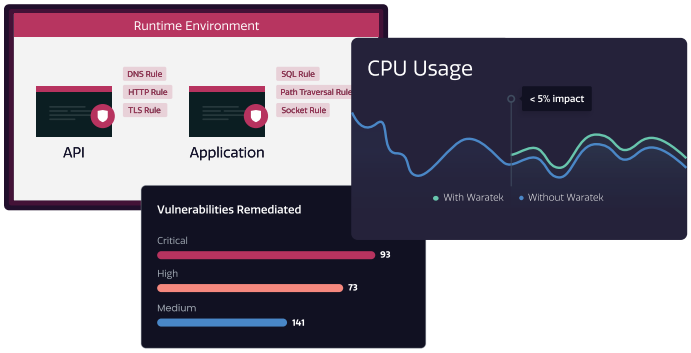


2. Apply Defined Behavior in Real-Time

Launch desired security updates without deployment. No longer wait to slot into a sprint or an in-the-future release, reducing Time-to-Protection to milliseconds.

3. Automatically Secure Every Request

Protection is applied to every file in the codebase and every request (no sampling) without the expensive performance cost or margin of failure found in most security platforms.



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