Security's Struggle in Scaling with Modern Development

INDUSTRY REPORT

waratek.com WARATEK

A Word From Our CEO

DevOps has proven pivotal to the growth and sustainability of many companies worldwide. However as with any form of progress, it's also introduced new obstacles. This is most evident amongst security professionals. These critical practitioners are responsible for evaluating and elevating the security posture of their organizations in effort to stop data breaches and bad actors.

As software grows in complexity and release cycles continue to accelerate to every other week, it becomes increasingly difficult to even just maintain your existing security posture. New CVEs pop up at an alarming rate and manual processes are slowing security teams down. If these critical employees can't find a solution to maintain pace with the rapid rate of deployment, their work is going to get away from them and we're going to see exponential increase in data breaches worldwide. Some companies will be able to sustain this, but most won't.

With this survey, we look at how security professionals have integrated with DevOps processes, what challenges they face with that integration, and what they believe is the path forward to not only secure companies, but happy & empowered security teams. Our goal is to share what challenges are fueling DevSecOps, projected to be a $23.42 billion market by 2028, in order to help us understand what we can do to fix that and help security teams perform the best work of their lives.

Doug Ennis
CEO, Waratek

Here are some key takeaways gained about security professionals. Through this survey we take a deeper dive into each of these findings in the body of this report.

61% of teams have to delay critical security work. Given the rapid rate of releases, security teams are often forced to delay critical security work. This finding is critical as even when security is "shifted left" the same process has to be performed to monitor, test, and patch vulnerabilities.

Existing tools waste more time than they save. 84% of security professionals spend hours per year investigating false positives, with 50% spending days if not weeks. Most security tools are limited to merely pattern matching network data, lacking context to make informed decisions. How does a WAF know there's a deserialization exploit? It doesn't.

92% want control through policy. 85% of security professionals believe manual security activities negatively impacts the rate of deployment. 92% of everyone surveyed believe the ability to define immutable security behavior, similar to an Infrastructure-as-Code approach is the only way for security to scale with modern software development.

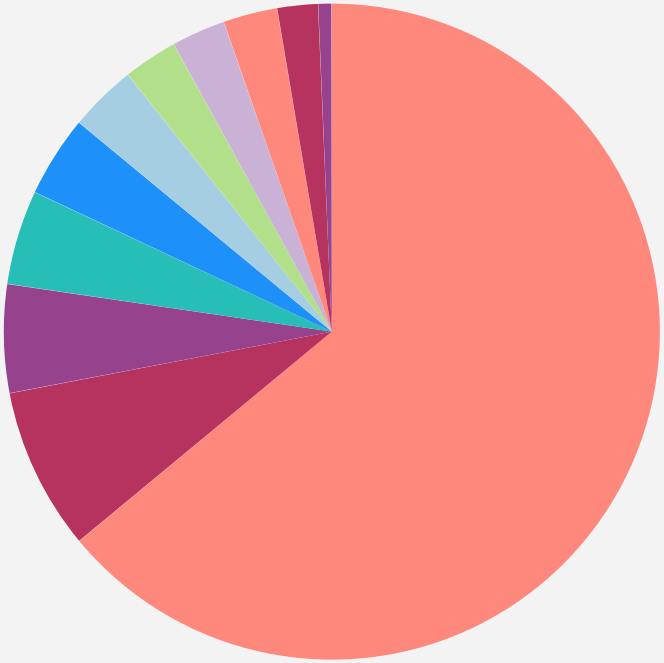
Profile of Who We Surveyed

PART 1

Because the purpose of this survey was to learn more about security professionals specifically, we limited our query to only those individuals actively working in that role. By far the largest group, 64%, work for companies described as being in the technology industry, and 50% of the respondents work for large-to-enterprise businesses (1.000 - 10,000+ employees).

If we were to build a baseline profile of the typical respondent for this survey, it would be a security leader who works at a large-sized, cloud-native technology company.

What Industry Does Your Company Operate In?

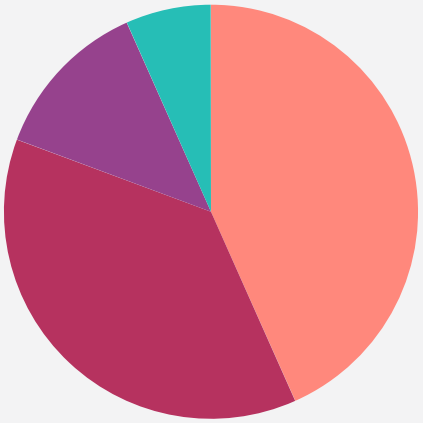


INDUSTRY	%
Technology	64%
Healthcare	8%
Government	5.3%
Finance	4.7%
Manufacturing	4%
Insurance	3.3%
Other	2.7%
Services	2.7%
Retail	2.7%
Education	2%
Utilities / Energy	0.7%

What best describes your job title?

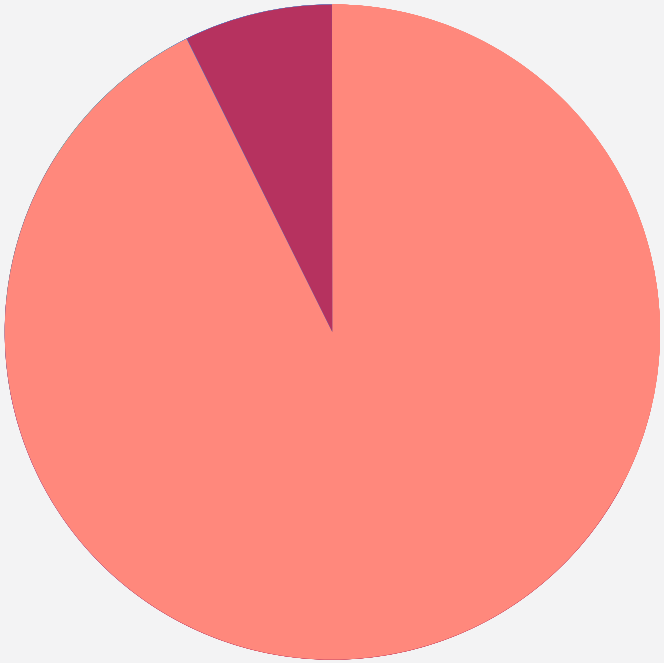
ANSWERS	%
Security Manager	32.7%
Director of Security	26.7%
Security Engineer	17.3%
CSO / CISO	14%
VP of Security	9.3%

What best describes the size of company you work for?



ANSWERS	%
Large (1,000 – 10,000)	43.3%
Medium (100 – 999)	37.3%
Small (1 – 100)	12.7%
Enterprises (10,000 +)	6.7%

Does your organization take part in DevOps or other agile deployment methodologies?



ANSWERS	%
Yes	92.7%
No	7.3%

The Majority of Security Professionals Work in Agile Methodologies

If our survey represents the industry at large, it suggests that most security professionals work inside an agile process, specifically DevOps. According to Gartner in 2021, 83% of IT decision makers reported implementing DevOps. Compared to the 47% in 2016, it's clear that this trend is not going away any time soon, and our response of 92% in 2022 suggests just that.

Experience Working in the DevOps Process

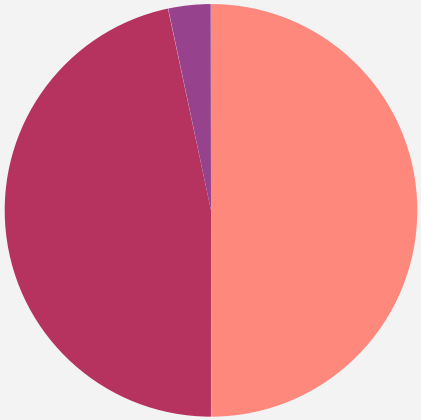
PART 2

Introduction

We created this portion of the survey to illuminate the challenges and dynamics of security professionals working in an agile process. We look at the impact on workload and prioritization, and how that crosses over into satisfaction.

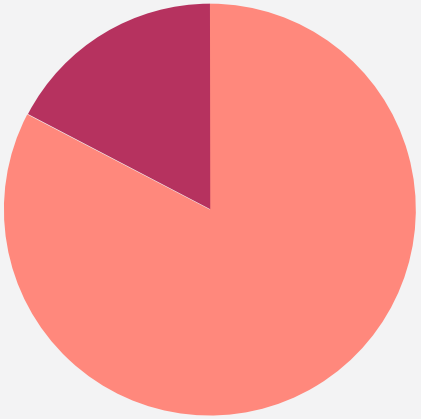
We'll provide insights into what security leaders should know about the experience of security professionals in DevOps.

Maintaining a strong security posture at the rate of my company's deployment velocity is



ANSWERS	%
Challenging	50%
Fine	46.7%
Not possible	3.3%

Has the increase in rate of deployment led to an increase in previously remediated vulnerabilities being reintroduced?

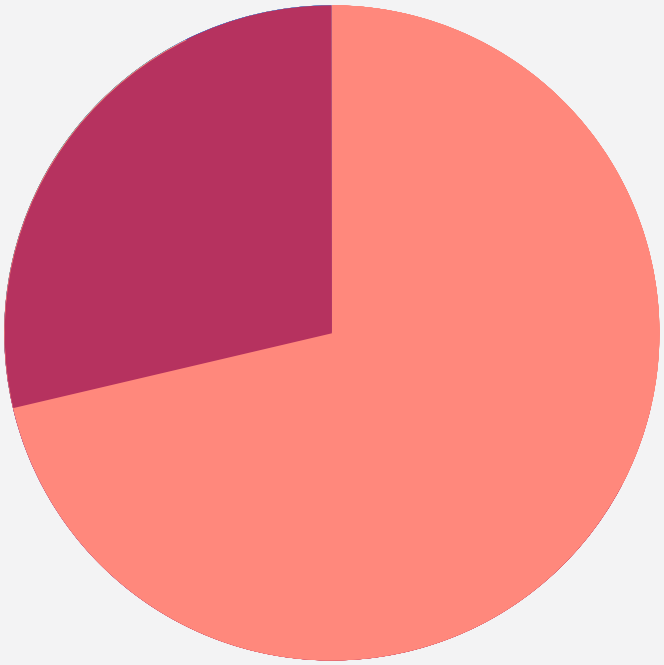


ANSWERS	%
Yes	82.7%
No	17.3%

The Growing Impact on Security Posture

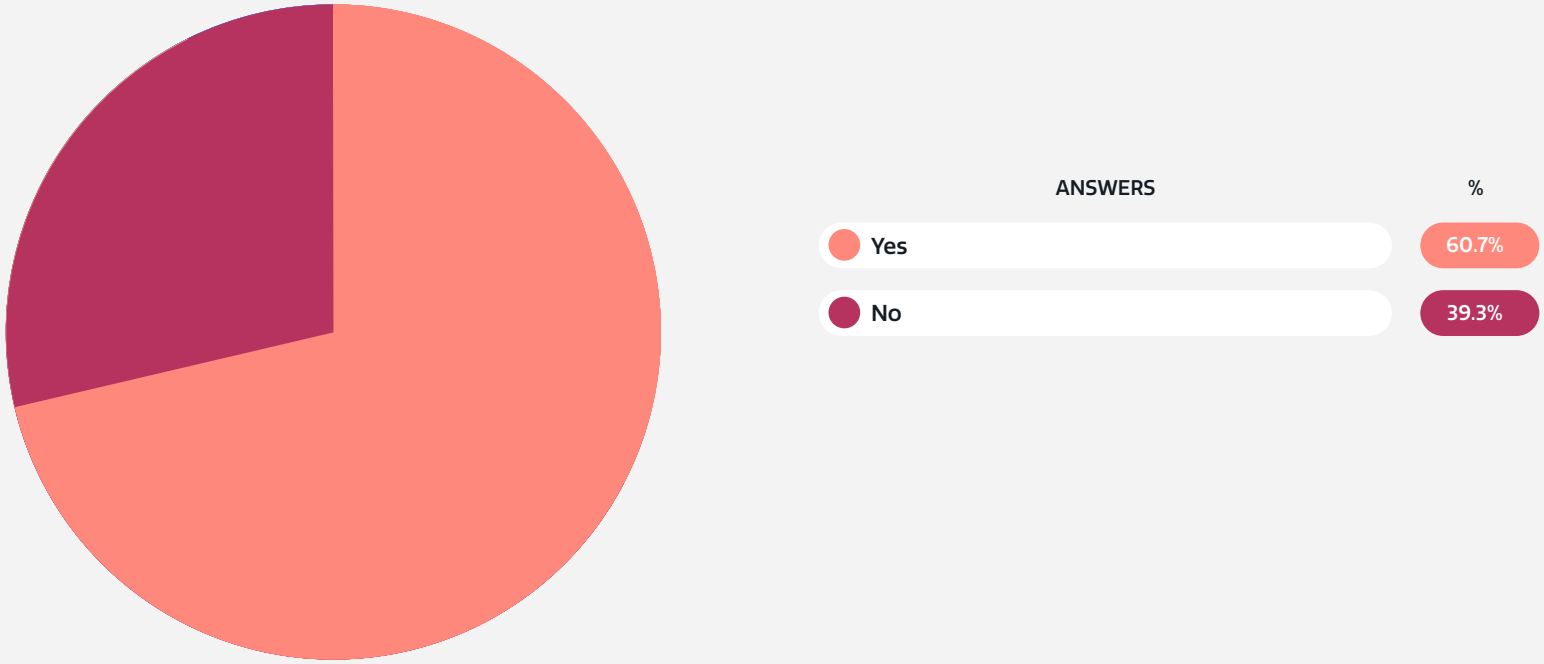
The growing adoption of DevOps lines up nearly perfect with the growing rate of CVEs year-over-year. As a result of shipping software faster, we're reintroducing previously fixed vulnerabilities at an alarming rate. This never-ending treadmill has security teams moving fast, but going nowhere. As organizations aim to deploy even faster, the difficulty to maintain a strong security posture and keep up with deployments is bound to grow.

Do you feel as though keeping pace with engineering and DevOps will get more difficult in the future?



ANSWERS	%
Yes	71.3%
No	28.7%

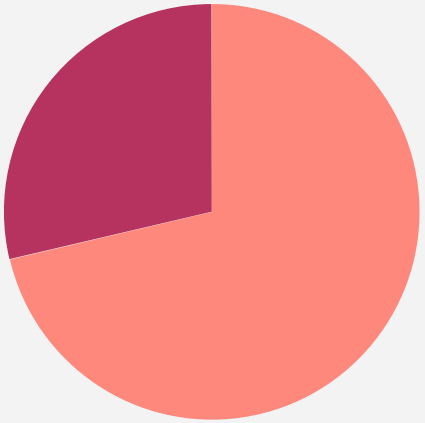
Does keeping up with deployments result in other critical security work being delayed?



Results of Decreased Autonomy

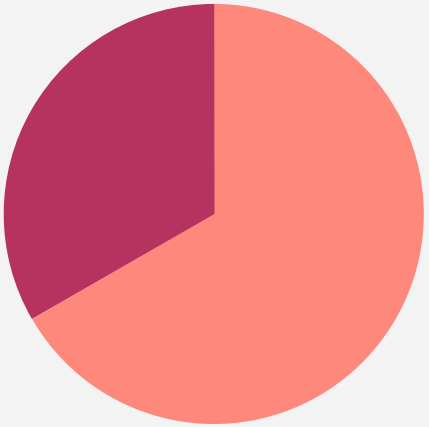
In order to keep up with the growing rate of deployments, the majority of security teams are forced to delay critical security work such as securing a remote workforce, or simplifying cloud access controls. While securing every deployment is important, these critical security projects drive busines value and reduce risk in a constantly shifting security landscape.

Does implementing security in the DevOps process slow down the potential rate of deployment?



ANSWERS	%
Yes	57.3%
No	42.7%

Would you ever be willing to sacrifice security in order to make an important release date on time?

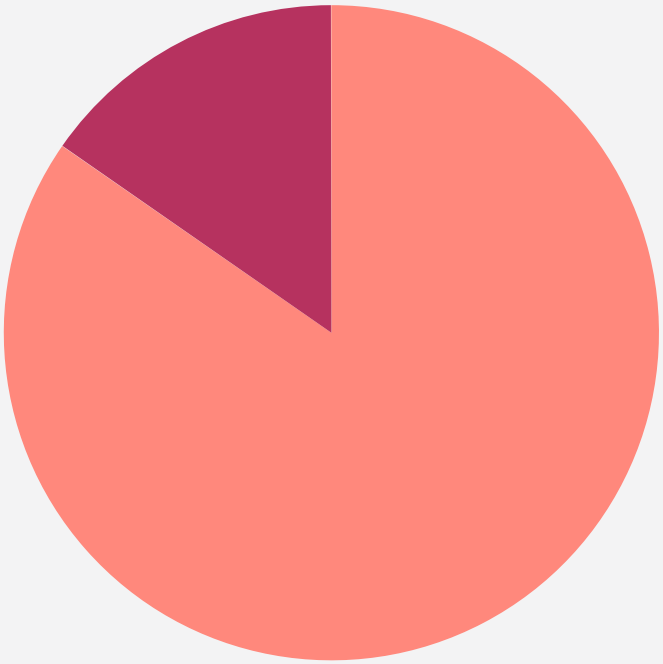


ANSWERS	%
No	66.7%
Yes	33.3%

Removing the Slow Pitstop from an Otherwise Agile Process

It's also interesting to note that a sizable percentage of respondents indicated that they believe removing manual security activities from the DevOps process would have a positive impact on the process as a whole. As organizations deploy faster, automating security is the only path forward if security is to scale with modern software development.

If you could achieve the same level of security but remove the manual security activities, do you feel it would have a positive impact?



ANSWERS	%
Yes	84.7%
No	15.3%

Summary

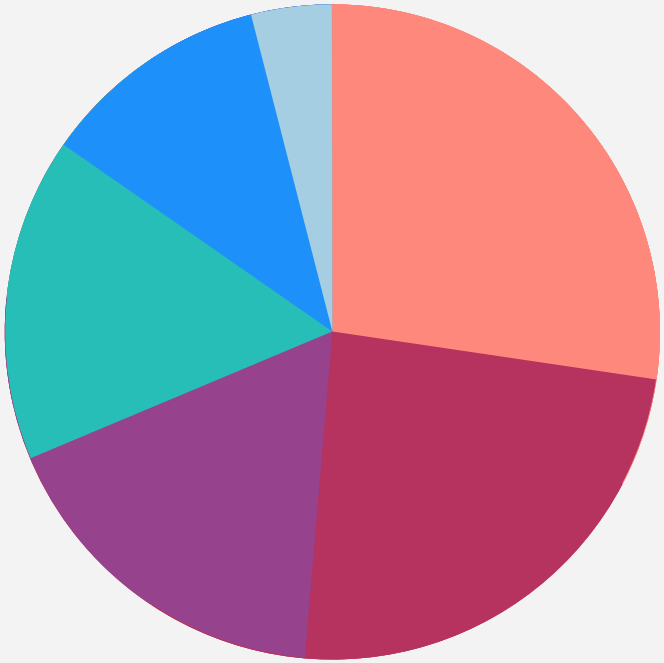
Our picture has become more clear as we have looked deeper at what security professionals' experience is with the DevOps process. We know from their answers that the increase rate of deployments have introduced a serious and concerning challenge. They want a different way to work, but aren't sure what that looks like.

Let's now pivot to look at the tools they use, how they add to the existing workload.

The Impact of Current Tooling

PART 3

How much of your week do you spend investigating vulnerabilities uncovered by a vulnerability scanner?

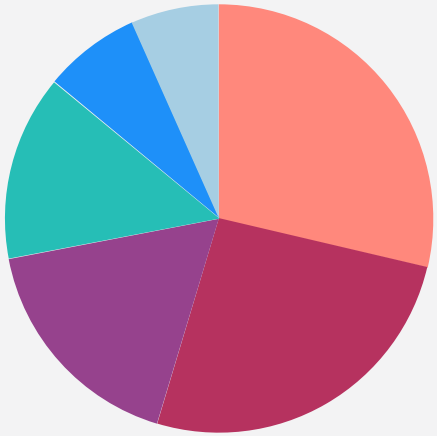


ANSWERS	%
20 – 29%	27.3%
30 – 39%	24%
50% +	17.3%
40 – 49%	16%
10 – 19%	11.3%
less than 10%	4%

Economics of Toil

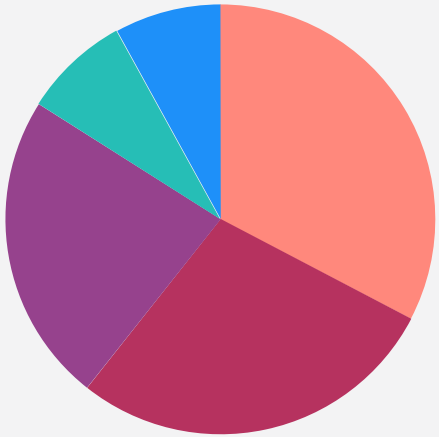
Tooling is designed to save us time, yet almost a third of security professionals spending nearly a third of their week investigating scanner results. Not only is this a manual process that doesn't scale with the modern software development process, but it's economically impossible to dedicate resources to cover every application in the enterprise.

Estimating, which of your security alerts are false positives?



ANSWERS	%
10 -19%	28.7%
Less than 10%	26%
20 -29%	17.3%
40 - 49%	14%
50% +	7.3%
30 - 39%	7.3%

Estimating, how much time do you spend investigating false positives per year?



ANSWERS	%
Hours	32.7%
Days	28%
Weeks	23.3%
Months	8%
Minutes	8%

Summary

When your tooling focuses on a symptom, like network data, rather than the cause, like your applications' code, the best you can do is make an educated guess.

Security teams have too little time and too much to do to base their workload on assumptions. As the rate of deployments increase the number of false positives and negatives that security teams have to investigate will also increase.

There's hope though. Next let's turn our focus to a path forward.

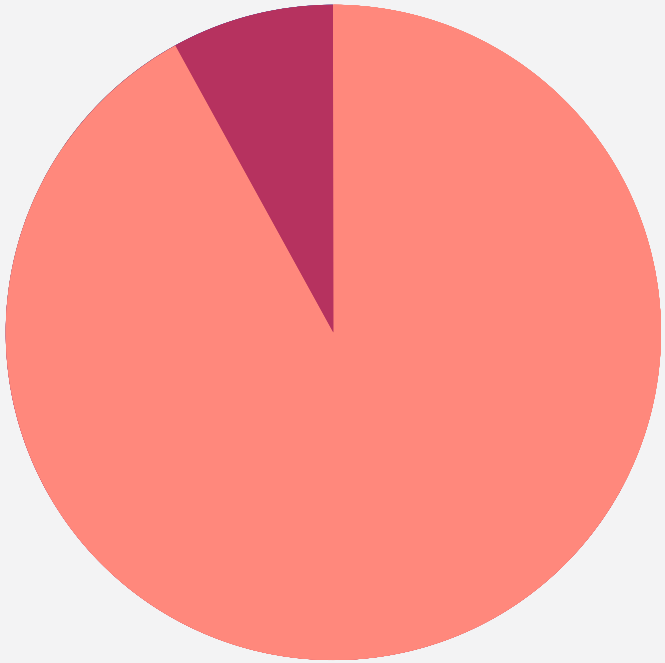
The Path Forward with Security-as-Code

PART 4

Automating Security with Security-as-Code

The notion of shifting security earlier in the process is only a part of the equation. If you merely shift the same activites earlier in the process, you still have to do those same activities. Most security professionals don't want to just shorten the feedback loop with engineering, but automate it with control through policy, where security happens as the application executes.

Would you prefer to immutably apply desired security outcomes in a configurable file similar to Infrastructure-as-Code



ANSWERS	%
Yes	92%
No	8%

Summary

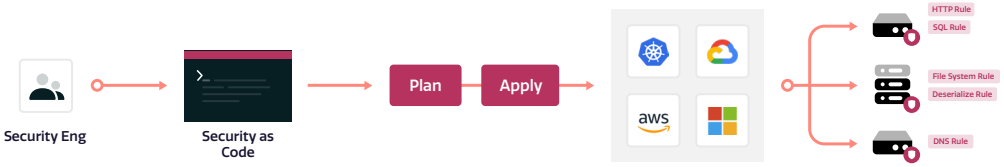
Security-as-Code enables security to scale with modern software development for the first time. By providing security teams the template to immutably tell their applications what behavior they want to secure and what they expect, both security and development teams can focus on just doing their jobs without the back-and-forth.

Next let's dive into an introduction on Security-as-Code.

An Introdution to Security-as-Code

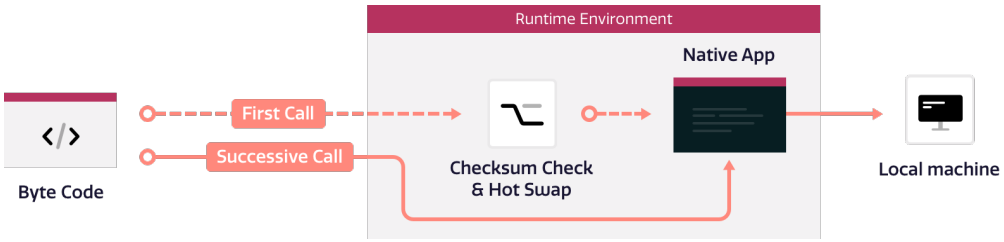
What is it?

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.



How Does it Work?

When an action is performed on your applications for the first time and an attempt is made to execute vulnerable code & a checksum check tells your application to ignore the code. A healthy version of the code is returned instead in real-time as defined in your Policy Config file. On any additional call to that same function, the healthy version will be made available, resulting in even faster execution.



Solve Security at Scale

Protect all your apps by preventing false positives, removing dependency on engineering, & 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 exploits without engineering intervention and deploy security behavior with no downtime

> **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

INSTANT SECURITY-AS-CODE DEMO

To learn how Security-as-Code can help your security team get in front of the growing rate of deployments, never experience another security regression and wave goodbye to false positives & negatives, watch the Waratek Demo.

Start Demo

www.waratek.com