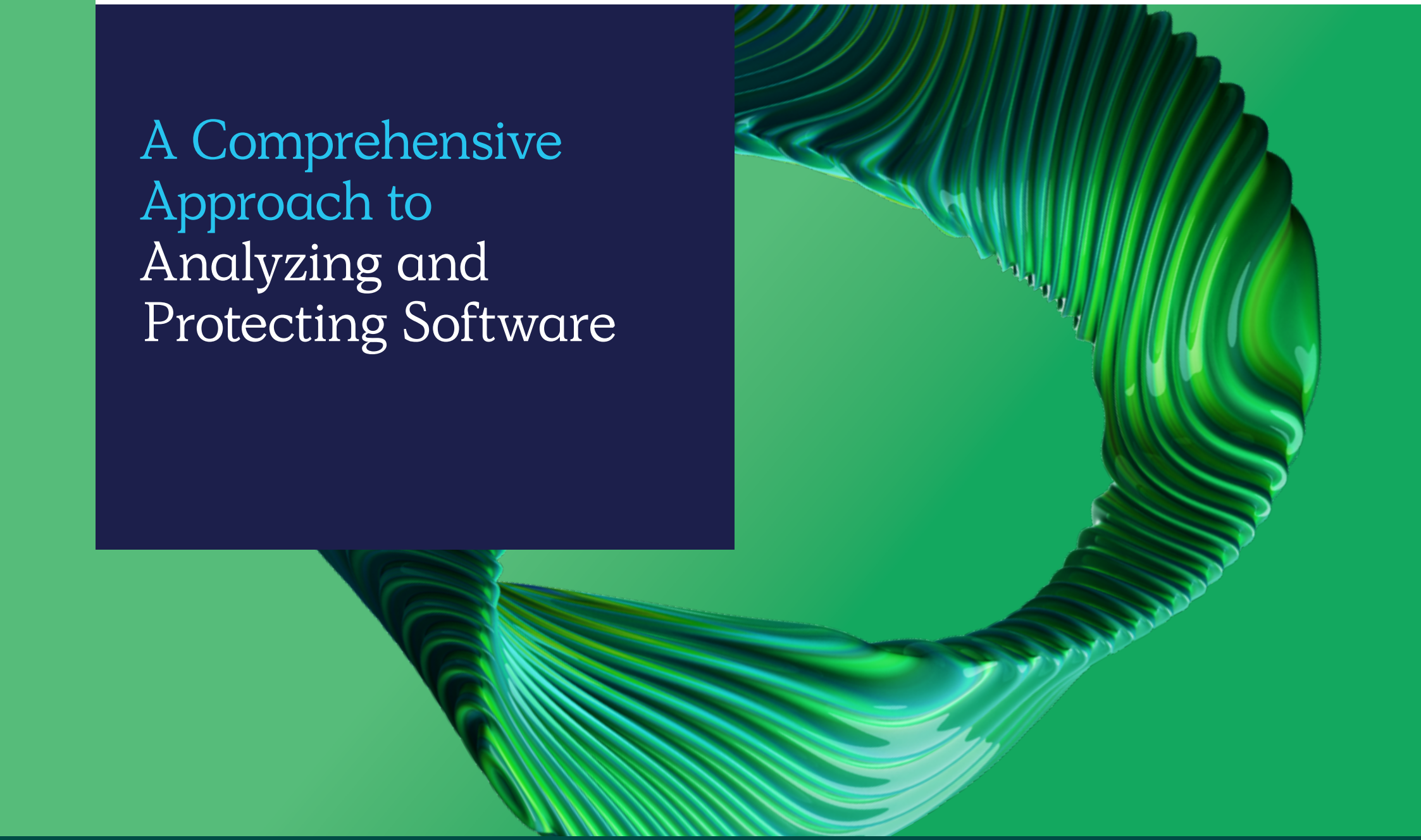
EBOOK

Contrast SECURITY

A Comprehensive Approach to Analyzing and Protecting Software



Executive Overview

Traditional approaches to application security (AppSec) rely on a patchwork of disconnected tools and processes that add more noise than protection. Organizations deploy disparate security solutions for static code analysis, dynamic code analysis, software composition analysis, and attack detection/prevention—which are ineffective in sorting actual vulnerabilities from a sea of noise caused by false positives.

This "tool swamp" adds complexity to both security operations and development pipelines. It requires multiple teams of experts to interpret results and consumes far too many resources. It frustrates developers and puts them at odds with security—impeding efforts to collaborate across teams. A unified AppSec platform that provides continuous and comprehensive security across the software development life cycle alleviates these problems. This same AppSec approach enables organizations to accelerate the release of better, stronger software while easing the burden of IT budgets and security staffing.

The AppSec tool swamp adds complexity and requires multiple teams of experts to interpret results.

Contrast SECURITY

Table of contents

01

Stuck in the AppSec Tool Swamp

While over 100 billion lines of new software code are written each year, the average number of security vulnerabilities per application has remained unchanged for the last two decades—26.7 serious problems in every release.[1] DevOps teams are well aware of the problem—only 10% of organizations report repairing critical vulnerabilities satisfactorily and in a timely manner.[2] And it's not for a lack of trying to solve the problem: The strategy for many companies to reduce application security risk is to simply stack up multiple tools and hope they do the job.[3]

When combined with a rising tide of sophisticated cyberattacks in search of easy targets, the consequences are obvious. More than half (52%) of all breaches involve hacking, and web applications are by far the most common vector for hacking-based breaches.[4]

> The combined costs of Equifax's disastrous data breach—caused | by a failure to patch a known web application security flaw—totaled over $1.38 Billion.[5]

[1] "Malware and ransomware attack volume down due to more targeted attacks," HelpNet Security, February 5, 2020.
[2] "A New Approach to Application Security Testing," Dark Reading, April 9, 2019.
[3] "AppSec 'Spaghetti on the Wall' Tool Strategy Undermining Security," Dark Reading, October 10, 2019.
[4] "2019 Data Breach Investigations Report," Verizon, April 2019.
[5] "2017 Data Breach Will Cost Equifax at Least $1.38 Billion," Dark Reading, January 15, 2020.

Contrast SECURITY

As statistics show, traditional testing methods for AppSec vulnerabilities are outdated and thoroughly ineffective. And this is due in part to the AppSec "tool swamp"—pervasive use of disconnected tools that are siloed and specific to different users. Subsequently, this kind of testing requires major staff resources for management, interpretation of results, and manual remediation. And it impedes collaborative workflows between development and security teams. Developers have often moved far beyond a specific chunk of code by the time security can offer advice regarding vulnerabilities in that section.

> More than half of organizations say that their security team has reached a tipping point where the number of security tools in place has adversely impacted their Security posture and increased risk.[6]

26.7

The number of critical vulnerabilities per application release cycle has remained the same for the past two decades.

[6] "The rise of cyber security product sprawl," Security Boulevard, March 10, 2020.

02

A Platform Offers a Unifying System

To address these problems, organizations need to integrate a solution for AppSec that unifies the objectives of development, security, and operations—a concept known as DevSecOps. Many companies have already combined development and operations into a unified organization and that promotes system thinking and collaborative workflows (i.e., DevOps). The objective of DevSecOps is to add security to that harmonious union.

> 55% of security professionals said it is difficult to get development teams to prioritize remediation of vulnerabilities—even if it's a performance metric for developers.[7]

[7] "2019 Global Developer Report: DevSecOps," GitLab, July 2019.

03

Continuous AppSec Across the Entire Life Cycle

CONTINUOUS, UNIFIED APPLICATION SECURITY

In support of achieving a functional DevSecOps organization, an instrumentation-based AppSec platform provides continuous, unified application security across the software development life cycle. It does this by giving each phase of the application life cycle what it needs to be successful.

Key elements include:

- Development gets immediate feedback in tools and processes with AppSec built into integrated development environment (IDE), development stacks, and “ChatOps” (real-time communications such as chat clients and bots) tools.
- Continuous integration/continuous deployment (CI/CD) and quality assurance (QA) teams get seamless integration with Jenkins and testing tools to ensure that a release will pass a quality gate for application security.
- Operations get integration with notification tools to provide forensics and exploit prevention for production applications.

COLLABORATION AND SYSTEMS THINKING

By doing the above, security instrumentation unifies objectives across the organization and eliminates the tool swamp of disparate and disconnected security tools. A comprehensive AppSec platform helps organize collaboration by encouraging effective participation of various stakeholders across silos. It also promotes "systems thinking" by sharing information and helping individuals in different roles broaden their perspectives.

REDUCED RISK

Perhaps most importantly, this approach drastically reduces vulnerabilities and risks from attack through interactive application security testing (IAST). Every exercise root is examined for code safety to see if the code is properly sanitizing and validating the data. If it isn't, an actual runtime vulnerability is confirmed. Traditional AppSec testing tools that use static application security testing (SAST) and dynamic application security testing (DAST) are incredibly slow because they infer vulnerabilities by building and scanning hypothetical models of source code repositories. As a result, their findings yield a high volume of false positives.

And today's problems are not limited to custom code—each year, the number of new common vulnerabilities and exposures (CVE) is increasing.[8] Instrumentation-based testing can include custom code, all libraries, and anything that reaches into the runtime.

[8] "2019 Vulnerability and Threat Trends," Skybox, February 2019.

A comprehensive AppSec platform built on instrumentation works in the same context that developers use with their native tools as they write and test software. Vulnerabilities can be continuously discovered with the flow of existing workflows. This allows for actual security vulnerabilities to be discovered and fixed in real time, the same way developers fix bugs. This enables developers to check in cleaner code from the very beginning of the application life cycle.

And because instrumentation-based AppSec goes with the application beyond development, it can continue to find vulnerabilities and help protect the application. In production, the same platform can act as an additional line of defense—embedded inside the application behind the web application firewall (WAF) as supplemental protection from within the application itself. If an attack gets past traditional perimeter protections, instrumentation-based AppSec detects and blocks threats at the point of attack inside the software code.

Security instrumentation means that security is built into the same native tools that developers use to write and test software. It also enables security to continue with the application into production.

Contrast SECURITY

04

Scalability that Reduces Risk and | Resource Burdens

The embedded nature of an instrumentation-based approach not only reduces risk but it's inherently scalable. It deploys with the application—whether it's in an IDE, with CI/CD tooling, containerization, cloud platforms, microservices, or even on-premises behind a firewall. Regardless of how an application is deployed, security goes with it.

This protection is infinitely extendible—without any additional demands on staff time or budgetary resources. This, in turn, directly reduces costs such as penetration testing, managing multiple tools, or manually checking for false positives and vulnerability remediation. Over half of cybersecurity professionals indicate their organization is at moderate or extreme risk due to staff shortages, and AppSec is an area where the gaps are the most glaring.[9]

> 69% Of organizations report their security team spends more time managing security tools than effectively defending against threats.[10]

[9] "Strategies for Building and Growing Strong Cybersecurity Teams," (ISC)2 Cybersecurity Workforce Study 2019, accessed February 10, 2020.

[10] "The rise of cyber security product sprawl," Security Boulevard, March 10, 2020.

05

Realizing Devsecops Functionality

AppSec instrumentation supports security at the speed of DevOps—scaled across an entire application portfolio within a common, unified platform. If developers are able to secure code as they work on it, this decreases the number of application defects early on in the development life cycle and helps to tighten iteration loops. This accelerates the time to market for a new product while reducing risks and costs associated with extended human workflows.

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com