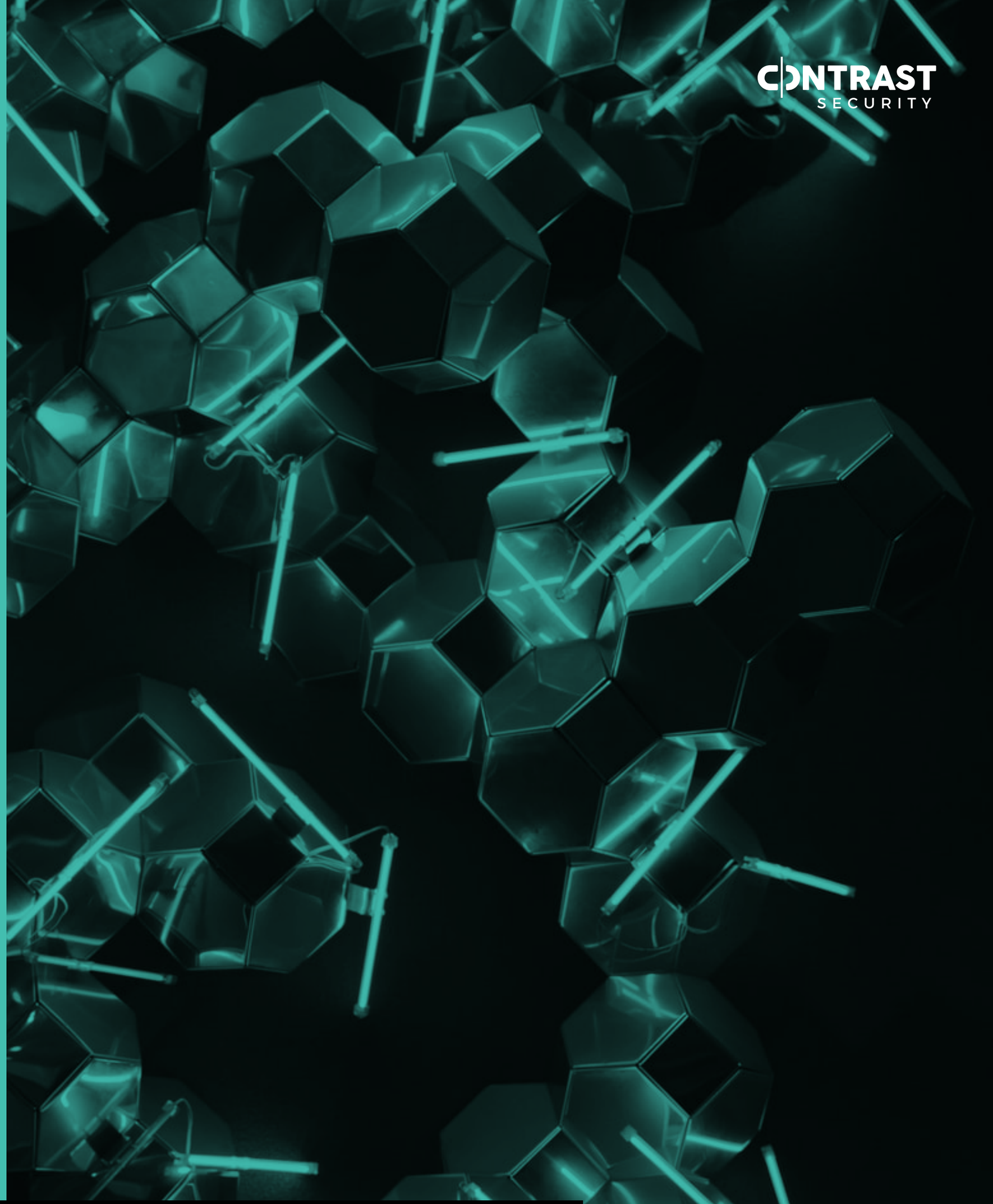

CONTRAST APPLICATION SECURITY PLATFORM

Realizing the Full Potential of DevSecOps in Modern Software

SOLUTION BRIEF

EXECUTIVE SUMMARY

Traditional application security solutions have increasingly limited effectiveness when it comes to reducing vulnerabilities in software development processes, keeping track of open-source software (OSS) components, and protecting applications in production. The Contrast Application Security Platform uses instrumentation to observe, analyze, and protect software from within the application. In doing so, Contrast makes security continuous and integrates seamlessly with modern software—from development into production. In addition, this approach offers an unprecedented application security orchestration layer to improve enterprisewide risk reporting and policy enforcement.

To compete in today's marketplace, developers must meet increasingly aggressive delivery targets for new applications. Most organizations have integrated security with DevOps and Agile processes because traditional application security tools create bottlenecks and add to project costs and delays. The vast majority of developers (91%) say that vulnerability scans take at least three hours—and 35% take eight or more hours.[1] As a result, application security is often sacrificed in order to accelerate development cycles—which creates new security problems downstream.

THE CONTRAST APPLICATION SECURITY PLATFORM INCLUDES:

- **Contrast Assess** provides continuous vulnerability assessment that integrates seamlessly with existing software development life cycle (SDLC) processes.
- **Contrast OSS** delivers automated software composition analysis (SCA) by detecting security and compliance vulnerabilities in third-party libraries and frameworks.
- **Contrast Protect** observes code behavior in running applications and intelligently blocks threats with runtime protection and observability.
- **Contrast DevSecOps Control Center** provides a comprehensive view of risk across the SDLC, and control of security policy of an application (or group of applications).

Organizations also need greater accuracy from their application security solutions to eliminate the overwhelming noise created by false-positive alerts. Traditional security based on decades-old, outside-in scanning models lacks the capabilities to discern actual threats from a sea of probes that blindly search for any chance to exploit an application. This, in turn, causes alert fatigue for security teams that are typically under-resourced. Nearly three out of four organizations (73%) report that each security alert they receive consumes an hour or more of application security time.[2]

Security must also be able to effortlessly scale with applications across all stages of the software development life cycle (SDLC)—without adding support staff or requiring any specialized security training resources. For example, many perimeter-based solutions flag every potential threat, requiring teams to spend valuable cycles on triage and verification. A more intelligent solution is needed.

A UNIFIED FOUNDATION FOR MODERN APPLICATION SECURITY

The Contrast Application Security Platform is designed to integrate with Agile and DevOps processes by operating within the application itself. Contrast leverages instrumentation to embed security within the application runtime that solves the challenges legacy application security tools present in modern software environments. This inside-out approach to application security removes the guesswork of outside-in application security tools, delivering the accuracy, efficiency, and scalability modern software demands.

Contrast offers a platform-level approach that addresses the three main shortfalls of traditional application security solutions. Contrast accelerates DevOps by removing security bottlenecks from application development, reducing the noise of false positives, and scaling security wherever an application exists across its life span without specialized security training and staff. It also provides runtime observability of application code in production to protect both known and unknown vulnerabilities from being exploited.

The Contrast Application Security Platform is comprised of three core solutions:

- **Contrast Assess** offers interactive application security testing (IAST) with elements from static application security testing (SAST) and dynamic application security testing (DAST) to automatically identify software vulnerabilities in real time while developers write code. Contrast Assess agents monitor code and report from inside the application—enabling developers to find and fix vulnerabilities without involving security experts and without specialized security expertise. In addition to removing delays in development cycles, Contrast Assess also frees up security teams to focus on providing governance.

- **Contrast OSS** detects which open-source software components are called in the application runtime and prioritizes vulnerability remediation based on which libraries are actively being used. It also helps organizations avoid unnecessary security risks or legal problems due to open-source licensing complications. Contrast OSS provides critical versioning and usage information and triggers alerts when risks and policy violations are detected. This eliminates the need for a separate assessment with different tools. There are no scans to manage and no extra steps for developers—just continuous insight.

- **Contrast Protect** uses real-time analysis of application runtime events to confirm exploitability before taking action to block an attack. This accuracy virtually eliminates the problems associated with false-positive alerts. Contrast Protect continuously detects and prevents both known threats and zero-day attacks by leveraging multi-technique precision sensors and dynamic control over the runtime. It offers an instrumentation-based approach that simplifies security deployment and scalability.

KEY PLATFORM CAPABILITIES

The Contrast Application Security Platform continuously identifies application vulnerabilities in custom and open-source code—from left in development through release to production.

> ***Contrast customers report 25% of serious vulnerabilities remediated in one day and 75% in 16 days—as compared to 19 days and 292 days, respectively, for traditional SAST application security.[3]***

ONE DEPLOYMENT

The Contrast platform offers vulnerability testing as well as protection against attacks in production through a single deployment. It can therefore present a full-stack view of application risk posture. With a single integration point, the Contrast platform delivers true DevSecOps with software composition analysis (SCA), application security testing (AST), and exploit prevention capabilities using instrumentation across the entire SDLC.

DEVSECOPS CONTROL CENTER

Only Contrast provides a true DevSecOps view of an application (or portfolio of applications) from development to production—including open-source components. Through instrumentation, the Contrast platform provides comprehensive visibility and control of software risk at every level—from a single application or microservice up to team, business unit, or even enterprisewide levels. This advantage manifests itself as two key capabilities:

- **Policy Assurance and Orchestration.** The Contrast platform offers a full life-cycle view of an application's risk, associated with open-source and custom code as well as attacks on vulnerabilities that can be exploited. This allows for enterprisewide reporting, assurance, and benchmarking of application security risk posture. This capability also allows security teams to enforce consistent, cross-SDLC software security policies across the enterprise, on a business unit, on a specific team, or across a portfolio of applications.

- **Runtime Informed Risk Posture.** This capability affords more accurate and effective vulnerability fixes, without correlating with other systems or requiring security expertise. In addition, certain cross-phase analysis techniques can greatly improve the fidelity of results (compared to stand-alone tools). Here, the Contrast platform's static analysis techniques can identify security controls and rule out exploitable flaws to strengthen the accuracy of code analysis results.

> ***With Contrast, a specific rule firing in a live application in production can inform developers to prioritize remediation of that vulnerability in development.***

ZERO-DAY DEFENSE

In production, Contrast monitors runtime data flows to detect the exact moment an attack reaches an application vulnerability. Then, before a breach can occur, it instantly blocks any exploitable runtime events without affecting the application. This includes unknown threats, new variants, and zero-day attacks that often slip past perimeter defenses (e.g., web application firewalls), directly exposing internal application stacks to exploitation.

Contrast's runtime protection capabilities offer two critical benefits. First, it provides "air cover" protection against a vulnerability in the application until a patch is released or developers can fix the issue. Second, it discovers and defends against open-source and zero-day exploits that do not have a patch or fix.

SECURITY AT THE SPEED OF DEVOPS

The Contrast platform aligns development and security efforts from design to production, applications new and old. It helps teams unblock the SDLC by finding true vulnerabilities in real time. It turns developers into security experts with developer-friendly "how-to-fix" guidance and prebuilt command-line interface (CLI) tools. It provides production air cover that allows organizations to ship securely, even with open vulnerabilities. And it defends against zero days and unpatched libraries with runtime protection.

---

[1] "The State of DevSecOps Report," Contrast Security, December 2020.

[2] "The State of DevSecOps Report," Contrast Security, December 2020.

[3] "2020 Application Security Observability Report," Contrast Security, June 17, 2020.

CONTRAST SECURITY

240 3rd Street
Los Altos, CA 94022
888.371.1333