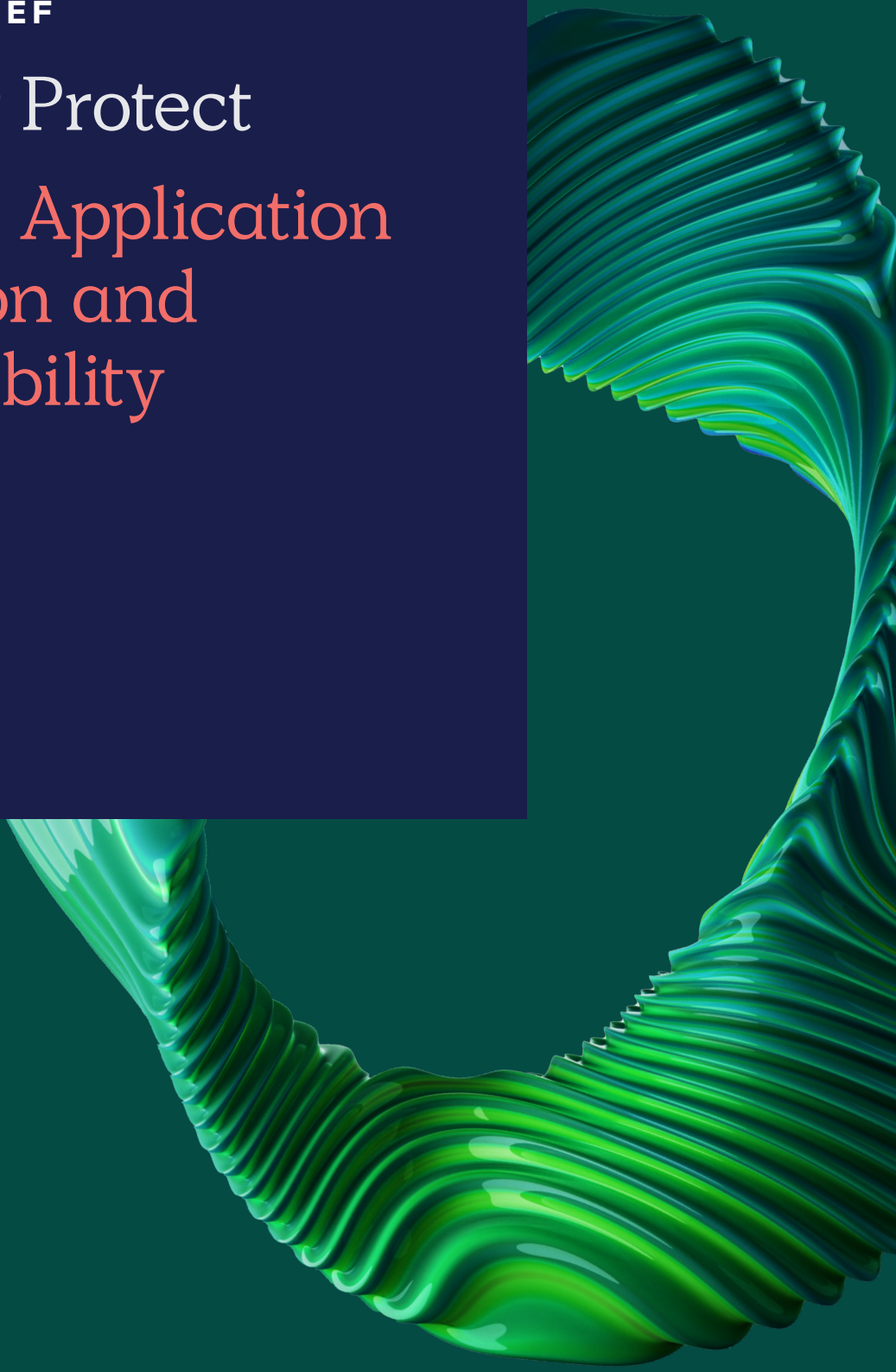
Contrast SECURITY

SOLUTION BRIEF

Contrast Protect

Runtime Application Protection and Observability



Executive overview

Web applications and application programming interfaces (APIs) continue to be a leading attack vector for expensive, reputation-damaging breaches. And security leaders have struggled to mount effective protection against both known and unknown threats by relying solely on perimeter-based application security solutions that include web application firewalls (WAFs). Not only that, but the cost of trying to do so—in human and financial terms—is untenable.

While perimeter solutions provide necessary network-layer protections, security leaders also need application-layer visibility into how vulnerabilities are impacted as they are exposed to actual threats in runtime. Only this type of observability, in the runtime context, enables targeted blocking of business-impacting threats and optimized allocation of DevOps resources in fixing the associated vulnerabilities.

Contrast Protect is a runtime application protection and observability solution that uses real-time analysis of application runtime events to con rm exploitability before taking action to block an attack. Leveraging both multitechnique precision sensors and dynamic control over the runtime, Contrast Protect maximizes detection and protection against known and unknown threats, while virtually eliminating false-positive alerts. Easy to deploy and running continuously in applications wherever they reside, Contrast Protect aligns with modern DevSecOps processes, facilitating rapid, cost-effective application scalability with security compliance.

Effective protection from the inside

Contrast Protect works by means of software instrumentation through agents, which introduce observability and control elements into the binary (runtime) code. These agents deploy easily, in minutes, from the Contrast web dashboard, without requiring security or development staff to make any changes to the source code.

> *For the past two decades, the average number of security vulnerabilities per application has remained unchanged—26.7 serious problems in every release.[1] In 2020, 43% of data breaches were attacks on application vulnerabilities,[2] which is more than double the percentage from the previous year.[3]*

Contrast SECURITY

Once deployed, Contrast Protect provides continuous protection through Runtime Exploit Prevention™. This unique, multistep approach analyzes application runtime events and confirms exploitability, improving the likelihood of thwarting zero-day attacks by detecting and automatically blocking breach attempts during real-time code execution within the application runtime. This all happens in sub-millisecond time frames, even under the heaviest attack loads.

Contrast Protect detects the top threats identified by the Open Web Application Security Project (OWASP) and all other common attack classes. It also provides observability across the entire application stack, including the binary code, custom and open-source libraries and classes, and APIs. By providing this deeper visibility, Contrast Protect detects and blocks attacks that perimeter defenses often miss. Through built-in integrations with security information and event management (SIEM) systems, Contrast Protect also enhances the accuracy of security analysis.

> *Even under the heaviest attack load, Contrast Protect provides sub-millisecond protection. There is no faster way to enforce security policy.*

GET A WIN WITH DEVELOPERS: UP AND RUNNING IN THREE CLICKS, IN THE WAY DEVELOPERS KNOW AND LOVE

Contrast Protect not only protects effectively but it also does so efficiently, discerning between real, impactful attacks and probes that do not reach a targeted vulnerability. For example, if a SQL injection attack alters the expected syntax of a SQL query, Contrast Protect instantly blocks this exploitable runtime event without affecting the application before a breach can occur and sends an alert to the SIEM system. Conversely, if a SQL injection attack never reaches a SQL query, Contrast Protect recognizes this as a harmless probe, does not block it, and does not trigger a false-positive alert in the SIEM system.

Since harmless probes constitute the majority of application attacks,[4] Contrast Protect can help security and development teams avoid spending numerous hours fixing low-value vulnerabilities and possibly disrupting business operations through application downtime.

> *Alert fatigue is the enemy of SecOps talent retention. The global cybersecurity workforce (including application security) needs to grow by 89% worldwide to meet the current demand for skilled talent.*[5]

The reduction in false positives also significantly reduces SecOps alert fatigue, which is a major area of concern for security leaders. In addition to increasing the risk of dangerous oversights by an exhausted team, alert fatigue also leads to burnout and high turnover in a professional field that already faces a persistent skills shortage.

Contrast SECURITY

SIMPLIFIED DEPLOYMENT PRESERVES STAFF RESOURCES

Security teams that work with WAFs and other perimeter tools are accustomed to the deployment of hardware or software devices, as well as to network configuration changes to reroute traffic through the WAF. Static perimeter rules must be updated regularly to ensure they are appropriately tuned to the right traffic. This setup, tuning, management, maintenance, and troubleshooting across SecOps, DevOps, and networking departments is time-consuming and ultimately very costly. For example, in one survey of security professionals, 30% of respondents found it difficult to alter WAF policies to guard against new web application attacks.[6]

Contrast Protect, on the other hand, is deployed within the application runtime. It knows all the contextual information about how the application is configured and how transactions and flows move inside the runtime. This allows Contrast Protect to be deployed in blocking mode straight out of the box, with minimal deployment effort.

With Contrast Protect, security becomes part of the usual and standard application deployment process without additional implementation steps or business interruption. Contrast Protect then works wherever the application runs—in the data center or in the cloud, on physical servers, virtual machines, or containers. This always-on, embedded simplicity greatly reduces setup effort and costs—which in turn enables development teams to move more quickly and re-architect solutions without compromising on security.

ELASTIC APPLICATION SECURITY SCALABILITY ACROSS THE ENTIRE PORTFOLIO

Because Contrast Protect is instrumented into the runtime code, it stays with the code through version upgrades, ports to different operating systems, migrations to and from cloud environments, and other changes.

For example, if an application creates copies of itself on multiple server instances to serve a distributed user base, Contrast Protect will seamlessly scale within every instance of an application in complete lockstep—all without configuration or tuning, no matter where the application is deployed. Additionally, if placed on virtual or cloud servers, Contrast Protect can leverage the added CPU and memory resources right alongside the application.

> *Whatever code you run, Contrast has your back. Contrast Protect supports Java, .NET, Python, Ruby, Node, NGINX, and Golang.*

Contrast SECURITY

ENABLES COMPLIANCE WITH MAINSTREAM STANDARDS

Maintaining compliance with the latest industry standards and government regulations helps organizations keep pace with an evolving threat landscape and adhere to minimum best practices for security and network infrastructure—including deployed application security defenses.

As an instrumentation-based runtime protection and observability solution, Contrast Protect helps organizations comply with mainstream industry standards such as the National Institute of Standards and Technology (NIST) and the Payment Card Industry Data Security Standard (PCI DSS). The latest releases of these standards require state-of-the-art security instrumentation for "application self-protection at runtime" to reduce the susceptibility of software to attacks by monitoring inputs and blocking those inputs that could allow attacks.[7]

Contrast puts protection where applications need it most

As a complement to WAFs and other traditional perimeter defenses, Contrast Protect instrumentation-based runtime application protection and observability provides visibility, accuracy, ease of deployment, and instant scalability for applications. Contrast Protect helps organizations protect application vulnerabilities from both internal and external attacks in real time and eliminates the false positives that squander security staff resources. Additionally, it helps organizations stay compliant with emerging industry standards for effective and modern application security.

> *"NIST's SP 800-53B publications include a safeguard standard SI-7 (17), which requires state-of-the-art runtime application self-protection.[8]*

Contrast SECURITY

[1] "Malware and ransomware attack volume down due to more targeted attacks," Help Net Security, February 5, 2020.
[2] "2020 Data Breach Investigations Report," Verizon, May 2020.
[3] "2019 Data Breach Investigations Report," Verizon, April 2019.
[4] "Contrast Labs Application Security Intelligence Report: January-February 2020," Contrast Security, March 2020.
[5] "Cybersecurity Professionals Stand Up to a Pandemic: (ISC)2 Cybersecurity Workforce Study 2020," (ISC)2, 2020.
[6] "International Cyber Benchmarks Index, May 2020 Survey Results," Neustar International Security Council, May 2020.
[7] "AppSec Solution Guide for Complying with New NIST SP 800-53 IAST and RASP Requirements," Contrast Security, March 2020.
[8] "Control Baselines for Information Systems and Organizations," NIST, October 2020.

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