Contrast
SECURITY

SOLUTION BRIEF

Contrast Application Security Platform

Unifying Observability, Assessment, and Protection for Federal Agencies

Executive summary

Traditional application security tools have increasingly limited the effectiveness of federal agencies when it comes to reducing vulnerabilities in software development. The Contrast Application Security Platform analyzes applications for vulnerabilities and protects them from being exploited in production. This approach dramatically improves application security accuracy and efficiencies—from development into production.

In today's federal agencies, developers must meet increasingly aggressive delivery targets for new applications. Most agencies have seen an increase in DevOps and Agile process timelines because traditional application security tools stress application release cycles—adding to project costs and triage delays. As a result, application security is often sacrificed in order to accelerate development cycles—which creates security risks downstream.

Federal agencies also need greater accuracy from their application security solutions to eliminate the overwhelming noise created by false positives. Security teams currently spend 25% of their time chasing false positives.[1] Traditional security based on decades-old scanning models lack the capabilities to discern actual threats from a sea of probes that blindly search for any chance to exploit an application. Instead, security must be continuous and effortlessly scale with applications across all stages of the SDLC—without adding specialized security staff or training.

A unified foundation to support modern federal application security

The Contrast Application Security Platform is signed to integrate with Agile and DevOps processes by operating within the application itself. Contrast embeds security within the application runtime that solves the challenges legacy application security tools present to federal agencies 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 federal agencies require.

The Contrast Application Security Platform Includes:

Contrast Assess provides continuous vulnerability assessment that integrates seamlessly with existing software development life cycle (SDLC) processes.

Contrast SCA delivers automated software composition analysis (SCA) by embedding security and compliance controls in open-source applications.

Contrast Protect automatically reduces false positives and developer backlogs with runtime protection and observability.

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

Contrast Assess uses code instrumentation to embed sensors inside the application, as it's running, and watches every line of code that gets called inside the application. By doing so, it automatically finds vulnerabilities that legacy static application security testing (SAST) tools find and provides valuable information that dynamic application security testing (DAST) tools provide. Contrast Assess accomplishes this without attacking the application and jeopardizing data integrity. Contrast finds vulnerabilities instantaneously as the application is being written by developers.

Contrast SCA detects which open-source and closed-source software components are called in the application runtime, if they are vulnerable, and whether they expose the mission to unnecessary security risks or legal problems due to licensing complications. Contrast SCA provides critical versioning and exact class 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 intelligence and visibility.

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. In addition, Contrast Protect continuously detects and prevents known and zero-day attacks by leveraging both multi-technique precision sensors and dynamic control over the runtime. It offers an instrumentation-based approach that simplifies security deployment and scalability.

Key capabilities

The Contrast Application Security Platform continuously identifies application vulnerabilities in custom and open-source code that legacy application security tools miss and protects from zero-day attacks that put federal agencies at risk. Contrast accelerates processes by removing security bottlenecks from application development, reduces triage and remediation expenses of false positives, and scales security wherever an application exists across its life cycle.

OBSERVABILITY

Because the Contrast Application Security Platform operates from inside the application itself, it can monitor all the parts of the application in runtime, including custom code, application programming interfaces (APIs), and open-source libraries. This occurs regardless of where the application is running—containers, microservices, and cloud. This deep visibility enables Contrast to focus on the vulnerabilities that actually matter, ignoring the vast sea of noise created by probes searching to exploit weaknesses that often do not exist.

ASSESSMENT

Contrast uses instrumentation to automatically pinpoint and prioritize critical software vulnerabilities. This approach provides the highest accuracy, efficiency, and coverage possible. By embedding sensors inside applications, departments can "shift left" and discover vulnerabilities earlier in the SDLC. Here, developers gain efficiency and effectiveness by detecting and remediating problems with virtually no false positives.

PROTECTION

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. In addition to known vulnerabilities, these include unknown threats, variants, and zero-day attacks that often slip past perimeter defenses (e.g., web application firewalls) and directly expose internal application stacks to exploitation.

COMPLIANCE AND INDUSTRY STANDARDS FOR FEDERAL AGENCIES

Federal agencies are mandating National Institute of Standards and Technology (NIST) and other industry standards for application security. Regulatory and compliance guidelines acknowledge that legacy application security tools are unable to address the advanced threat landscape risking agency missions. NIST 800-53, PCI DSS, PA-DSS, and the PCI Security Framework specifically call out interactive application security testing (IAST) while the OWASP Top 10 documents security risks as a vital, needed solution to continuously combat modern software threats affecting federal agencies in today's modern software era. The Contrast Application Security Platform is compliant with Security Technical Implementation Guides (STIGs) and Risk Management Framework (RMF) and is certified and authorized to operate (ATO) via Platform One.

> Contrast is certified on platform one and its containers are accessible through the Iron Bank.

Security at the speed of devops

Contrast automatically identifies and diagnoses applications and APIs by using instrumentation to pinpoint and prioritize software vulnerabilities while protecting deployed and legacy applications from zero-day attacks. Embedding sensors inside the applications enables agencies to shift left, empowering teams using DevOps and Agile to write clean code and dramatically reduce security incidents. This also extends security "right" to protect applications in production runtime.

GOVERNMENT VEHICLES

NIST 800-53 REVISION 5 COMPLIANT

CERTIFIED ON PLATFORM ONE

CERTIFIED TO FIELD (CTF) ON PLATFORM ONE

SOC2 TYPE II

[1] "Ponemon Institute Reveals Security Teams Spend Approximately 25 Percent of Their Time Chasing False Positives; Response Times Stymied by Legacy Tools," Exabeam, August 1, 2019.

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

Contrast
SECURITY

contrastsecurity.com