Contrast SECURITY

SOLUTION BRIEF

How Contrast Security Supports And Improves Government Reference Designs

Executive Overview

Federal agencies like the Department of Defense develop software for a variety of missions in accordance with published government reference design guidelines.[1] But as application teams embrace modern development environments (e.g., DevOps, Agile) to improve speed and effciency, de facto application security tools are causing workflow bottlenecks while missing critical vulnerabilities in the code. Contrast Security's Application Security Platform was designed for these modern environments, securing the entire software development life cycle (SDLC). It improves the productivity of DevOps teams, accelerates operations, reduces risks, and streamlines compliance obligations—including federal reference design recommendations.

LEGACY TOOLS PUT APPLICATION DEVELOPMENT AND DEFENSES IN JEOPARDY

Applications were the most common breach pattern in the public sector last year.[2] Like most federal agencies, the Department of Defense (DoD) still relies on penetration testing and scanning tools for application security. Periodic and partial application scans from static application security testing (SAST) and dynamic application security testing (DAST) tools do not support current government agency requirements for continuous security.

More importantly, these legacy practices do not provide the agility to deploy new software at the speed of operations. At the same time, security remains an afterthought—not built into the SDLC and underlying infrastructure.[4] There are also varying layers of underlying software between the development and production environments that create complexity and elevate the risk of a breach. Human workflow dependencies with these tools further increase process inefficiencies and are prone to errors.[5]

> *"Traditional application security approaches cannot keep pace with the speed of modern Agile and DevOps. Constant security scans slow release cycles and increase developer inefficiencies.[3]*

Developers at government agencies need a modern, instrumentation-based approach to application security in order to improve DevOps productivity, accelerate operations, reduce risks, and streamline compliance obligations and continuous authority to operate (ATO). The Contrast Application Security Platform offers this approach, embedding comprehensive security capabilities across the entire SDLC of public sector applications.

Contrast SECURITY

MEETING AND EXCEEDING GOVERNMENT REGULATIONS

The need for security modernization through innovation is called out several times in the DoD Enterprise DevSecOps Reference Design.[6] The Contrast Application Security Platform supports and improves upon the recommendations for security tools and processes outlined in these guidelines. Contrast's platform has been certified for use in Platform One and is available in the Iron Bank DoD Centralized Artifacts Repository (DCAR).7 These certifications offer continuous ATO, support requirements for setting up software factories, and enhance application development.

THE CONTRAST APPLICATION SECURITY PLATFORM SUPPORTS SYSTEMS INTEGRATORS THAT ARE:

- Building or needing to harden containers
- Managing or building software factories
- Using software factories or developing/securing/operating mission applications
- Requiring continuous ATO for customer applications

The Contrast Application Security Platform can replace minimum viable products (MVPs) such as outdated SAST/DAST tools. Contrast's application security solution for vulnerability assessment provides testing with greater speed, higher accuracy, better scaling, lower manpower requirements, and more advanced automation features than legacy SAST/DAST products. This combination enables Contrast to meet and exceed government requirements for continuous security, including:

- Placing multiple sensors inside the application
- Testing invoked lines of application code to find static analysis vulnerabilities, such as hardcoded passwords, or insecure hashing algorithms
- Automatically recognizing all open-source and custom libraries used inside the application, showing all Common Vulnerabilities and Exposures (CVEs) and which applications use the aforementioned libraries

ACHIEVING TARGET BENEFITS AND MAINTAINING BUDGETS

The Contrast Application Security Platform provides comprehensive security across all phases of the SDLC, while eliminating both the workflow and performance bottlenecks caused by legacy security scan tools. This improves the culture of DevOps organizations and delivers tangible business outcomes for the software building efforts. Contrast's platform enables all of the DoD's targeted benefits for DevSecOps implementation, including:

- **Reduced mean-time-to-production**—the average time it takes from when new software features are required until they are running in production
- **Increased deployment frequency**—how often a new release can be deployed into the production environment
- **Fully automated risk characterization, monitoring, and mitigation** across the SDLC
- **Software updates and patching** at "the speed of operations"
- **Support for weapons systems, financial, health**, and other mission-critical DoD use cases

AUTOMATION THAT INCREASES DEVSECOPS EFFICIENCY

The DoD's reference design guidelines define DevSecOps stages that include develop, build, test, and operate; they also state when security testing and monitoring should be performed.[8] Static code analyzers run when the application process is stopped, necessitating that separate scans be performed at each stage. While these can be automated to some degree, it is still an out-of-pipeline procedure, which inherently causes delays. Perhaps more importantly, these static scans throughout the code build only test for what has changed (delta), which means that organizations still need to do a full scan at the end.

> *A single application typically requires hundreds of scans during development.*[9]

Contrast SECURITY

Disaggregated approaches to application security that patch together products from different vendors also require additional tooling and solutions to cover individual security gaps—separate, siloed solutions that may include SAST, DAST, software composition analysis (SCA), penetration testing, web application firewalls (WAFs), and fuzzing. While all of those security capabilities are valuable, the lack of integration between solutions makes automated workflows and coordinated security responses much more difficult to achieve.

Contrast's platform is an integrated, purpose-built solution with centralized configuration, user interface (UI), and policy enforcement. Contrast's application security instrumentation is deployed only once at the start of development. From that point forward, it automatically monitors the application at all times, and throughout all stages of the continuous integration/continuous development (CI/CD) pipeline. In doing so, Contrast provides true continuous application security. The integrated Contrast platform approach eliminates the need for individual tools in silos, while simplifying automation for reduced resource strain and better overall application protection.

GREATER ACCURACY, BETTER PERFORMANCE

Because legacy tools scan inactive code, they also miss out on the interaction of the application process. They "guess" at how an application might run—which causes high volumes of vulnerability false positives as well as false negatives. The DoD's reference design guidelines highlight the inefficiencies of outmoded SAST and DAST solutions.[11]

Contrast's platform is not only continuous but also comprehensive. It reviews all of the distributed parts of an application during runtime—including application programming interfaces (APIs), custom code, and open-source frameworks and libraries. Nothing is missed and almost zero false positives are created.[12]

> *"Government agencies can deliver higher performing and better quality applications by embedding automated security controls and tests into their pipelines. They can also avoid bottlenecks and deliver capabilities faster by automating the tasks and approval gates that really don't need a human in the loop.*[10]

Contrast SECURITY

FORWARD-LOOKING COMPLIANCE WITH NIST STANDARDS

The National Institute of Standards and Technology (NIST) released a revision to Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Revision 5. Those responsible for application security need to capitalize on two new standards that address both **interactive application security testing (IAST)** capabilities as well as **runtime application self-protection (RASP)**.[13] As security instrumentation is pivotal to both IAST and RASP, it enables a comprehensive approach to application security that starts in development and extends into production runtime.[14]

The Contrast Application Security Platform includes both IAST and RASP functionality to cover the security gaps of stand-alone, legacy scanning tools. And while only some of these new NIST recommendations are currently required in the DoD reference design guidelines, Contrast's solution meets and exceeds those requirements.[15]

SIMPLIFIED MANAGEMENT AND OPERATIONS

Unlike siloed SAST and DAST tools, Contrast's platform requires no additional tooling or automation controls when being added to the application pipeline. No special programs or designs are required and Contrast doesn't need to be maintained, adapted, or redeployed when the application version changes. In containerized DevOps environments, Contrast instrumentation agents are part of the application code, which means they continue to provide all essential security functions inside containers. Other security products need to make use of a sidecar security container. Beyond the inherent security issues of using sidecars, they can quickly lead to problems with application stability and performance.[16]

CONTRAST SECURITY INCREASES DEVSECOPS VALUE FOR GOVERNMENT AGENCIES

The Contrast Application Security Platform exceeds the DoD guidelines for MVPs and objective technologies. In comparison to the legacy de facto application security solutions in place at many government agencies and departments today, Contrast offers better detection, protection, and greater accuracy while requiring fewer resources to install, operate, and maintain. Best of all, it offers a better return on investment versus siloed approaches to application security.

Contrast SECURITY

[1] "DoD Enterprise DevSecOps: Reference Design," U.S. Department of Defense, September 12, 2019.
[2] "2020 Data Breach Investigations Report," Verizon, June 2020.
[3] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.
[4] "DoD Enterprise DevSecOps: Reference Design," U.S. Department of Defense, September 12, 2019.
[5] John Morello, "Shift Left: DevSecOps and the Path to Continuous Authority to Operate," Nextgov, July 27, 2020.
[6] "DoD Enterprise DevSecOps Reference Design," United States Department of Defense, September 12, 2019.
[7] "Platform One: DoD Enterprise DevSecOps Services," United States Air Force, accessed October 27, 2020.
[8] "DoD Enterprise DevSecOps: Reference Design," U.S. Department of Defense, Septmeber 12, 2019.
[9] "State of Software Security," Veracode, October 2020.
[10] Michael Wright, "How DevSecOps Helps the U.S. Federal Government Achieve Continuous ATO," The New Stack, April 7, 2020.
[11] "DoD Enterprise DevSecOps Reference Design," United States Department of Defense, September 12, 2019.
[12] "Contrast Security Scores High Marks Running OWASP Benchmark," Contrast Security, accessed October 27, 2020.
[13] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.
[14] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.
[15] Derek Rogerson, "What You Need to Know About the New IAST and RASP Guidelines in NIST 800-53," Contrast Security, March 19, 2020.
[16] Apurva Dave, "5 Things We've Learned About Monitoring Containers," DZone, August 14, 2017.

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

Contrast SECURITY

contrastsecurity.com