EBOOK

Contrast SECURITY

Federal Agencies Must Transition to Instrumentation-Based Application Security

Executive Overview

Like any other organization, federal agencies depend on software development for a variety of critical operations. With the adoption of modern DevOps and Agile environments, outdated application security tools cause workflow bottlenecks while missing critical vulnerabilities that could lead to a breach. Developers in the public sector need a modern, instrumentation-based solution for application security that spans the entire life cycle of the code it produces. An effective solution should help improve development teams' productivity, accelerate operations, reduce risks, and streamline federal compliance obligations.

> Applications were the most common breach pattern seen last year in the public sector. Across all verticals, the percentage of overall data breaches tied to Application vulnerabilities doubled over the past year—hitting 43%.[1]

[1] " 2020 Data Breach Investigations Report," Verizon, June 2020.

Contrast SECURITY

Table of contents

01

Federal Software Development must Eliminate Security Roadblocks

Application development teams in federal agencies are facing bottlenecks because of a back-and-forth workflow between security (testing) and development (remediation). The main problem stems from legacy tools such as penetration testing and scanning. These require human experts to run, analyze results, and make recommendations before developers can begin to remediate an issue.

This inefficiency creates delays that may disrupt broader mission objectives. Even with Agile and DevOps processes in place, the Federal IT Dashboard shows the average project duration is almost 500 days.[3] Developers need effective application security that integrates into their integrated development environments (IDEs) and continuous integration/continuous development (CI/CD) tools.

> Outdated security testing can cause significant workflow delays—17 hours per week for each developer.[2]

[2] "The Developer Coefficient: a $300B opportunity for businesses," Stripe, September 2018.

[3] Jason Miller, "DevOps methodology helps agencies achieve citizen expectations," Federal News Network, January 8, 2020.

02

Application Security must Drive Efficiency and Productivity

Development teams are measured in terms of velocity and the value they add; application security must enable rather than inhibit these outcomes.[4] But the vast majority (79%) of developers today spend too much time triaging and diagnosing alerts—including false positives (69%), for which legacy application security tools are notorious.[5] With an ongoing shortage of skilled cybersecurity candidates, federal agencies often need to find ways to reduce application vulnerabilities without hiring more staff to manage the problem.

To account for this, a modern application security solution needs to embed directly into the CI/CD pipeline to automatically identify and diagnose software vulnerabilities—enabling organizations to develop and release secure software faster. The solution's specific capabilities should cover:

- **Accurate detection and prioritization of vulnerabilities** to greatly reduce the false positives that cause alert fatigue
- **Automated vulnerability management** that improves security awareness across the entire development life cycle with automated application runtime observability and application security telemetry

> "Government entities typically face greater risk exposure than most private sector companies—and often with fewer resources to recruit skilled cybersecurity talent.[6]

[4] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.
[5] "A Major Roadblock to Business Innovation: How Traditional AppSec Delays DevOps Release Cycles," Contrast Security, April 30, 2020.
[6] Paulette Perhach, "The Mad Dash to Find a Cybersecurity Force," The New York Times, November 7, 2018.

This kind of accuracy and Agile and DevOps automation can be possible through instrumentation—security that is placed inside the application itself. As a result, security instrumentation eliminates development delays connected to security scans and false positives that incur significant inefficiencies.[8] Federal agencies can deliver higher performing and better quality applications by embedding automated security controls and tests into their development pipelines. They can also avoid bottlenecks and deliver capabilities faster by automating the tasks and approval gates that really do not need a human in the loop.[9]

> If security is not integrated at the front end of software development, agencies that use agile and devops must repeat long development cycles by putting security in place at the end of the process.[6]

[7] Phil Goldstein, "NIST Considers DevSecOps Framework for Agencies," FedTech, April 7, 2020.
[8] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.
[9] Michael Wright, "How DevSecOps Helps the U.S. Federal Government Achieve Continuous ATO," The New Stack, April 7, 2020.

03

Agencies Need Security that is Accurate, Fast, Scalable, and Deployable

Effective application security must also be easy to deploy and manage—providing agility to keep pace with mission objectives. The solution must also be able to seamlessly scale within and across agencies and departments. To provide this, the solution must support interoperability with existing workflow tools as well as any planned Agile and DevOps infrastructure changes.

Complexity is the enemy of any security solution. Simplicity promotes speed, accuracy, and agility. Therefore, the solution needs to be an integrated platform—rather than an assembly of disaggregated tools that cannot seamlessly communicate or coordinate responses. And it should be built for the dynamic and modularized nature of modern applications with an "inside-out" (embedded) solution to analyze data flows in real time.

> Instrumentation empowers developers to build and release secured applications that are protected from errors or malicious activity—all while removing code halt Delays for manual line-by-line security testing.[10]

[10] Derek Rogerson, "What You Need to Know About the New IAST and RASP Guidelines in NIST 800-53," Security Boulevard, March 19, 2020

04

Eliminating Risks Against Known and Unknown Threats

To effectively mitigate risks, application security must improve security awareness across the entire software development life cycle (SDLC) using orchestrated application runtime observability and application security telemetry. These capabilities should include:

- Continuous, real-time monitoring and protection for both custom and open/closed source applications and application programming interfaces (APIs) (including legacy applications)
- Blocking attacks on exploitable vulnerabilities
- Vulnerability management that is fast, easy, and prioritized based on risk
- Visibility into the status of the application health (e.g., using a "scorecard" display)

An instrumentation-based approach to application security can support all of these critical needs. Instrumentation makes applications more resilient to cyberattacks, limits the damage that attacks can inflict, and protects the security and privacy of sensitive information.[11]

> "Instrumentation's "inside-out" approach reduces risk by enabling development teams to quickly address vulnerabilities that matter and respond to attacks by preventing vulnerabilities from being exploited in real time.[12]

[11] Derek Rogerson, "What You Need to Know About the New IAST and RASP Guidelines in NIST 800-53," Security Boulevard, March 19, 2020.
[12] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.

Contrast SECURITY

05

Certification, Compliance Validation, and ATO

It is also essential that the solution supports all certification, compliance validation, and authority to operate (ATO) requirements that may apply to the agency. To prove compliance with any combination of evolving requirements that apply to public sector applications, security teams need transparency and useful insights at every step of the SDLC—without waiting for developers to generate and share reports post-development.[13]

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 interactive application security testing (IAST) and runtime application self-protection (RASP).[14] 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.[15]

Instrumentation can also help organizations comply with security and regulatory standards such as NIST, Payment Card Industry Data Security Standard (PCI DSS), Open Web Application Security Project (OWASP), Security Technical Implementation Guides (STIGs), and Risk Management Framework (RMF).

> All U.S. Federal government agencies are now mandated to comply with nist, and many state, local, territorial, and tribal governments have followed suit.[16]

[13] Michael Wright "How DevSecOps Helps the U.S. Federal Government Achieve Continuous ATO," The New Stack, April 7, 2020.
[14] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.
[15] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.
[16] Derek Rogerson, "What You Need to Know About the New IAST and RASP Guidelines in NIST 800-53," Security Boulevard, March 19, 2020.

Contrast SECURITY

06

Instrumentation Enables a True Devsecops Environment

It is now critical to involve security in pipeline-related discussions to ensure that the right security steps are built in from the beginning.[17] An instrumentation-based approach to application security allows federal agencies to code securely and efficiently in a continuous manner, while reducing risk across the entire SDLC. It empowers development, operations, and security teams to improve their application risk posture while significantly improving business outcomes.

For developers: Effective application security must be capable of discovering custom and open/closed source applications and API vulnerabilities so they can be fixed during the SDLC.

For security: The solution must continuously monitor and protect from zero-day attacks/exploits while freeing limited security staff to work on more strategic initiatives.

For operations (SecOps): The solution must reduce time to delivery/implement/deploy and also streamline reporting and compliance workflows.

For division chiefs, department heads, and high-level management: Embedding security instrumentation within the application eliminates the current need to hire additional security experts, which reduces total cost of ownership (TCO). An effective solution should also offer an immediate scorecard of application vulnerabilities with priority levels for remediation.

[17] Michael Wright, "How DevSecOps Helps the U.S. Federal Government Achieve Continuous ATO," The New Stack, April 7, 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