SOLUTION BRIEF

The U.S. Department of Defense Is Expanding Its Security Framework to Include Continuous Monitoring Controls

Transitioning to a Continuous Authorization to Operate framework.

Government and federal agencies have long observed the National Institute of Standards and Technology's (NIST's) Risk Management Framework for security frameworks to help agencies select suitable safeguards relating to cybersecurity, privacy and supply-chain risk management.

One critical component for IT officials to assess risk and deliver new information systems is authorization to operate, or ATO. At the core, ATOs served as sign-offs given to IT systems, where officials consider the inherent risk in deploying them acceptable enough for them to be used. The Defense Department has recently indicated that it is time to move toward a framework known as continuous authorization to operate, or cATO.

On Feb. 4, 2022, the Pentagon issued a memo that described the benefits of using cATOs, which the memo notes represent a "challenging but necessary enhancement of our cyber risk approach to accelerate innovation while outpacing expanding cybersecurity threats." The goal is for this framework to allow for continuous monitoring and assessment of systems so that any potential weaknesses can be quickly identified and addressed before they become an issue.

To achieve continuous monitoring of security system controls within IT systems, officials must show that real-time or near-real-time cybersecurity countermeasures and a secure software supply chain can be deployed. The memo also stated that the Defense Department's framework should allow for effective monitoring of critical security controls within IT systems, including a secure software supply chain.

Additionally, cATOs are seen as providing more realistic checks of how cybersecurity functions in real-world conditions since they are based on current known vulnerabilities rather than what was known at the time security teams made assessments months or years ago. ATOs were traditionally allocated for three years and renewed every three years based on updated security requirements,

Continuous ATOs are sometimes referred to as ongoing authorizations based on a "full security authorization package and the results of defined continuous monitoring activities that security teams can use to determine changes in risk and risk acceptance determinations made by authorizing officials."

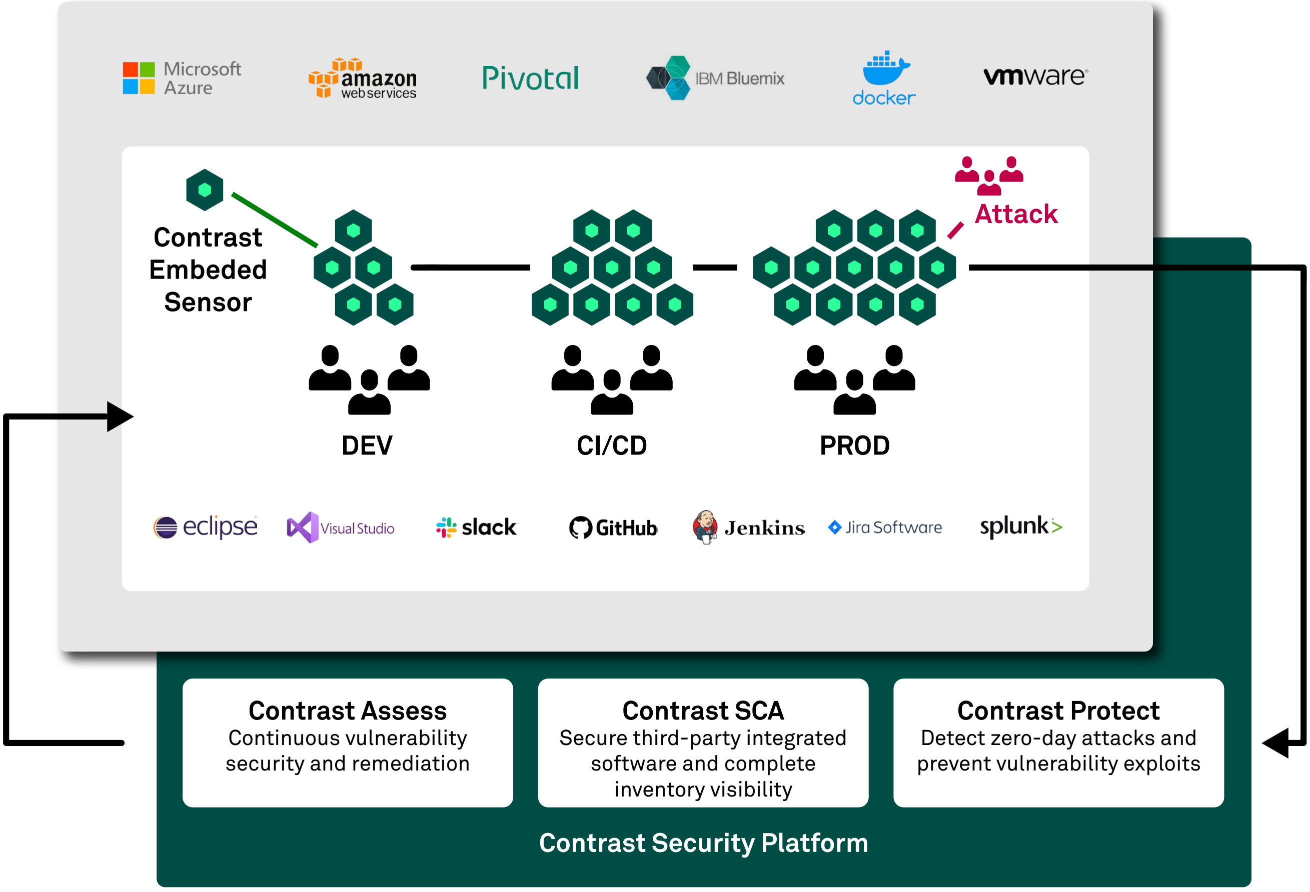
HOW CAN AGENCIES IMPLEMENT THE CATO PROCESS?

Bo Berlas, CISO General Services Administration, said in an interview that agencies looking to adopt the new cATO standards need to use a “robust and formalized continuous monitoring solution, which requires the ability to maintain ongoing situational awareness and ready response in the event of security events.”

To fulfill the requirements of a cATO operation, security measures must be able to demonstrate three primary competencies:

1. Ongoing visibility of key cybersecurity activities inside of the system boundary with robust continuous monitoring of Risk Management Framework (RMF) controls,
2. The ability to conduct an active cyber defense to respond to cyber threats in real-time, and
3. The adoption and use of an approved DevSecOps reference design.

The Contrast Solution harmoniously integrates these requirements into a single integration point. The Contrast platform delivers Software Composition Analysis (SCA), Application Security Testing (AST), and exploit prevention capabilities, allowing developers to instrument security across the Software Development Life Cycle (SDLC).



THE IMPORTANCE OF CONTINUOUS VISIBILITY IN THE CYBERSECURITY VALUE CHAIN

Web applications and application programming interfaces (APIs) remain a leading attack vector for expensive, reputation-damaging breaches. Security leaders have struggled to mount adequate protection against known and unknown threats by relying solely on perimeter-based Application Security (AppSec) solutions, including Web Application Firewalls (WAFs). 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. In addition, using experts to manually implement WAFs can be excessively costly.

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

Real-time protection and observability

Utilizing instrumentation-based runtime application protection and observability delivers contextual insights into application runtime events such as code, libraries and APIs. This process enables AppSec teams to defend against vulnerabilities with superior accuracy. Security teams can reduce dependency on manual workflows and focus on essential strategic and business-critical tasks. Since runtime application protection and observability are inseparable from the actual application, deployment and scaling become fast and frictionless.

Once deployed, Contrast Protect provides continuous protection through Runtime Exploit Prevention (REP). This 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. Detection monitoring takes sub-milliseconds, even under the heaviest attack loads. Contrast Protect detects the top threats identified by the Open Web Application Security Project (OWASP) and the NIST.

Key features of Contrast Protect

Continuous Security Observability from the Inside

- Immediately know when things go wrong and why
- Code-level telemetry with rich, actionable guidance
- Prioritized and confirmed vulnerabilities with remediation help specific to your environment

Active Runtime Application Protection that Responds to Threats in Real Time

- Accurate, compliant and dynamic runtime exploit prevention, aka RASP
- Application runtime instrumentation on the inside verifies exploitable attacks
- Dramatically reduces noise and accelerates security posture

Simple Auto-Scaling and Security Portability

- Simple auto-scaling protection in lockstep with your application runtime
- DevOps-native process fit that deploys anywhere without bottlenecks
- Seamless Continuous Integration/Continuous Deployment (CI/CD) and affordable total cost of ownership (TCO)

THE ACTIVE CYBER DEFENSE — SUCCESSFULLY RESPOND TO CYBER THREATS IN REAL TIME

Traditional approaches to AppSec that rely on scanning lines of code for known vulnerabilities lack visibility and accuracy. As a result, they depend on manual security checks by expert staff to triage and interpret the results before handing recommendations with limited context back to developers to fix the problems. This inefficiency inhibits development cycles, increases costs and often fails to eliminate many vulnerabilities that cyberattacks can exploit.

To avoid these issues, Contrast Assess uses instrumentation to embed security directly into the development pipeline. It automatically identifies and diagnoses software vulnerabilities in applications and APIs, enabling organizations to release secure software to end users faster and with fewer risk exposures. Plus, it offers the broadest language support in the industry among Interactive Application Security Testing (IAST) solutions.

Contrast Assess automatically identifies and diagnoses software vulnerabilities in applications and APIs using instrumentation to pinpoint and prioritize software vulnerabilities. By embedding sensors inside applications, organizations can “shift left” and discover vulnerabilities earlier in the SDLC.

This approach provides the highest accuracy, efficiency and coverage possible. Contrast Assess enables companies to decrease security team triage and DevOps remediation expenses significantly. In addition, reducing alert noise (caused by false positives) helps eliminate hours of work required of DevOps teams to find and fix vulnerabilities without an in-depth understanding of a specific vulnerability’s priority. Instrumentation is the key to transforming AppSec into a continuous process.

The solution’s sensor-driven assessment continuously monitors all parts of the application stack for vulnerabilities. Because it is embedded in the software, it runs anywhere the application runs — including in integrated development environments (IDEs), on a local testing server, on a quality assurance (QA) machine, as part of the CI/CD build, in a container or in the cloud. Contrast Assess then instantly alerts of any findings, empowering developers to identify, fix and verify remediations during runtime, thereby providing an “always-on” security assessment.

The accuracy and ease of use of Contrast Assess help organizations detect and fix threats earlier in the CI/CD pipeline.

Key features of Contrast Assess

- Extensive vulnerability coverage
- Code-level remediation advice
- Third-party code analysis
- Application inventory
- Live application architecture

When working against tight sprint deadlines, developers almost always default to using third-party open-source or commercial off-the-shelf (COTS) components to provide ready-made functionality for a particular business use case. Developers pull these components from various sources, including public repositories and project sites. This results in complex dependency trees that can be difficult to track. AppSec teams can quickly become overwhelmed with this volume of technical debt. In many cases, they struggle to answer the simple question, “What is in the application?”

CONTRAST SCA BRINGS ORDER TO THE CHAOS

Open Source Software (OSS) allows developers to build feature-rich applications on aggressive timelines. However, reliance on OSS adds layers of complexity across an organization’s software supply chain.

Contrast SCA delivers real-time feedback on third-party software risk by embedding SCA and compliance controls into applications throughout their life cycle. By leveraging instrumentation, Contrast SCA reduces friction between development, security and operations teams by showcasing critical insights — such as runtime library usage — that can help drastically reduce manual triaging and prioritize remediation efforts for developers.

Contrast SCA provides real-time feedback to developers by integrating that feedback into their native CI/CD workflows. SCA provides context into how vulnerable libraries are introduced, with no scanning required. This enables developers to take advantage of the many benefits of SCA while delivering AppSec teams the necessary safeguards they need to be confident that the libraries used in their code are secure.

Key features of Contrast SCA

Contrast SCA enables you to embed third-party software testing throughout the software life cycle. The benefits:

- As a shared service across the Contrast AppSec Platform, Contrast SCA provides third-party software visibility without the need to deploy any additional tooling.
- Avoid erroneous findings by assessing custom and third-party code simultaneously.
- Embed testing for vulnerable third-party libraries within native CI/CD and runtime testing.

Flag library risk within cloud-native applications and block attacks on vulnerable libraries in production. Prioritize the most immediate risk based on which libraries are used.

- Highlight which libraries are used by the application and how often, down to the specific class, file or module.
- Prioritize remediation workflows based on which libraries are actually called at runtime.
- Enable developers to fix vulnerable libraries fast by focusing on the most relevant third-party software risk.

Mitigate security debt by accounting for transitive dependency risk.

- Integrate the Contrast command-line interface (CLI) into native CI/CD processes to populate the dependency tree and highlight potential risk.
- Flag software supply-chain risk by identifying possible instances of dependency confusion.
- Contextualize how dependencies are pulled into the application to streamline remediation efforts.

Stay up to date on third-party software inventory and institute scalable controls.

- Export library versioning, vulnerability, licensing and environment data to a standardized Software Bill of Materials (SBOM).
- Ensure rapid response to emerging threats with automated alerts for new vulnerabilities in deployed libraries.
- Institute scalable policy controls for third-party security and licensing and enforce them within native pipelines.

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