CONTRAST SECURITY

Contrast One™ service offering

VERSION 1.0

Introduction

This document sets out Contrast Security's Contrast One Service Offering. Contrast One is a managed service that empowers organizations to build secure Applications with speed and efficiency. With Contrast One, customers benefit from continuous security testing, expert analysis and actionable guidance throughout their Software Development Life Cycle (SDLC). Contrast Security, Inc. is herein referred to as "Contrast."

Definitions

- **Agent:** A runtime application security tool for finding and fixing code vulnerabilities. The agent works by instrumenting code with sensors, collecting data and analyzing it for potential vulnerabilities at runtime or compile time (Golang).
- **Application(s):** Software programs, binary code, source code, components, libraries, modules and/or services that provide a set of capabilities in support of a business function.
- **Application Detection and Response (ADR):** Application Detection and Response (ADR) is a software solution designed to protect the application layer by analyzing and blocking malicious traffic.
- **Application Security Testing (AST):** The process of identifying security vulnerabilities in applications through various testing methods, including static, dynamic and interactive analysis.
- **Attack events:** Contrast attack events represent HTTP requests that contain malicious payloads. These events are detected and observed by Contrast agents within application runtime.
- **Business days:** Excludes Saturdays, Sundays and any day that is a nationally recognized federal holiday pursuant to United States federal law.
- **Concurrent host(s):** Runtimes or processes instrumented by the Contrast agent in which the customer application runs: for example, a Java Virtual Machine (JVM) for Java applications, such as Tomcat server or an executable Spring Boot Jar.
- **Contrast platform:** The Contrast platform is a software solution offered as a multi-tenant or dedicated software as a service (SaaS) and enterprise on-premises (EOP) solution.
- **Enterprise On-Premises (EOP):** The Contrast EOP platform is specifically designed to be run on the customer's own premises or the customer's public/private cloud infrastructure.
- **Mitigation:** Managing and mitigating risks when immediate remediation is not feasible.
- **Professional services:** Professional services offer expert guidance for setup, onboarding and workflow optimization to maximize product effectiveness.
- **Remediation:** The process of fixing identified vulnerabilities to prevent exploitation.
- **Technical support:** Technical support resolves product malfunctions (break-fix), assists with configuration and addresses compatibility issues within user environments. For full details of the scope and definition of technical support, please see the accompanying technical support reference guide.
- **Vulnerability:** A weakness or flaw in an application's code, architecture or design that could be exploited by attackers to compromise security.

Technology and service

Contrast One includes the following:

Technology

1. Contrast One for AST:
   Application Security Testing: Access to the multi-tenant SaaS version of the Contrast platform, including its suite of Runtime Security testing tools.

2. Contrast One for ADR:
   Application Detection and Response: Access to the multi-tenant SaaS version of the Contrast platform, including its suite of Runtime Security detection and response tools.

Note: On-premises and dedicated SaaS options are available at an additional cost.

Managed workflows

With Contrast One's service offering, managed workflows are executed by the Contrast One team, requiring active involvement of the customer in each managed workflow to optimize outcomes:

Contrast One for AST

1. End-to-end vulnerability management
   - Review and prioritize vulnerabilities.
   - Share documented vulnerabilities with customer's Application Security (AppSec) and development teams for action.

2. Open-source vulnerability management — available on customer request
   - Initial verification of vulnerabilities in open-source, vendor-developed and custom code.
   - Actively collaborate with customer's AppSec and development teams for evaluation and remediation.

3. Expert remediation guidance — available on customer request
   - Offer one-on-one remediation sessions to support developers, accelerating remediation rates and reducing resolution time.
   - Work alongside the customer development team to remediate vulnerabilities, eliminating the need for in-house security expertise.

Contrast One for ADR

1. Attack triaging consultation — available on customer request
   - Proactive attack anomaly pattern monitoring for tuning the agent configuration to reduce alert noise.
   - Provide event-driven tuning reports.
   - Deliver periodic configuration optimization reports.

2. Risk-mitigation strategies
   - Implement plans to manage risks effectively when immediate remediation is not feasible.

3. Zero-day notification and incidence response consultation
   - Provide a report highlighting risk of a new zero-day vulnerability.
   - Provide mitigation guidance related to a new zero-day vulnerability.

Managed operations

In order to facilitate the efficient and effective operation of Contrast One, the customer must grant administrator-level access to the Contrast One team on the Contrast platform.

1. Comprehensive Runtime Security program
    - Support Runtime Security program assessment, definition and updates.
2. Actionable insights and reporting
    - Detailed reports on customer's security posture with insights to support decision-making and compliance efforts (*Security Posture Reports*).
    - In order for Contrast to provide such *Security Posture Reports*, customer must enable product usage analytics on the Contrast platform.
3. Managed rollout and platform administration
    - End-to-end management of platform deployment, user onboarding and maintenance to ensure smooth operations without burdening internal teams.
4. Education and training
    - Contrast One includes role-specific training for AST and ADR end-user roles.
    - Training includes overviews of the Contrast AST and ADR solutions, utilizing vulnerability, library and attack event data and screens; and managing vulnerabilities, attack events and other end-user topics.
    - In most cases, training content is available as self-serve eLearning, but ad hoc live training sessions can be scheduled to address specific use cases outside of the standard offerings.

Responsibilities

To ensure effective execution of managed workflows, Contrast One offers customers access to the following resources:

Contrast

- **Engagement manager:** The primary liaison tasked with the overall success of service delivery.
- **Customer security advisor:** Collaborates with the customer to understand the customer's security requirements and aspirations to develop AppSec strategy; assists in implementing and utilizing Contrast products and services to fulfill those objectives.
- **Contrast SMEs:** Deliver the day-to-day operations of the Contrast platform, agent rollout and maintenance, attack and vulnerability triaging, remediation guidance, etc.

Customer

- **Management sponsor:** Senior-level customer representative (e.g., CISO, SVP) responsible for overseeing the successful implementation and adoption of Contrast products.
- **Application owner:** Individual responsible for managing application resources, delivering business objectives and ensuring alignment with security requirements.
- **IAM administrator:** Technical expert responsible for managing SSO/AD/LDAP solutions, configurations and integrations with Contrast products.
- **Network administrator:** Technical expert responsible for network infrastructure management and configuration of firewall rules to enable Contrast agent communications.

- **DevOps lead:** Technical administrator with authority to implement and manage DevOps infrastructure changes, including orchestration tools and deployment processes.
- **Application security lead:** Primary point of contact responsible for implementing and managing Contrast products within the organizatin's AppSec program.
- **Development team:** Team responsible for application development, implementing security fixes and integrating Contrast agents into the application environment.
- **Quality assurance team:** Team responsible for application quality assurance, including utilizing Contrast's route coverage capabilities to enhance security testing coverage.
- **Security Operations Center (SOC) team:** Team responsible for monitoring, analyzing and responding to security events and incidents identified by Contrast ADR.
- **Threat hunter:** Security specialist who utilizes Contrast tools to identify and investigate potential security threats that may bypass traditional security controls.
- **Governance, Risk and Compliance (GRC) lead:** Individual responsible for ensuring AppSec practices meet industry regulations and internal policies through Contrast's reporting and risk management capabilities.

Sevice Level Objectives (SLOs)

- **Contrast platform availability:** The availability policy for the Contrast platform is described in paragraph 4 of Contrast’s technical support reference guide.
- **Support response time:** Contrast One will follow the Contrast standard support response times, as set out here.
- **Escalation:** Contrast One will follow the escalation process described in paragraph 3.11 of Contrast’s technical support reference guide.

Contrast One for AST

Application onboarding

- **Target:** The onboarding process for new customer software applications will start following Contrast’s receipt (via email) of details of the application(s) and validation of Contrast compatibility.
- **Customer responsibilities:**
  - Provide accurate and complete software application details (e.g., technology stack, code repository access, deployment environment).
  - Participate in onboarding meetings and provide timely feedback.
  - Configure necessary access permissions for Contrast agents.

Vulnerability triaging

- **Target:** Triaging and prioritization of new vulnerabilities will start within 1 business day of detection by the Contrast agent.
- **Severity levels:** The triage process will be based on the severity levels that are configured on the Contrast platform based on the customer’s own remediation policy. For example, if a customer's remediation policy mandates addressing only critical and high severity vulnerabilities, vulnerabilities with medium and lower severity will be excluded from proactive triage activities.

- **Customer responsibilities:**
  - If customer does not provide Contrast with customer's own vulnerability remediation policy, Contrast will use the Contrast vulnerability remediation policy to triage and prioritize detected vulnerabilities.
  - Provide context and information about the application and its environment to aid in triaging.
  - Assign appropriate personnel to review and address vulnerability reports.

Vulnerability remediation guidance

- **Target:** Contrast One will start remediation assistance within 1 business day of receiving a customer's written request over email. The Contrast One team will also proactively contact the customer development team (where contact information has been provided to Contrast) and offer remediation assistance.
- **Guidance format:** Remediation guidance will include vulnerability descriptions, potential exploits and recommended fixes or mitigations over remote conference calls and via email.
- **Customer responsibilities:**
  - Review and collect remediation questions and open remediation assistance requests.
  - Email Contrast regarding any challenges or roadblocks encountered during remediation.
  - Provide access to the customer's AppSec lead and development team to address Contrast SMEs' questions on current application implementation and security controls.

Reporting and communication

- **Formal communication:** Customers should employ all forms of written correspondence to communicate with the Contrast One team. All written notifications should be sent via email to support@contrastsecurity.com.
- **Reporting frequency:** Provide monthly reports on AppSec posture, vulnerability trends, remediation progress, coverage and risk status.
- **Communication channels:** Maintain open communication channels (e.g., email, online portal, dedicated Slack channel, etc.) for ongoing support and updates.
- **Customer responsibilities:**
  - Review reports and provide feedback..
  - Communicate any changes to the application environment or security requirements.

Contrast One for ADR

Application onboarding

- **Target:** Onboarding new applications will start within 2 business days of Contrast's receipt of application details and validating that Contrast's agent is compatible with the customer application technology stack.
- **Customer responsibilities:**
  - Provide accurate and complete software application details (e.g., technology stack, code repository access, deployment environment).
  - Participate in onboarding meetings and provide timely feedback.
  - Configure necessary access permissions for Contrast agents.

Attack triaging consultation

- **Target:** Consultation services will start within 1 business day of Contrast's receipt, via email, of the consultation request. Contrast will provide attack triage action advice through Contrast ADR.
- **Customer responsibilities:**
  - Provide context and information about the attack events to aid in triaging.
  - Assign appropriate customer personnel to review and own post-review actions.

Risk mitigation strategies

- **Target:** Consultation services will start within 1 business day of Contrast's receipt, via email, of the customer's consultation request. Contrast will provide mitigation advice through Contrast ADR and fine-tune attack occurrence in cases of noise. Contrast will perform periodic attack trend analysis to fine-tune ADR rules.
- **Customer responsibilities:**
  - Provide context and details regarding the attack events to aid in triaging.
  - Assign appropriate customer personnel to implement mitigation advice.*Reporting and communication*

Zero-day notification and incident response consultation

- **Target:** Contrast provides zero-day notification information including but not limited to severity, risks, libraries, impacted applications and risk mitigation strategies to prevent zero-day attacks.
- **Customer responsibilities:**
  - Assign appropriate customer personnel to implement mitigation advice.

Exclusions

The following is a non-exhaustive list of what Contrast One does not cover:

1. Vulnerability remediation with respect to third-party libraries or components outside the customer's direct control.

2. Delays or issues caused by the customer's failure to meet its responsibilities as set out in this document.

3. Security incidents or breaches resulting from factors unrelated to Contrast One or other Contrast products or services.

4. Contrast One provides remediation guidance only. Customer is responsible for implementing code changes.

The following is a non-exhaustive list of what Contrast One for ADR does not cover:

1. 24/7 monitoring and response: Contrast's personnel do not provide the continuous, real-time monitoring or immediate incident response services typically associated with a Security Operations Center (SOC).

2. Log analysis and threat hunting: Contrast One for ADR does not encompass the collection, analysis and correlation of logs from various sources for threat hunting or advanced threat detection purposes.

The timelines set out in this document do not apply to customers who have ordered Contrast products on an on-premises deployment basis.

Customer participation

To ensure successful delivery and maximize the value of Contrast One, the following forms of customer participation are necessary:

- **Active collaboration:** Active involvement in the onboarding and integration process, including timely responses to requests for information or access.
- **Vulnerability remediation:** Timely remediation of identified vulnerabilities by the customer development team, including prioritization and resource allocation.
- **Feedback and communication:** Regular communication and feedback on the managed workflow and Contrast platform, including progress updates, challenges and suggestions for improvement.
- **Designated point of contact:** A primary point of contact within the customer's organization who is responsible for coordinating with Contrast and facilitating internal communication. This point of contact can be the management sponsor or application security lead.
- **Stakeholder engagement:** Involvement of relevant stakeholders within the customer's organization, including development, security and operations teams.

Deliverables

- **Security maturity assessment:** The Customer Security Advisor (CSA) conducts an AppSec maturity assessment based on industry-standard frameworks like Building Security In Maturity Model (BSIMM) or Open Software Assurance Maturity Model (OpenSAMM). This assessment establishes a baseline for organizations to measure their AppSec maturity.
- **Onboarding and integration plan:** A comprehensive plan detailing the onboarding process and schedule to ensure a seamless integration of services.
- **Reporting:** Regular reports are provided, including but not limited to activity logs, AppSec posture assessments, status updates and vulnerability reports. These reports offer insights into the overall security posture and help organizations maintain compliance.
- **Role-specific training program:** Offer tailored training and educational resources specifically designed for various roles within the customer's organization, aligning with the customer's AppSec strategy. These training sessions can be delivered in multiple formats, including e-learning modules, instructor-led workshops, personalized team coaching and comprehensive playbooks.

Conclusion

Contrast One offers a comprehensive and proactive approach to AppSec, encompassing both Application Security Testing (AST) and Application Detection and Response (ADR) capabilities. The partnership with Contrast Security provides access to a powerful platform, expert support and actionable guidance. This empowers organizations to strengthen their security posture and accelerate their development process, ultimately enabling them to build secure applications with confidence.

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.

contrastsecurity.com

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333