Contrast support and professional services policies

VERSION 1.2

Introduction

Contrast Security's ("Contrast") support services provide a comprehensive offering that is designed to ensure customers have the support they need, when they need it. When problems arise, a dedicated technical support team will quickly and efficiently resolve any questions or challenges.

Contrast's professional services aim to accelerate a customer's security transformation by proactively assisting with Contrast setup, onboarding, implementation and workflow optimization. This partnership offers a guided path to launch, helping customers quickly get value and achieve improved security posture.

Contrast Security offers:

- Expert support services: Comprehensive technical support, reducing internal operational needs and adding planning assistance.
- Technical Account Manager (TAM): Dedicated technical advisor for accelerating deployment, adoption and value realization.
- 90-day launch package: Professional services assistance to quickly launch and implement Contrast.
- Additional professional services hours available.

This document details Contrast's support and professional services offerings.

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.
- **Thirty-day subscription period:** Each thirty (30) day period beginning on the subscription start date and ending on the subscription end date. The thirty-day subscription period is defined as the start of the subscription date and 30 days after the start date and so on. Example: Where a subscription period starts on March 15, 2025 and ends on March 14, 2026, the first thirty-day subscription period will start on March 15, 2025 and end on April 14, 2025.
- **Vulnerability:** A weakness or flaw in an application's code, architecture or design that could be exploited by attackers to compromise security.

Contrast support and professional services plans

Contrast support services

Contrast Security offers expert support services that provides comprehensive technical support, reducing internal operational needs and adding planning assistance.

Support services	Expert
Technical support	
Web, email, phone	✔
First response time SLAs	P1 = 1 hour P2 = 2 hours P3 = 4 hours
Dedicated support dashboard	✔
Contrast Security University	
Access (additional seats available for purchase)	Up to 20 seats

Contrast Security University: Contrast offers self-paced learning through the online portal "Contrast Security University". The learning modules cover Contrast product overviews, adoption workflows and product best practices. It also includes additional content and links related to application security best practices.

Contrast support and professional services plans (cont.)

Contrast professional services

Contrast Security's professional services aim to accelerate a customer's security transformation by proactively assisting with Contrast setup, onboarding, implementation and workflow optimization.

Contrast Security offers:

- 90-day launch package: Professional services assistance to quickly launch and implement Contrast.
- Technical Account Manager (TAM): Dedicated technical advisor for accelerating deployment, adoption and value realization.
- Additional professional services hours available.

Profressional services	
90-day launch package	
Regular touchpoints	Weekly
Launch and implementation support	✔
Contrast SME	✔
Contrast launch consultant	✔
AppSec consulting requests	Up to 2 requests per thirty-day subscription period
Custom reporting	Up to 4 requests
Custom scripting	Up to 2 requests
Post-implementation training	1 knowledge transfer and team readiness training
Technical Account Manager (TAM)	
Dedicated technical POC	✔
Quarterly business and technical reviews	✔
Deployment and adoption support	✔
Coordination of escalations and cross-team alignment	✔
Best practices and optimization recommendations	✔

Custom scripting: The support services will offer custom scripting to automate the Contrast product adoption workflow and reduce manual efforts.

Priority and urgency levels

Priority levels are primarily determined by the impact of the issue. However, the urgency of a resolution to the customer is also taken into account, allowing the priority level to be increased based on the circumstances, as indicated below the table:

Priority, urgency and impact levels are defined below as:

Impact/urgency	Standard	Major	Critical
Normal	P3	P2	P1
High	P2	P1	P1

Priority level

Priority level, which is determined by a combination of impact and urgency, identifies the sequence in which support cases are to be worked. A higher priority entails escalation and notification to higher levels within the company. Contrast support priority levels are:

- **Priority 1 (P1):** This level implies immediate and sustained effort using any and/or all available resources as required until the issue is resolved with real-time/daily customer interaction and follow up.
- **Priority 2 (P2):** The situation is considered highly volatile, requiring regular follow-up communications with a resolution provided in the next software release to the extent that this is commercially feasible.
- **Priority 3 (P3):** This priority level dictates that the issue be addressed as soon as possible, but after P1/P2 issues.

Impact level

The impact level of an issue is determined based on the type of issue encountered. Contrast impact levels are:

- **Critical:** The product is not usable in any form. No workaround is available.
- **Major:** Severe errors that disable major software functions. The customer's ability to perform tasks is significantly impeded. The error may be repetitive in nature and impacts timely performance of tasks. A workaround may be available.
- **Standard:** Errors disabling only certain non-essential functions in the software as described in documentation. Impact is confined to an inconvenience with minimal impact on basic functionality. A reasonable workaround will be provided if available.

Urgency level

The majority of tickets handled by the Contrast technical support team will have a normal urgency level. However, if the issue is preventing further adoption of Contrast products or causing significant delay to the customer's project timelines, the urgency will be marked as high.

Responsibilities

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

Contrast

- **Technical support team:** A highly trained technical support staff is available to answer questions, diagnose failures and troubleshoot problems.
- **Enterprise account manager:** Responsible for ensuring enterprise customers receive maximum value from Contrast's solutions.
- **Contrast launch consultant:** The primary liaison tasked with the overall success of service delivery.
- **Contrast SMEs:** Deliver the day-to-day operations of the Contrast platform, agent rollout and maintenance, attack and vulnerability triaging, remediation guidance, etc.
- **Technical Account Manager (TAM):** Designated technical advisor to drive deployment success, adoption and ongoing value through proactive guidance, reviews and coordination across Contrast teams to ensure maximum value realization.

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)

Application onboarding

- **Target:** The onboarding process for new customer software applications will start within 2 business days 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.

AppSec consulting request

- **Target:** AppSec consulting requests will be limited to AST vulnerability triaging or remediation guidance sessions. Also, include the ADR event triaging and mitigation guidance. These sessions will be scheduled within 5 business days after receiving a written request via email.
- **Guidance format:** Remediation guidance will include vulnerability descriptions, potential exploits and recommended fixes or mitigations over remote conference calls and via email.
- **Customer responsibilities:**
  - Provide access to vulnerability details via Contrast TeamServer or vulnerability export.
  - Provide or collect answers to questions from Contrast AppSec experts related to the vulnerability in question.
  - Ensure application experts, developers and AppSec members participate in the triaging call to speed up triaging and remediation guidance.

Communication

- **Formal communication:** Customers should employ all written notifications sent via email to support@contrastsecurity.com.
- **Communication channels:** Maintain open communication channels (e.g., email, online portal) for ongoing support and updates.

Hours of operation

- **Global support:** Technical support is provided to all Contrast customers in their jurisdiction, unless applicable sanctions prohibit us from doing so.
- **Business hours:** Contrast's support team is available via web, email, phone or chatops (Slack, Teams, etc. where applicable) from 12am UTC Monday to 12am UTC Saturday.
- **Out of hours support:** Contrast technical support maintains an on-call support engineer 24x7 in case of any P1 issues raised outside of normal business hours. In order to alert the on-call support engineer, customers must open or update a support ticket via email, with the string #CriticalSupport in the body of the email. The support engineer will be in touch as soon as possible to assist further.
- **Consulting support:** Contrast's professional services team handles consulting requests (business days only), which require lead time and are based on Contrast SME availability.

Exclusions

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

1. Vulnerabilities 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 products or services.
4. Contrast provides remediation guidance only. The customer is responsible for implementing code changes.

The following is a non-exhaustive list of what Contrast's 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's 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's solutions, 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

Committed service deliveries will be completed remotely. The support services include the following deliverables:

- Support dashboard
- Access to Contrast Security University
- Following only applicable to 90-day launch package:
  - Post-implementation training
  - Custom automation scripts
  - Custom reporting
- Application onboarding project plan
- Following only applicable with a Technical Account Manager (TAM):
  - Quarterly business and technical reviews
  - Deployment and adoption support
  - Coordination of escalations and cross-team alignment
  - Best practices and optimization recommendations

Conclusion

Contrast Security's support services offer full technical support and customer service to ensure organizations have the service they need, when they need it. Contrast's expert support team is well qualified to answer questions, assist with critical issues and troubleshoot problems. By leveraging Contrast's support services, customers can reach their desired security program outcomes through ongoing success planning, tracking and robust reporting.

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