Contrast SECURITY

SOLUTION BRIEF

6 Benefits of Contrast Security SAAS

Contrast Security recommends choosing the Software-as-a-Service ("SaaS") version of our central management and reporting server, TeamServer. SaaS accelerates time-to-value, simplifies scaling as your deployment grows, and ensures the highest levels of security. Below are six benefits of using Contrast SaaS.

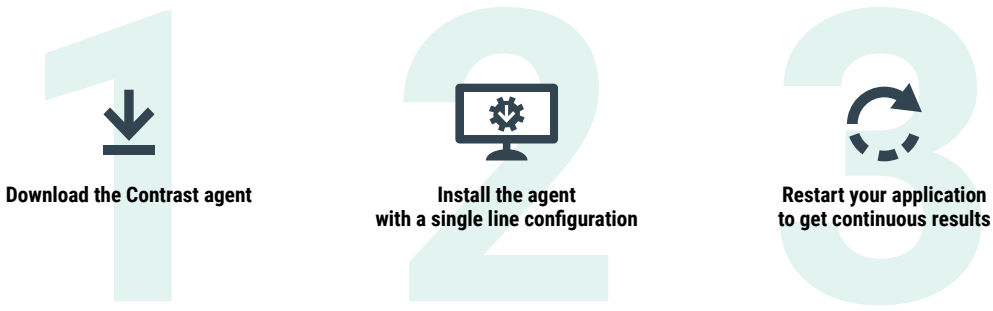
Contrast TeamServer

TeamServer is a central management and reporting server that provides policy-based control over a Contrast deployment. TeamServer aggregates all vulnerability and attack data produced by Contrast Assess and Protect agents. Organizations use TeamServer to view vulnerability and attack data and reports, integrate that data with other systems, and implement code fixes security policy across the application portfolio.

1. Immediate App Assessment and Protection

SaaS lets you focus on assessing and protecting your applications right away. Download the Contrast agent[1] install in minutes to begin instrumenting applications in your environment. SaaS means no additional server software or hardware to install, configure, upgrade, monitor, or manage.

Figure 1. Assessing applications is complex, but Contrast makes it easy



2. Latest Innovations and Enhancements

Using SaaS lets you take immediate advantage of the latest Contrast functionality, feature innovations, and productivity enhancements. Contrast is constantly deploying new features, and the SaaS environment always runs the latest code base. On-premises users must download and install the latest software update to take advantage of new features.

3. Elastic and Automatic Scaling

As your application security needs increase, the Contrast SaaS TeamServer scales elastically, allowing for simultaneous testing of an unlimited number of applications. Start assessing and protecting one application today, and scale up to hundreds more – without the hassles of provisioning new servers or other infrastructure.

4. Intellectual Property Secured in your Own Environment

Your application source code and binaries never leave your servers. Our instrumentation approach means you don't upload your software into our SaaS environment (see the sidebar to learn more about instrumentation). The Contrast agents analyze software wherever it is run, and collect only the metadata needed to provide analysis and metrics. Contrast agents collect the following types of metadata and send them to the TeamServer:

- Vulnerability and attack data including HTTP request data and a series of method invocations
- Summary information about what libraries and classes are loaded by each application
- Sitemap information, including URLs, but not parameters
- Software architecture information about back-end components and connections

Instrumentation

Contrast Security's instrumentation technology uses agents and passive sensors to monitor the behavior of applications and discover vulnerabilities with speed and accuracy. Unlike traditional point-in-time static or dynamic scanning techniques, Contrast instrumentation provides your developers with continuous security feedback as soon as they run their code. The Contrast agent automatically reports application vulnerabilities to the SaaS TeamServer, which displays critical security information, vulnerabilities, and remediation advice across all applications in a realtime dashboard.

Security Built for the Cloud

Contrast Security completed and passed SOC 2 audits in February 2017, validating organizational controls related to security availability and confidentiality.

Contrast SECURITY

5. Enterprise-Grade Security

Contrast Security follows the same best practices for security as the world's largest enterprises. The information TeamServer manages is very valuable and is protected with multiple defense layers to segregate your data from other customers.

HOSTING ENVIRONMENT PROTECTION

Contrast's SaaS TeamServer is hosted in Amazon Web Services (AWS), the world's leading cloud service provider, and is protected by controls that AWS uses – including FedRAMP, ISO 27001, FIPS, SOC 2/Type II, FERPA, and HIPAA. A full list of AWS certifications is available at: http://aws.amazon.com/compliance/. No Contrast employees have physical access to AWS Data Centers.

DATA AT REST PROTECTION

Each application's vulnerability data is stored encrypted at rest in Contrast Security's secure multi-tenant environment on AWS. All disk volumes storing Contrast Security data at AWS are fully encrypted with Amazon's EBS encryption.

DATA ACCESS PROTECTION

All access to the TeamServer employs strong encryption and mutual authentication to protect against sniffing, spoofing, and other communications attacks. Your organization's administrator can control access to certain applications based on user roles and membership user-defined organizations, from within TeamServer.

USER AUTHENTICATION

Individual users must authenticate, and TeamServer checks password strength and performs lockouts on multiple failed login attempts to prevent brute force attacks. Users can leverage SAML-based single sign-on (SSO) and Two-Step Verification using time-based one-time passwords (TOTP). The Contrast agent connects to the TeamServer over an SSL socket connection that can be configured to use an outbound proxy. The agent verifies the TeamServer certificate, and sends TeamServer an authorization key to establish mutual authentication. All back-end TeamServer connections are encrypted and mutually authenticated.

6. Dependable Uptime

The Contrast Security operations team proactively monitors uptime, and uses several industry-trusted monitoring solutions to measure the health, security, and performance of the SaaS service:

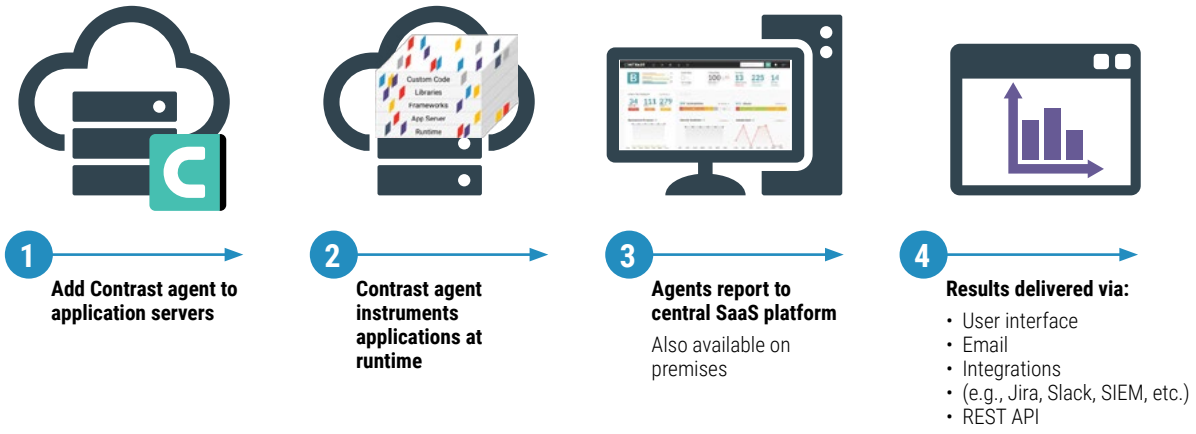
- Application Performance Monitoring
- Workload Insights, Infrastructure Monitoring, Vulnerability Management, Threat Intelligence, Compliance Reporting
- Log Aggregation and Management for system and application logs, AWS CloudTrail, AWS Config, and other AWS Services

Conclusion

The Contrast Security SaaS TeamServer offers all the power, security, and control of the on-premises TeamServer, with the added benefits of cloud computing: lower cost,[2] rapid time-to-value, ease of deployment, and transparent scalability. Your software remains in your environment, and all vulnerability and attack metadata in the TeamServer is secured with multiple layers of security from both Contrast Security and Amazon Web Services.

Work with your Contrast Security representative to discuss the best options for your environment and needs. You may also visit **www.contrastsecurity.com** and click on the "Get DEMO" button on the top of every page to schedule a personal introduction to Contrast.

Figure 2. Contrast Enterprise Deployment Diagram



[1] Contrast currently supports Node.js, Microsoft .NET, and Java.
[2] An on-premises TeamServer increases the overall purchase price of Contrast Assess and Contrast Protect by 15%.

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