SOLUTION BRIEF

Facilitating Secure Journeys to the Cloud with the Contrast Application Security Platform

Executive Overview

Enterprises vary widely in the extent and maturity of their cloud deployments. What they all share, however, are deep and pervasive security challenges throughout their cloud journeys. Cloud architects and CloudOps teams struggle to accurately assess the risk of interdependent applications and application components. They are not sure how to best refactor application security as they transition from on-premises to cloud hosting or from private to public clouds. And they lack effective means to secure rapidly proliferating and potentially at-risk application programming interfaces (APIs) in multiple public and private clouds.

Implementing DevSecOps principles can help overcome these and other obstacles. The Contrast Application Security Platform offers a unified approach to DevSecOps that maximizes DevOps and CloudOps efficiencies. Combining security instrumentation and continuous testing with runtime application self-protection (RASP), the Contrast solution enables automated application security at scale.

Cloud Journey Archetypes and the Shared Responsibility Model

Though every company's cloud story is unique, most cloud journeys start with the migration of existing enterprise consumer off-the-shelf software (COTS) solutions. These well-tested applications with clear cloud migration paths provide a good point of entry to the cloud for brick-and-mortar firms.

Once companies are more familiar with the cloud environment—or if they are a cloud-native enterprise—they begin to develop new applications directly in the cloud. As they gain experience with cloud development, they may migrate existing custom applications, employ microservices, and leverage serverless architectures to develop new capabilities. Finally, they apply their learnings in their first cloud environment to additional public and private clouds.

The Contrast Application Security Platform helps companies to:

- *Understand risk in applications as they migrate to the cloud*
- *Rebuild/refactor application security for cloud hosting*
- *Secure production workloads for applications deployed in the cloud*
- *Manage application workload security across hybrid and multi-cloud environments*

From their initial forays into the cloud environment, cloud architects and CloudOps teams shoulder a significant portion of the risk due to the cloud services providers' shared responsibility model. Details vary among providers, but the basic model stipulates that services providers protect the infrastructure of their clouds, and it is up to customers to secure what they deploy in the cloud. This includes operating systems, networking tools, application components, data, and any other IT controls pertaining to these assets.

Cloud Journey Archetypes and the Shared Responsibility Model

The Contrast Application Security Platform helps cloud architects and CloudOps teams maintain application security continuously and cost-efficiently, regardless of the application's location, life-cycle stage, or dependencies. The Contrast Application Security Platform leverages sensors embedded in the application code, which monitor it continuously throughout the software development life cycle through production.

While code is in development, Contrast sensors detect vulnerabilities in custom code and in open-source libraries and frameworks used by the application. The Contrast platform gives developers immediate feedback on how to eliminate the detected vulnerabilities. Further, developers do not need specialized application security training to be able to implement the suggested code modifications. As a result, developers can satisfy the requirements of the application security team while continuing to focus on their development roles.

For applications in production, Contrast detects deviant and potentially malicious behavior as the application is in use (runtime application self-protection [RASP]). A key distinction between Contrast and web application firewalls (WAFs), which are commonly used in the cloud, is that Contrast focuses on vulnerabilities that are actually exploited, rather than generating alerts for every potential threat. Contrast can do this because as soon as its agent is installed in an application, it automatically maps all the externally available APIs and third-party libraries. Contrast then tracks what part of these resources the application uses as it runs. This significantly reduces the vulnerability space that analysts need to address, eliminating high volumes of false positives that consume valuable time triaging and diagnosing.

Both in development and in production, the security instrumentation that underlies the Contrast platform delivers accurate results. It provides continuous, real-time security context versus legacy application security approaches that employ point-in-time models that rely on security signatures. This dramatically reduces false positives, which improves efficiencies for CloudOps teams, while delivering fewer false negatives that lowers application risk.

Next, we will see how the Contrast Application Security Platform follows applications through their cloud journeys, reducing testing complexity, and more importantly, ensuring that security gaps are found and fixed.

> *Through instrumentation and continuous testing, cloud architects can assess vulnerabilities more accurately and mitigate them faster.*

Migrating Legacy Applications

When on-premises applications move to the cloud, cloud teams must be aware of all dependencies between the core application and the components that tie into it. New cloud-based components that were not present in the on-premises version may have vulnerabilities that the CloudOps team is unaware of. New transaction paths or data access changes may also introduce vulnerabilities.

Understanding these dependencies is the top migration challenge for nearly two-thirds of enterprises.[1] As the web of dependencies grows with increasing cloud adoption, it becomes cost-prohibitive and time consuming to discover and remediate every vulnerability using traditional application security tools. Instrumentation is the key to overcoming this complexity.

The Contrast Application Security Platform is available as a service directly through cloud providers. As an application starts up, Contrast agents automatically embed sensors at specific locations within the application code to observe operating conditions and ensure safe operation. If an outside threat seeks to exploit a vulnerability, sensors detect the activity in real time and the attack is blocked before it can exploit the vulnerability.

Options For Custom Applications

Some applications—particularly custom applications developed for on-premises environments—present additional security challenges as they move to the cloud. Custom applications tend to evolve organically, in response to changes in the business. This often results in considerable variation in infrastructure for computing, data storage, and networking. When deployed in the cloud, these components have differing integration and interoperability requirements, which are extremely difficult to manage. This is probably a key reason why 79% of organizations list governance of cloud components as a major cloud challenge.[2]

Cloud architects and CloudOps teams have two options to mitigate risks for these types of applications. If they have the time and the development staff, they can refactor the applications for the cloud infrastructure. As they do, they can leverage the Contrast platform in the same way they would when developing new applications in the cloud.

Alternatively, they can move their code to the cloud as it is, using the Contrast Application Security Platform to monitor and protect the application in real time.

Developing New Cloud-Native Applications

For cloud-native companies, or for enterprises migrating their development environments to the cloud, the Contrast platform provides application security testing that has been certified by the cloud environments in which it operates.

Rohit Gupta, global segment leader for security at Amazon Web Services (AWS), indicates that Contrast gives AWS customers “a means to get continuous visibility into application layer attacks and the ability to immediately protect themselves from new threats.” AWS and other cloud leaders have joined the Contrast Application Security Lifecycle Stack Program, which helps integrate security into all stages of the DevOps application life cycle.

Contrast also offers numerous integrations with cloud-based integrated development environments (IDEs), continuous integration/continuous delivery (CI/CD) environments, as well as quality assurance and operations tools. These integrations make it easy for cloud developers to close application-layer security gaps in the course of their usual work processes, using the tools they already know (Figure 1).

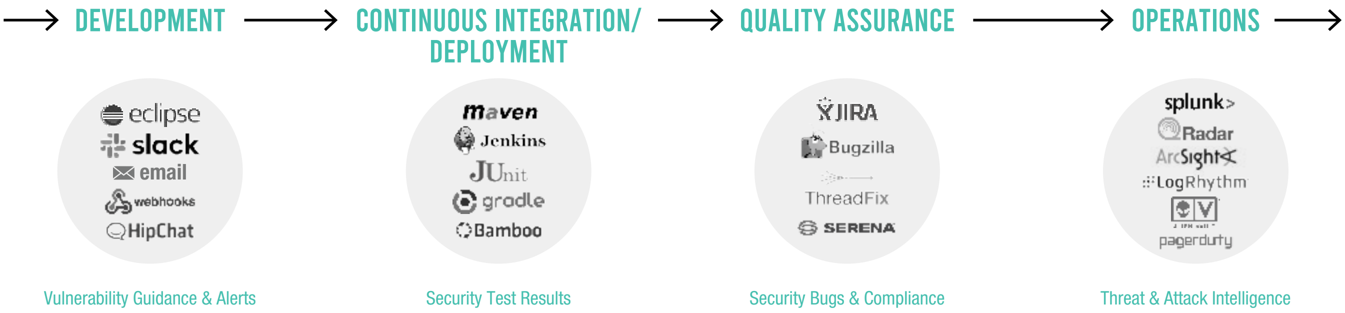

Figure 1. Contrast supports a wide variety of development and operations tools through APIs and plug-ins.

> *SApplications that are built and deployed in a rapid cadence within the AWS cloud offer us greater scalability, agility, and resilience. With Contrast, automating application security into DevOps processes helped GreenSky keep up with the demand to keep delivering business value with increasing speed.*
>
> – Dustin Butterworth, Sr. DevSecOps Engineer, GreenSky

Securing Applications in Hybrid and Multi-Cloud Environments

Cloud platforms are similar in many ways, but each cloud service comes with its own infrastructure components and management tools. CloudOps teams typically do not have enough security staff to maintain proficiencies in multiple cloud-specific application security tools. Also, when one application runs on several different clouds, or in a hybrid cloud, it can be error-prone and inefficient to use multiple tools to remediate vulnerabilities across environments.

The Contrast Application Security Platform solves this problem. Because it leverages sensors within the application code, it is independent of the cloud infrastructure. Once CloudOps teams learn the Contrast platform, any staff member can proficiently monitor application security, regardless of the application's development or deployment environment.

The Contrast platform also helps to unite development and operations teams. It enables both teams to continuously identify application vulnerabilities throughout the CI/CD pipeline. The dashboard (shown in Figure 2) gives all teams a unified view of application security, making it easier for them to troubleshoot collaboratively. This reduces the time and costs associated with fixing vulnerabilities and minimizes their recurrence. The Contrast Application Security Platform also eliminates the need for a suite of external testing tools or for additional staff to perform point-in-time vulnerability scanning, which further reduces costs.

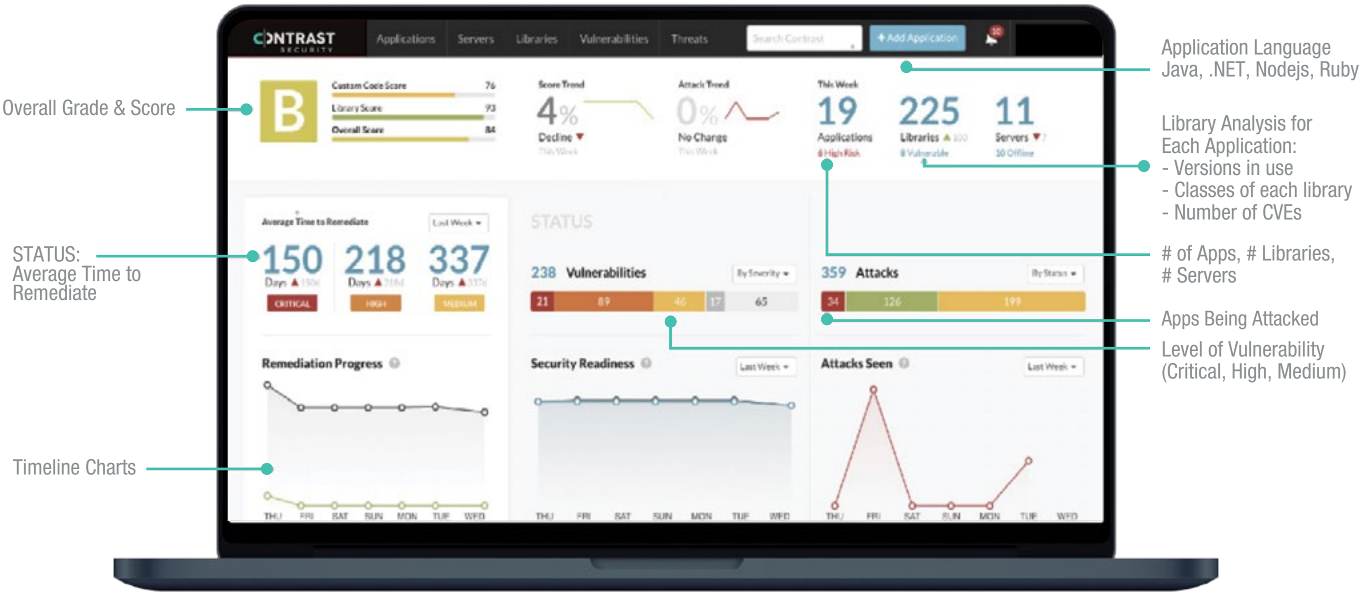

Figure 2. Applications are observable at a glance through the Contrast Application Security Platform dashboard.

Full Speed Ahead, Full Visibility Ahead

Considering the increasing complexity of modern applications and the pressure to deploy quickly in the cloud, it is easy to see why many cloud architects and CloudOps professionals view security as a hurdle. What changes this mindset is a security-first approach to DevOps, with continuous, instrumentation-based application testing.

Your organization can begin to apply this approach today with the Contrast Application Security Platform. Schedule a demo to see how simple it is to make application security continuously and ubiquitously observable at every stage of the software development life cycle (SDLC). The unique advantages of the Contrast Security solution translate not only into enhanced cloud application security, but also into greater time and cost efficiencies in application development and operations in the cloud.

[1] "2020 State of the Cloud Report," Flexera, 2020.
[2] "2020 State of the Cloud Report," Flexera, 2020.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast
SECURITY

contrastsecurity.com