Contrast
SECURITY

WHITE PAPER

3 ways to recession-proof your application security program in 2023 with Contrast Assess

As we approach the midpoint of 2023, many businesses are facing uncertainty. Economic growth has been uneven in recent months, with some industries seeing significant layoffs and others continuing to struggle with a labor shortage. With polarized political dynamics at home, a war in Europe, and instability in the banking sector, the second half of the year may be tumultuous for the economy.

One thing we know for sure: An economic slowdown, if it happens, will not slow the barrage of cyber threats impacting your organization. You might wonder how to tackle these challenges without disrupting your entire application security program.

Navigating the complexities of the security landscape

Cybersecurity risk as a share of the overall risk portfolio continues to grow. The threat landscape is constantly evolving, and your organization continually faces new cyber threats.

And as the threat landscape becomes more complex, the compliance landscape tends to follow. Governments, industry organizations and other compliance authorities are always introducing and tweaking regulations and standards. At the same time, cyber insurance carriers are tightening their underwriting criteria, and businesses must go beyond current required standards to get the best rates.

As organizations try to keep up, the current cybersecurity marketplace creates as many problems as it solves. Most security tools available today require a full-time dedicated expert to operate them, at a time when budgets are tight and the cybersecurity skills shortage continues to worsen. Additionally, security teams need multiple tools to protect all the elements of their attack surface. If these tools are not fully integrated, the resulting architecture can be time-consuming and produce disjointed results, necessitating even more security expertise to interpret the findings.

Let’s use code security as an example. How complex do you think it would be to correlate the results from these three common scanning tools?

- A Static Application Security Testing (SAST) scan that reports vulnerability data by source code line number;
- A Dynamic Application Security Testing (DAST) scan, which typically reports the vulnerability by URL and HTTP request data; and

- A Software Composition Analysis (SCA) scan, which provides a library, the library version and a list of Common Vulnerabilities and Exposures (CVEs) in those libraries.

Given that these three tools report their results using totally different fields, correlating and normalizing all these reports to get a clear picture of security exposure is a daunting endeavor.

The end result is a tug-of-war between resources, launch schedules, hiring talent and the number of security tools needed to maintain a robust cybersecurity program.

I. Traditional approaches take nearly two months

The primary goal of a cybersecurity program is to ensure the overall security of an organization. When it comes to protecting applications and application programming interfaces (APIs), one important measurement of how well you're doing is the mean time to remediate (MTTR) software vulnerabilities. Minimizing MTTR speeds release cycles and helps prevent problems in production.

Unfortunately, organizations take nearly two months on average to remediate just the most critical vulnerabilities. Security teams must quickly and accurately identify vulnerabilities and work closely with development teams to resolve the issues. The challenge lies in navigating a market saturated with vendors specializing in SAST and DAST technologies. (For an in-depth report by IDC on these approaches, click here, or for a concise version, click here.)

There are two fundamental problems that arise when an organization depends on these systems:

1. Security teams are overwhelmed by the number of detected vulnerabilities when utilizing SAST and DAST. Out of the box, these scanning tools generate inaccurate results with many false positives. The sheer volume of detected vulnerabilities can't simply be handed off to development. Often, the list is passed between security and development teams like a hot potato because neither has the bandwidth to validate what is real and what is noise. Moreover, opening hundreds or thousands of tickets is undesirable for both parties.

2. Scans can take hours or, in some cases, days to complete. The combination of extensive, noisy lists and long feedback loops causes teams to adopt a waterfall or sprint cycle approach, slowing down development.

Typically, the process unfolds as follows:

- **Applications are scanned by the security team:** 4 to 7 days
- **Results are analyzed by security experts:** 14 days
- **Tickets are created:** 7 days
- **Remediations are integrated into sprint cycles:** 30 days
- **Best scenario total: 54 to 58 days—if everyone works in sync and maintains high priority**

In about two months, priorities and business scenarios shift to the next pressing issue, causing many tickets to turn into backlogs or to be left behind.

BRINGING DOWN THAT MTTR TO JUST 8 DAYS

How can an organization streamline these processes and bring down MTTR? The most powerful approach is to deliver real-time analysis and remediation through security instrumentation during development and runtime analysis in production.

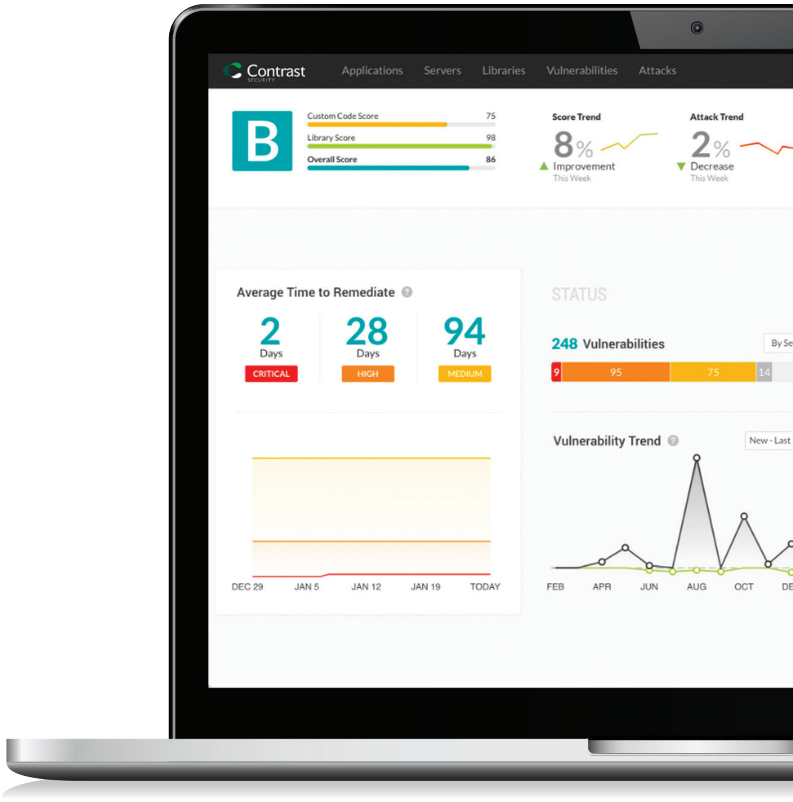
Contrast Assess enables development and security teams to detect vulnerabilities in real time from within the application itself. This helps organizations reduce MTTR to just eight days. With real-time results, development and security teams can examine the findings together, enabling an instantaneous feedback loop. This allows organizations to address security issues before they become significant threats. The real question is: What will the security team be able to accomplish when there is no backlog?

II. No experts? No problem.

As we said, companies struggle to hire cybersecurity experts these days. A professional with the specific skills your organization needs may be difficult or impossible to find. And if you have multiple security tools that need dedicated experts to manage them, you may be out of luck.

One way to withstand the current expert shortage is to rely less on experts — and more on platforms like Contrast's Secure Code Platform. The platform, which includes Contrast Assess, is unique because it analyzes all the libraries and lines of code just like an expert would. It monitors all the normal interactions with the endpoints and provides clear visibility of all the vulnerabilities that exist on a single UI dashboard.

By using a platform like Contrast Secure Code, security teams can reduce the number of tools needed, as it provides all the necessary insights and mappings. This approach drastically lowers the number of security experts required and reduces the total cost of ownership (TCO) of security operations. Just imagine that: a world where security experts can focus on other pressing matters while benefiting from an efficient, streamlined cybersecurity process.



III. How well do you really know your applications?

Contrast Assess uses deep instrumentation as a vital component to understanding and securing the application. Instrumentation enables informed decision-making that would be impossible with a static view in time. Here’s how it bolsters a company’s security posture:

1. It allows the company to detect security incidents or anomalies in real time, as the instrumentation generates logs that can be used to identify unusual activity.

2. It helps the company to identify and fix security vulnerabilities in the application by providing visibility into how the application is being used and any potential weaknesses that may be exploited by attackers.

3. It enables the company to track and monitor user activity within the application, which can be useful for identifying potential insider threats or unauthorized access to sensitive data.

4. It helps the company to comply with regulatory requirements and industry standards that mandate the use of certain security controls, such as logging and monitoring.

Deep knowledge of your applications helps determine the number of real vulnerabilities and their locations, eliminating false positives. Developers can swiftly address critical vulnerabilities, especially those within frequently used traffic routes. Security teams can identify the most significant risks in their applications and develop countermeasures. And they achieve efficiency through accurate remediation without the burden of false positives.

Final thoughts

Contrast Assess, part of the Contrast Secure Code Platform, can help organizations recession-proof their application security program in 2023. By using this tool, organizations can reduce MTTR in order to remediate critical vulnerabilities, from two months to just eight days. This enables them to address security issues before they become significant threats. It also allows security teams to monitor their applications in real time and identify potential insider threats or unauthorized access to sensitive data.

Additionally, Contrast Assess drastically reduces the number of security experts needed, thereby lowering the TCO for security operations. Furthermore, it can quickly identify vulnerabilities in an organization’s code, allowing developers to fix them before they become problems. In summary, Contrast Assess provides organizations with a powerful tool to stay ahead of security threats and protect themselves in a recession.

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

Contrast
SECURITY

contrastsecurity.com