

Who's Watching Your Applications and APIs **Right Now?**

Why the Financial Sector Needs
Real-Time Runtime Security.



Security must move at the speed of development

Protecting customer data is always top of mind in the financial sector, but, unfortunately, the work of security teams is never done. Cybercrimes are increasing and growing more complex.

In 2023, ransomware attacks surged thanks to the use of artificial intelligence by cybercriminals.¹ Also, an estimated 97 zero-day vulnerabilities were exploited in the wild—a 50% increase over the previous year.² And application and application programming interface (API) attacks also intensified. This ever-shifting kaleidoscope of risks is just one reason why more than 70 Fortune 500 companies in the financial sector are already working with Contrast Security.

Criminals won't rest in their search for the next big payoff, but your security team cannot work around the clock alone. It's necessary to look beyond legacy tools in favor of real-time, runtime solutions that can automatically monitor applications and API code inside and out—and keep your data protected from within, whatever the next wave of crime may bring.



¹ Contrast Security, "Modern Bank Heists Report 2024."

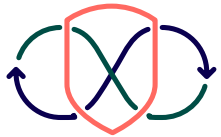
² Google, "A Year in Review of Zero-Days Exploited In-the-Wild in 2023," March 2024.

To see every threat, look in every corner

Web applications are among the assets most impacted by security incidents.³ But it's important to remember the application itself is not necessarily the prize for attackers. More than half of financial sector leaders experienced island-hopping, a tactic in which cybercriminals attack a company's applications or APIs to get access to customer data.⁴ Creating a security strategy that overlooks application and API security is a little like building a steel-clad bank and leaving a side door open.

Contrast Security's Runtime Security platform offers continuous, accurate, and scalable application and API security. Runtime Security observes the full application stack as it runs, monitoring for attacks targeting zero days, custom code and third-party vulnerabilities, which is essential for operating in the cloud. This mitigates the exploitability of security debt and prevents insecure programming while saving time.

With one platform to manage it all, it's easier for teams to implement and more effective at preventing attacks across your entire portfolio.



³ Verizon 2023 Data Breach Investigations Report.

⁴ Contrast Security, "Modern Bank Heists Report 2024."

Revealing hidden threats

In the 2024 Modern Bank Heists Report, financial sector security leaders from around the world reveal the types of attacks they're seeing and what threats they're most concerned about. **Among the latest findings:**

58% saw an increase in application attacks

77% experienced attacks on APIs

45% believe they experienced attacks that went undetected

You can't protect what you can't see

According to one report, 97% of companies don't have adequate visibility into their cloud-native applications.⁵ This can create huge blind spots that become playgrounds of exploitable security debt for criminals to explore.

Even established application and API security approaches, including scan-, perimeter- and pen testing-based methods, do not continuously monitor code at runtime. As security threats rapidly evolve, these traditional tactics are unlikely to keep pace.

Further, the noise of false positives can dilute and even thwart your team's good-faith efforts. To address more issues faster, teams need help accurately identifying real vulnerabilities in real time.

Embedded directly into software via instrumentation, Runtime Security can see what was previously invisible within a fully assembled application or API and detect vulnerabilities that may have been missed.

This lets Runtime Security provide greater context about each vulnerability detected and results in dramatically reduced false positives, so teams have more time and resources to respond to the most pressing threats. And the platform supports faster remediation by providing detailed guidance on how to isolate, triage and understand vulnerabilities.

What's included in a continuously updated Runtime Security blueprint:

- Attack paths to exposed endpoints
- Security mechanisms/controls at work
- Dangerous behavior that occurs on routes and the ability to stop its execution
- Context on back-end connections

⁵ Tigera, "The State of Cloud-Native Security," April 2022.

Blind spots in applications and API code can become playgrounds of exploitable security debt for criminals to explore.

Results we've seen so far

- Mean time to remediate (MTTR) **reduced from 275 days to three.**
- New vulnerability rate **reduced from 50+ per year to 11.**
- Code analyzed **10x faster than traditional tools**, such as dynamic application security testing (DAST).



If you're not protecting everything, you're not protected

With one platform, Runtime Security can monitor thousands of applications with fully distributed infrastructure—including third-party applications—without requiring extra infrastructure or manual scans.

Runtime Security is designed to automatically detect all known and unknown vulnerabilities, including those documented in the [OWASP Top Ten](#). And the platform works almost anywhere, including data centers, containers, and the cloud—helping you prevent attacks in production and detect vulnerabilities in development.

With this platform, vigilance becomes more sustainable across the software development lifecycle (SDLC). Runtime Security seamlessly integrates into developer tools, such as integrated development environments (IDEs) and continuous integration and continuous delivery (CI/CD) pipelines.

Runtime Security also supports all major languages and frameworks, including Java, .NET Framework, .NET Core, Node, Ruby, Python, Kotlin, Scala, PHP, and Go. It integrates easily with almost any tool, and insights can fold into existing reporting methods. No additional dashboards are required.


Compliance ready

The Runtime Security platform is designed to maintain compliance with a wide range of standards, including:

 [National Institute of Standards and Technology \(NIST\)](#)

 [Open Worldwide Application Security Project \(OWASP\)](#)

 [PCI Data Security Standard \(PCI DSS\)](#)

 [Defense Information Systems Agency \(DISA\)](#)

 [Cybersecurity & Infrastructure Security Agency \(CISA\)](#)

“

In order to release code more rapidly, we are seeing more aspects of the SDLC being forced to shift left. Due to the rapid pace of the speed in which software is updated and delivered, automated application security via Contrast enables us to deliver on this.”

Lori Temples, Senior Director of IT Security,
GreenSky

“Contrast has increased our confidence in the quality and security of our applications. It has empowered our developers, and it is an integral part of our SDLC. It has enhanced developer productivity and security.”

Gartner Peer Insights



Secure applications from within

As institutions across the financial sector continue to advance their digital transformations in the cloud, security teams must scale their efforts to continue safeguarding customer data. However, sustaining security vigilance throughout digital transformation and at scale in the cloud requires time, expertise and resources that some teams simply do not have in-house.

Runtime Security extends robust protection across the entire SDLC. It enhances vulnerability detection in third-party applications and libraries and it provides real-time defense against both known and unknown zero-day threats.

Continuous, accurate and scalable, the Runtime Security platform delivers everything you need to secure your applications and APIs from within—and protect your customers from relentless risk.

See Runtime Security at work. [Request a demo.](#)

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep-security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches and secure the entire enterprise from development, to operations, to production.

6800 Koll Center Parkway
Suite 235
Pleasanton, CA 94566
Phone: (888) 371 3333