REPORT

Contrast SECURITY

# Modern Bank Heists Report

## 2024


—Tom Kellermann, CISM
Senior Vice President
of Cyber Strategy, Contrast Security

# Table of Contents


01 2024 Cyberattack trends

02 Application Security

03 Trends in cyber defense

04 Contrast report methodology

# Foreword

The magnitude and the complexity of cybercrime attacks continue to grow each year. The ingenuity and imaginations of the criminals are impressive, as the world of cybercrime continues to evolve from past pig butchering[1], ransomware[2] and business email compromise (BEC)[3] attacks to sextortion and cryptocurrency scams. But the focus on financial institution (FI) cyberattacks is more alarming because of the monetized payoff when the criminals succeed. As the criminals' attacks evolve, the rest of the world must evolve as well, or we will become the next victim.

— Derek Booth
Assistant to the Special-Agent-in-Charge, U.S. Secret Service,
Head of the Mountain West Cyber Fraud Task Force

[1] Pig butchering scam explained: Everything you need to know | TechTarget
[2] Report: How financial firms are fending off ransomware | Contrast Security
[3] Financial cybercrime trends: Reverse BEC & 'shoxing' | Contrast Security

# Executive Summary

This annual report sheds light on the cybersecurity threats facing the financial sector. The report provides cyber ground truth, specifically manifesting an eye-opening perspective on the changing behavior of cybercriminal cartels and the defensive shift of the financial sector. In this year's report, financial sector security leaders from around the world revealed during a series of interviews the type of attacks they're currently seeing, what threats they're most concerned about and how they're adjusting their security strategy.

# 01

## 2024
## Cyberattack trends

# 2024 Cyberattack trends

2024 ushered in the evolution of cybercrime cartels. Cybercrime conspiracies in the financial sector have evolved dramatically. New attack vectors are being employed, and systemic attacks are being launched against critical infrastructures within the sector.

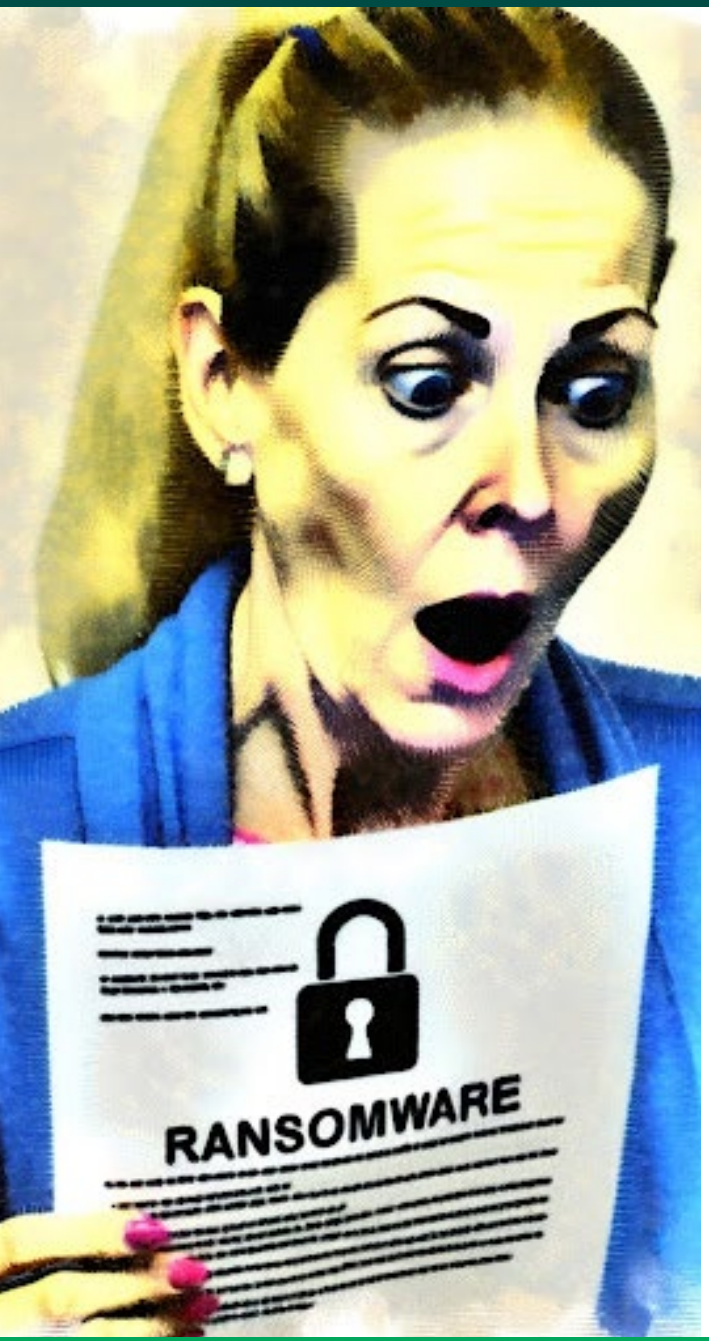
## 58% EXPERIENCED COUNTER-INCIDENT RESPONSE.

Counter-incident response occurs when adversaries disable cybersecurity agents, manipulate logs or timestamps, or launch distributed denial-of-service (DDoS)[4] attacks to slow the victim's response.

## 45% BELIEVE THEY HAVE BEEN SUCCESSFULLY ATTACKED WITHOUT HAVING DETECTED THE ATTACK.

This is a jarring admission. Given the increase of application and application programming interface (API)[5] attacks[6], coupled with the trend for adversaries to counter incident response, many FIs can suffer a stealthy intrusion[7].

[4] Malicious Cyber Intrusion: DDoS | Contrast Security
[5] Contrast API Security Testing Platform | Contrast Security
[6] Feeble APIs = Feeble app security | Contrast Security
[7] If you're seeing zero API attacks, you're probably not detecting them | Contrast Security




## 48% HAVE BEEN VICTIMIZED BY INTEGRITY/DESTRUCTIVE ATTACKS.

Destructive attacks[8] are launched punitively to destroy data.

In the past year, 48% of financial institutions (FIs) were victims of destructive attacks. It is worth noting that cybercriminals in the financial sector will typically leverage destructive attacks as an escalation to burn the evidence as part of a counter-incident response. Destructive malware variants seek to destroy, disrupt or degrade victim systems by taking actions such as encrypting files, deleting data, destroying hard drives, terminating connections or executing malicious code.

## 42% WERE IMPACTED BY A RANSOMWARE ATTACK.

Ransomware attacks surged in 2023 due to the use of AI by cybercrime crews to improve distribution. One recent example occurred in early December 2023, when attackers targeted a cloud service provider named Ongoing Operations[9]. The downstream effect: Island hopping affected data processors and about 60 credit unions using the Ongoing Operations environment. The systemic ransomware attack rippled out, causing outages and otherwise disrupting banking operations for a wide swath of the primary target's customers. Although ransomware is a significant threat to many sectors, FIs are collectively more prepared to mitigate these threats due to the widespread use of endpoint detection and response (EDR), microsegmentation, immutable backups and regular threat hunting.

[8] Report: Cyberattacks against financial sector surge 64% | Contrast Security
[9] 60 credit unions facing outages due to ransomware attack on popular tech provider | The Record

## 52% HAVE BEEN VICTIMIZED BY ISLAND HOPPING[10].

The financial sector is being targeted by cybercrime cartels and nation-states that are evolving in both attack sophistication and organization. A recent example of island hopping is the MOVEit vulnerability[11]: In June 2023, a number of organizations whose supply chains use the MOVEit application suffered a data breach as a result of criminals exploiting the vulnerability, with customer and/or employee data being stolen at organizations including the BBC, Aer Lingus and British Airways.

Cyber defenders must modify their response to these cartels and embrace situational awareness. These are not the bank heists of old, as mere wire transfer fraud is no longer the ultimate goal. Cyber cartels' objective is to hijack the digital transformation of an FI.

The modus operandi is simple: Infiltrate the corporate environment via application attacks or API attacks and then use access to the environment to launch attacks against the customer base. This is called island hopping[12]. There has been a dramatic increase in island hopping — an increase that represents a tremendous operational and reputational risk to victim organizations. Cybercrime cartels have studied the interdependences of FIs and now understand which managed service provider (MSP) is used and who the outside general counsel is.

FIs are concerned with the security posture of their shared service providers. Shared service providers, when compromised, pose a systemic risk to the financial sector, as their infrastructure can be polluted to attack dozens of FIs at a time. This form of island hopping is very concerning.

[10] The evolution of island hopping | Contrast Security
[11] MOVEit vulnerability and data extortion incident | National Cyber Security Centre
[12] Brand protection in an era of island hopping | Contrast Security

## 43% HAVE BEEN TARGETED BY WATERING-HOLE ATTACKS.

Similar to how predators stake out watering holes to attack their prey, in watering-hole cyberattacks, adversaries hijack and booby-trap a website or mobile app used by e-finance customers. Eventually, financial customers who visit the compromised site or who use the poisoned application get infected with the malware that adversaries have planted to compromise their data or systems.

## 58% SAW AN INCREASE IN APPLICATION ATTACKS.

Application attacks such as Class Loader manipulation[13], Expression Language Injection[14] and untrusted deserialization[15] are becoming more common. The new threats to supply chains are targeting software development, integration and delivery infrastructure.

[13] Contrast Protect Blocks Spring4Shell | Contrast Security
[14] Expression Language Injection | OWASP Foundation
[15] Deserialization of untrusted data | OWASP Foundation

# 02

# Application Security

## Application Security

In this section we will take a deep dive into the state of play of Application Security (AppSec) in the financial sector. The findings are eye-opening.

# 38%

**HAD AN APP/API SECURITY BACKLOG[16] OF 100,000 ISSUES OR MORE.**

Carrying this level of vulnerability is expensive and dangerous for the FI and customers alike. It also slows down innovation. In order to address this situation, continuous monitoring must extend to development.

# 55%

**ARE SHARING APP/API THREAT INTELLIGENCE[17] WITH DEVELOPMENT TEAMS.**

Organizations are creating fast cyber-feedback loops from production to development to ensure risks are prioritized properly and addressed quickly.

[16] Learn about the hidden dangers of traditional AppSec tools and why Runtime Security is replacing them: podcast writeup | Contrast Security
[17] Building a modern API security strategy — API testing | Contrast Security

> “Finding vulnerabilities is of net negative value … unless you rapidly resolve them. Why do I say it’s net negative? It’s better to know than not know, right? You must know before you can resolve anyway, right? It’s net negative for several reasons. First, on the cost side of the value equation, you must pay for licenses and operate the tools to find them. Second, no matter how hard you work on minimizing the impact on development, there is always some impact. Third, and still on the cost side, you must manage an ever-growing inventory of vulnerabilities. However, the fourth and most important reason is on the other side of the value equation, meaning that your liability and compliance risks exhibit a huge step-function increase once you know about a vulnerability. It’s infinitely better from a legal perspective to be able to honestly say, ‘We didn’t know’ over ‘We knew but didn’t do anything about it until it was too late.’
>
> The key is to focus on the resolution rather than the detection. That seems obvious, but the most common pattern I see with the adoption of vulnerability detection tools is a focus on spreading the use of the tool as widely as possible as quickly as possible. What I recommend instead is a depth-first approach. Here’s how that works.

# 81%

## HAD A MEAN TIME TO REMEDIATE (MTTR) APP/API VULNERABILITIES OF 3 MONTHS OR LONGER[18].

42% had a mean time of 6 months or longer, thus leaving their organizations exposed to exploitation. (Note that there are much longer MTTR rates to be found — Veracode's State of Software Security 2022 report, for example, cites an MTTR of 290 days for static analysis, which is far slower than Runtime Security's remediation time.) Three months is an exceptionally large window of exposure, given that widespread, automated attacks generally start within one day of a new vulnerability being discovered.

# 58%

## ARE REQUIRED TO CREATE SBOMS TODAY.

Some government agencies are now mandating SBOMs. While SBOMs are only required by some agencies and vendors today, the market is trending toward high levels of adoption. That's true not only for government agencies; SBOMs are starting to be required across the entire supply chain for anyone doing business with governments around the world.

[18] Let's talk stats: Why AppSec's running on broken math | Contrast Security

“

For each development team, have them pick one application. Decide to focus on either the code you write (Common Weakness Enumeration- [CWE]-style vulnerabilities) or the third-party libraries you import (Common Vulnerability and Exposure- [CVE]-style vulnerabilities). Then set the policy dial on your tool so low — say, critical-severity only — that the development team is willing to commit to resolving all those vulnerabilities in one or two sprints. Then have them install a gate in their pipeline such that no future vulnerabilities of that type and severity will ever be promoted in the future.

You now have reduced the time between the second and third points on the vulnerability life cycle timeline to less than one day for that (admittedly) limited scope, but you've accomplished something super important. You've established a point below which you will never fall. You will never have a greater than one-day MTTR for that scope again. Perhaps more importantly, you've empowered them to take ownership of the security of the product they are building.

—Larry Maccherone, DevSecOps Transformation Architect

# 35%

**ONLY 35% CAN TRACE ATTACKS TO THE EXACT LINE OF CODE FOR THE VULNERABILITY THEY ARE TARGETING.**

Participants grade their visibility[19] into AppSec at a 3.5 out of 5.

## Observability is paramount

In today's AppSec, the details are mostly invisible. Security teams get vulnerability reports and possibly a Software Bill of Materials (SBOM), but very little about how security works across code, components, framework, platform and services. According to a Tigera report[20], 97% of companies are observability-challenged with cloud-native applications, for example.

The key to implementing a healthy and cost-effective AppSec program is understanding context and visualizing how the software works. One way for AppSec to do this is with security observability tools that automatically create full-context digital security blueprints by watching the software as it actually runs[21].

Traditional AppSec tools — such as Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA) and web application firewall (WAF) — can't provide this kind of visibility into system behavior. They don't have access to the necessary context. This lack of context prevents them from recognizing vulnerabilities, makes it difficult to prioritize properly and causes them to flag many false positives.

[19] Security Observability: Intelligent security assessment = seeing what others can't | Contrast Security
[20] MARKET REPORT: The State of Cloud-Native Security 2022 | Tigera
[21] How Security Observability Can Impact AppSec Teams | Forbes

Similar to performance observability tools, security observability tools are lightweight components that install on application and API servers quickly and with minimal configuration. Once the software starts, the AppSec blueprint is created almost immediately and updated continuously.

Based on real application behavior, this blueprint provides clarity amid complexity, as an alternative to wasting time in conversations with development teams manually drawing data flow diagrams and threat models.

Observability answers an essential question: What does each workload do? To answer, security teams need to know:

- What is the environment? Server, platform, upstream, configuration and other details?
- What route does data travel?
- What defenses are in place?
- How are authentication, authorization and logging managed and used, and how often?
- What dangerous functions are called, using which interpreters, parsers, file systems, network functions and more?
- What services and connections are used?
- What are the data characteristics?

Security observability monitors all application and API activities in multiple directions, including outbound calls to API endpoints, to provide an expanded view of system interactions, database connections and file system interactions. Security observability also identifies the nature and protocol of each endpoint in the system to provide a comprehensive view of the application diagram.

– Jeff Williams, CTO & Founder, Contrast Security

# 77% HAVE EXPERIENCED ATTACKS AGAINST THEIR APIS.

This is a 27% increase from last year's report, where only 50% of respondents had experienced an API attack. We will continue to see APIs increase as an attack vector for a number of reasons:

- The total number of public and private APIs in use is approaching 200 million[22].
- There is a shift in new development approaches to microservices architecture.
- Shadow APIs abound.
- Continuous development leads to sprawl and versioning issues.
- Hybrid apps spanning on-premises, cloud and serverless environments increase the attack surface.

In response to recent significant API vulnerabilities and breaches[23], we will see organizations fully include APIs in their AppSec practices. Organizations will move beyond legacy scan and firewall approaches in favor of inside-out solutions that can understand the full context of API code. Organizations will also expand their open-source security programs and runtime protection initiatives to specifically include APIs.

[22] Building a modern API security strategy — API inventory | Contrast Security
[23] T-Mobile hacked to steal data of 37 million accounts in API data breach | Contrast Security

# API security best practices

**01** Maintain a complete inventory of APIs running in your environments, in development and exposed in production.

**02** Ensure rigorous access control.

**03** Perform full security testing against running APIs during development to identify and remediate unknown vulnerabilities.

**04** Identify security gaps in the software supply chain. Find known vulnerabilities in active third-party libraries, frameworks and services.

**05** Validate schemas, ensuring proper API behavior per input and output.

**06** Protect against zero-day attacks from day one by ensuring all APIs are deployed with runtime protection[24] in place.

[24] It's time to replace our broken AppSec tools with something that actually works: Runtime Security | Contrast Security

Contrast SECURITY

## Trends in e-fraud

# 74%

### HAVE DETECTED CAMPAIGNS TO STEAL NONPUBLIC MARKET INFORMATION.

This was a 24% increase from the 2023 Cyber Bank Heists report[25]. This year's report validates that cybercrime cartels have realized that the most significant asset of an FI is not wire transfers or the access to capital; rather, it's nonpublic market information. This encompasses corporate information or strategies that can affect the share price of a company as soon as it becomes public, such as earnings estimates, public offerings and significant transactions. Fifty percent of financial institutions experienced attacks that targeted market strategies. This threat aligns with economic espionage and can be used to digitize insider trading and to front-run the market. Front-running is the illegal practice of purchasing a security based on advance nonpublic information regarding an expected large transaction.

# 48%

### EXPERIENCED AN INCREASE IN ACCOUNT TAKEOVERS.

Account takeovers are characterized by unauthorized individuals taking over someone else's online bank account. Incidence of account takeovers are still high due to inadequate customer device cybersecurity.

# 71%

### FEEL THAT GEOPOLITICAL EVENTS SERVE AS HARBINGERS FOR CYBERATTACKS.

Geopolitical tension is metastasizing in cyberspace. The majority of FIs stated that both Russia and China are both equally significant threats to cybersecurity in the financial sector. In the past, China was not considered a significant threat to the financial sector, but that has changed as economic espionage flourishes due to nationalism and protectionism.

[25] Cyber Bank Heists | Contrast Security

Contrast SECURITY

# 03

# Trends in cyber defense

## Trends in cyber defense

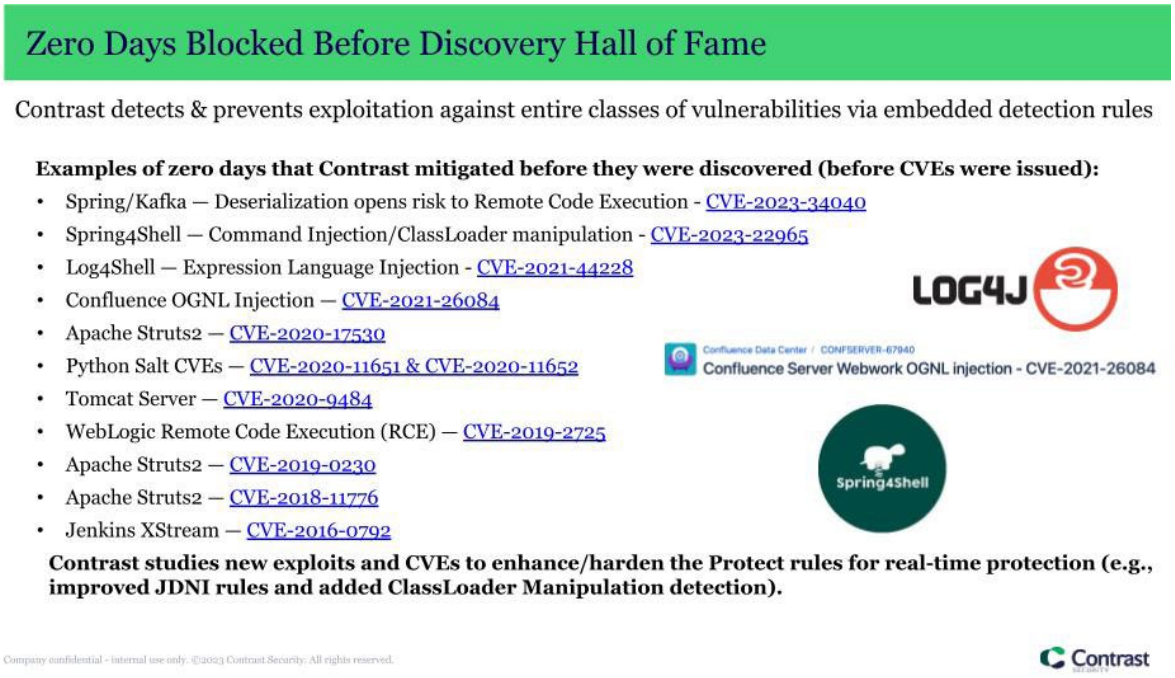
Offense must inform defense. Given the surge in API attacks, FIs are beginning to invest in API security tools and RASP.

**48%** CURRENTLY EMPLOY AN API SECURITY SOLUTION.

**52%** UTILIZE RUNTIME SECURITY — E.G., RASP.

It's worth pointing out that there's some overlap here, as Runtime Security provides both security testing and runtime protection for APIs as well as applications. But there's no question that protecting APIs is a key requirement for FIs.

The FIs that participated in this study stated that they will increase investment in Extended Detection and Response (XDR) and Managed Detection Services, API security and runtime protection. This was underscored by a Forrester survey of Security Technology Decision Makers wherein the vast majority of FIs have either adopted or plan to adopt runtime protection[26].




[26] Contrast Protect | Application and API Protection | Contrast Security

Contrast SECURITY

## Cyber governance

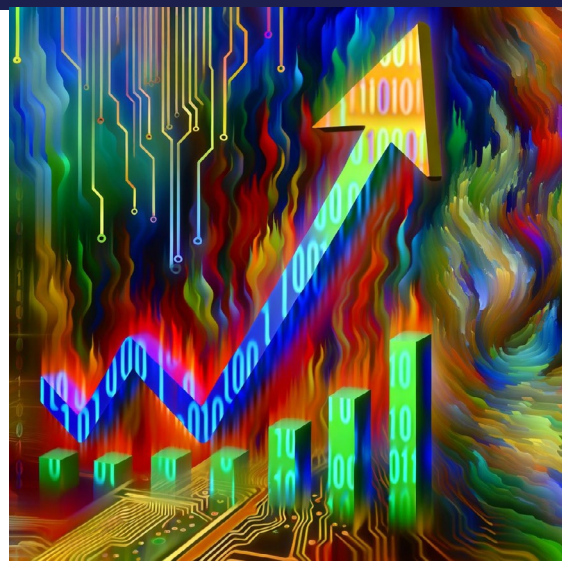
**42%** OF CISOS STILL REPORT TO CIOS.

This represents significant progress from last year. Chief information security officers (CISOs) are being empowered in the financial sector, yet more work needs to be done. We must provide CISOs with a direct line of access to the CEO, along with greater authority and resources. In CISA's Shields Up guidance[27], the need to empower CISOs is the top recommendation for corporate leaders and CEOs to better protect their organizations.

As detailed in CISA's guidance, "In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term." The defensive mindset is necessitated at the top. That's why proactive FIs have elevated their CISOs to report to the CEO.

**58%** WILL INCREASE THEIR CYBERSECURITY BUDGET IN 2024.

Whereas this is a decrease from last year's findings, I am heartened that most FIs are continuing to increase investment in cybersecurity. Consolidation of cybersecurity controls is occurring, but greater investment in best-of-breed platforms is now the priority.



**33%** OF FIS HAD A CYBERSECURITY SPECIALIST ON THEIR BOARD.

Objective, holistic security guidance is fundamental in an era of cybercrime conspiracies and cyberespionage. Having a cybersecurity specialist on the board increases the authority and resources endowed to the CISO. It also provides an objective perspective on cyber risk and correspondent priorities. On Dec 15, 2023, the Securities and Exchange Commission (SEC) adopted new rules[28] to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incidents by public companies. These SEC disclosure requirements are game-changing.

Cybercrime has a material impact on business operations. Cybersecurity can no longer be viewed as an expense but rather as a functionality of conducting business. This is no longer a question of duty of care but rather a duty of loyalty to the digital safety of your customers. Cybersecurity is a brand protection imperative. Trust and confidence in the safety of your institution depends on effectively mitigating and responding to cyberattacks.

[27] Shields Up | CISA
[28] Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure | SEC

# 04

## Contrast
## report methodology

## Contrast report methodology

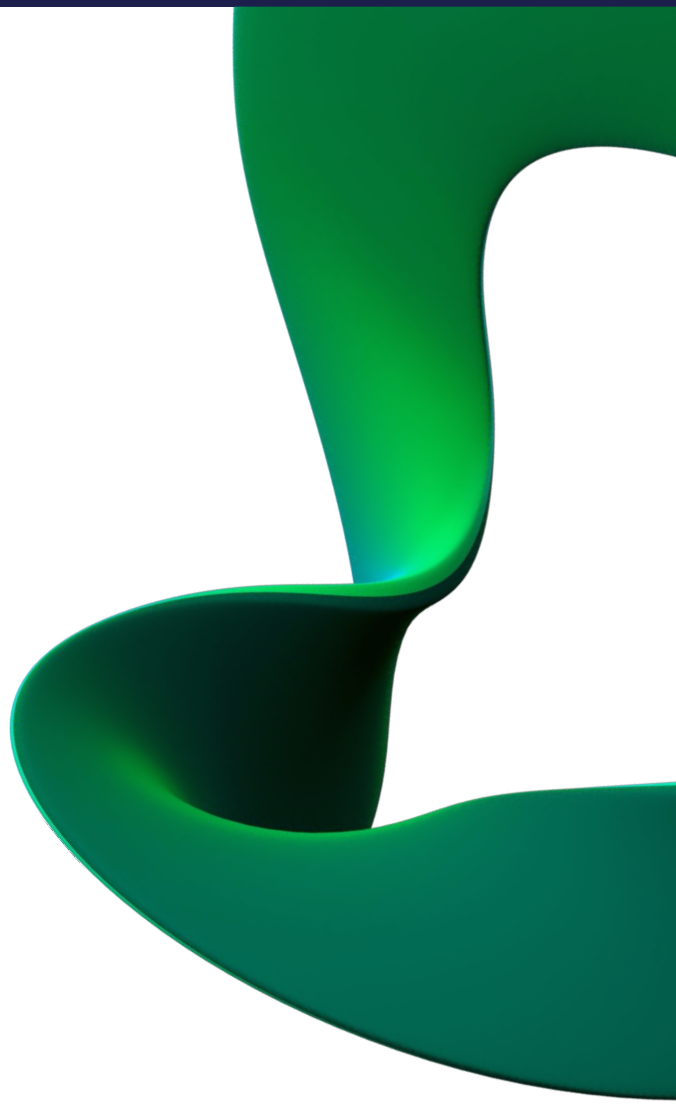
Participants interviewed for this study consisted of CISOs, SVPs of Cybersecurity, and Managing Directors of Information Security in Financial Institutions.

## About the author

Tom Kellermann is the Senior Vice President of Cyber Strategy at Contrast Security, Inc. Previously, Tom held the positions of Head of Cybersecurity Strategy for VMware, Inc. and Chief Cybersecurity Officer for Carbon Black, Inc., wherein he authored the "Modern Bank Heist Report" for the past six years. In 2020, he was appointed to the Cyber Investigation Advisory Board for the United States Secret Service. On Jan. 19, 2017, Tom was appointed the Wilson Center's Global Fellow for Cybersecurity Policy. Tom previously held the positions of Chief Cybersecurity Officer for Trend Micro, Inc., Vice President of Security for Core Security and Deputy CISO for the World Bank Treasury. In 2008, Tom was appointed a commissioner on the Center for Strategic & International Studies' (CSIS') Commission on Cyber Security for the 44th President of the United States. In 2003, he co-authored the Book "Electronic Safety and Soundness: Securing Finance in a New Age."

## About Contrast Security

Contrast is a leading Application Security vendor providing a unified Runtime Security platform that observes, tests and protects critical web applications and APIs in organizations around the world. Contrast's revolutionary technology enhances software to empower developers and protects against exploitation. Our innovative, instrumentation-based approach embeds trust boundaries in the application for the most accurate and actionable security outcomes in a fully automated manner. Development and security teams realize measurable increases in developer velocity, improvements to security posture and optimized efficiency while saving time and money. Modernize your application security program and empower your teams to innovate with confidence. Contrast's mission is to democratize software security and enable amazing Application Security outcomes.



Contrast SECURITY

**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