2022 CISO Research Report: Financial Services

Observability and security must converge to enable effective vulnerability management.

Introduction

Evolving customer demands and intense competition have driven massive digital change in the financial services industry. Throughout the sector, institutions providing retail banking, insurance, and investment services are harnessing new technologies to overhaul operations and deliver financial solutions in new, user-friendly ways.

To enable these capabilities, financial services providers are adopting dynamic multicloud environments, cloud-native architectures, and open source code libraries to improve digital agility. However, this has made it increasingly difficult to manage and reduce enterprise risk throughout the software development lifecycle.

The process of developing, testing, securing, and releasing applications and software updates has become more complicated, compounding the opportunities for vulnerabilities to enter the development lifecycle. The Log4j vulnerability that emerged in late 2021 demonstrated the severity of this problem, as it highlighted a serious gap in the security posture of countless businesses. Financial services firms were no exception, despite the fact that most have a robust, layered cybersecurity strategy.

This report explores these challenges and highlights how converging observability and security can enable more effective vulnerability management and attack detection and blocking across the financial services sector.

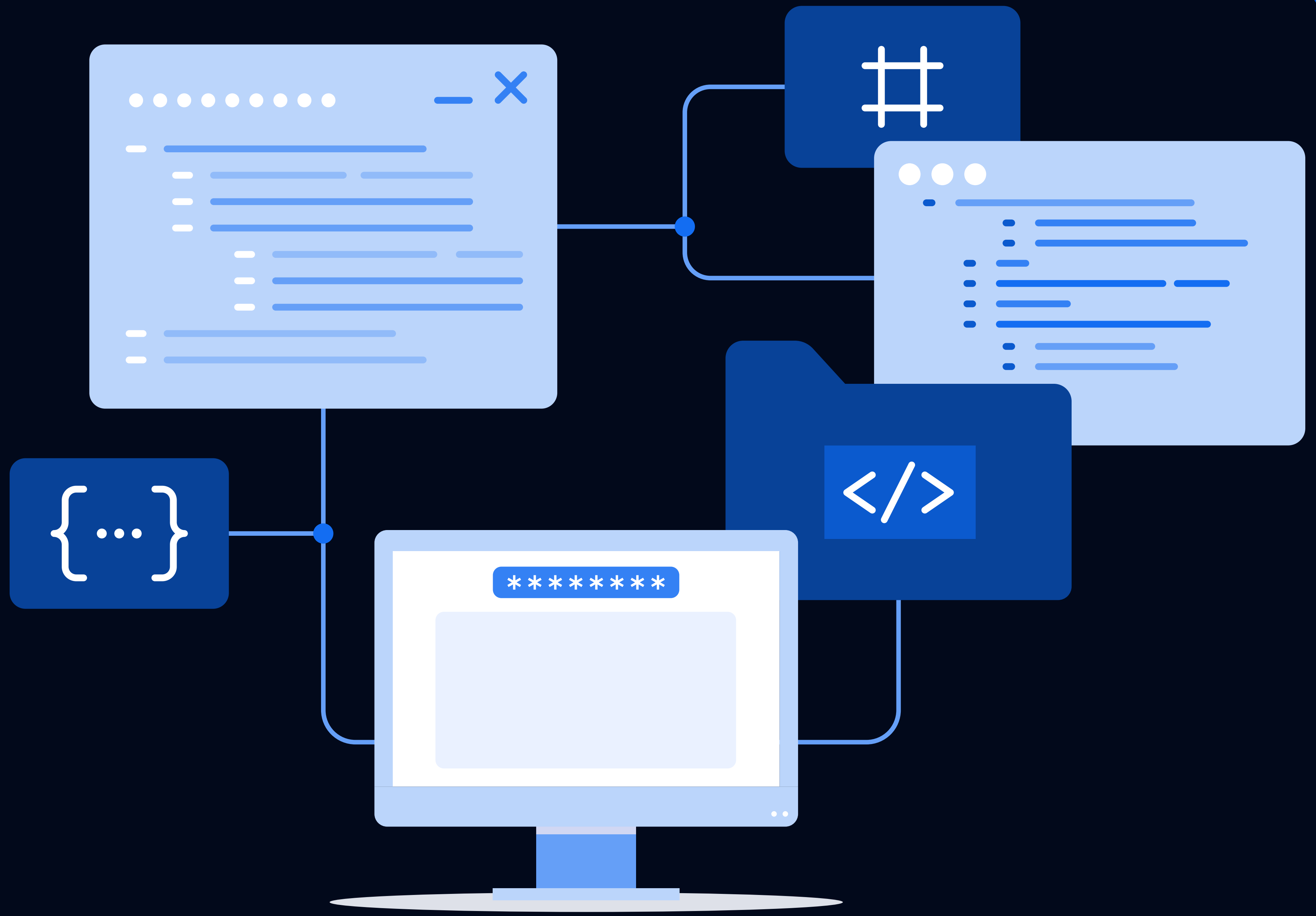
dynatrace

What's inside

CHAPTER 1

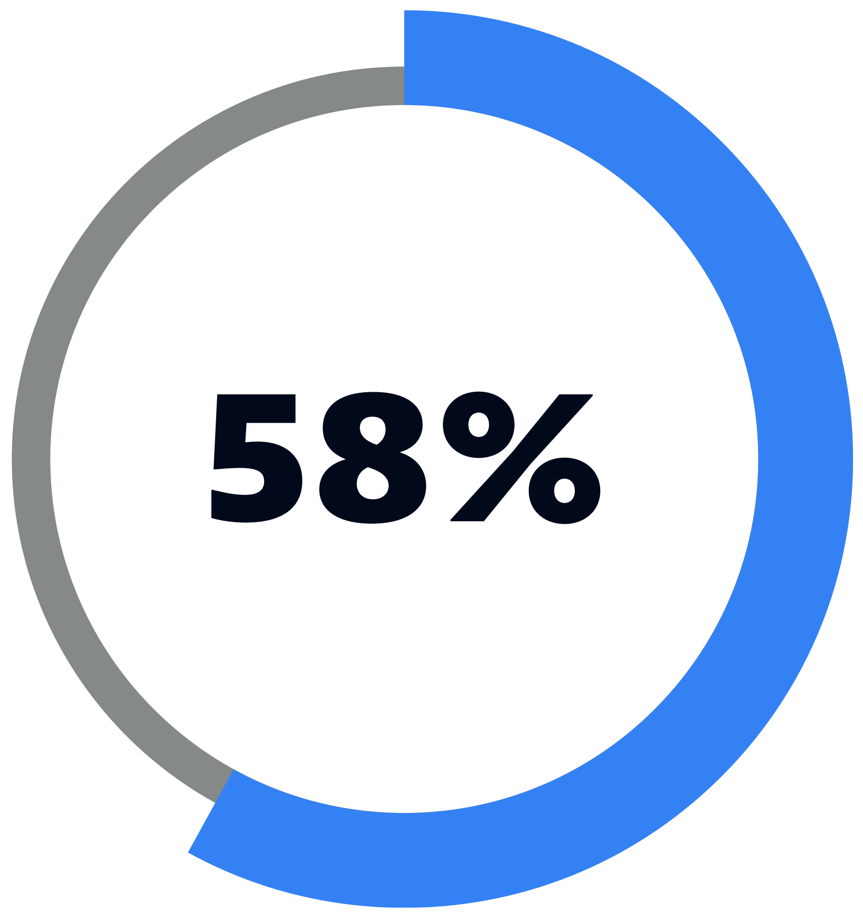
You can’t bank on layered security strategies

The rise of modern cloud environments has created a conundrum for IT, development, and security teams within the financial services industry. The growing use of microservices, Kubernetes, and serverless computing delivers greater business agility, but it also creates complexity for which many security solutions weren’t designed. Even with the most robust, layered approaches to cybersecurity, many organizations still lack the ability to see inside today’s dynamic containerized applications. They also struggle to access the context their teams need to distinguish a potential risk from a critical vulnerability that could be exploited. As a result, it’s increasingly difficult for them to manage the security of their applications at runtime, allowing more vulnerabilities to escape into production — where they can put sensitive financial data at risk.

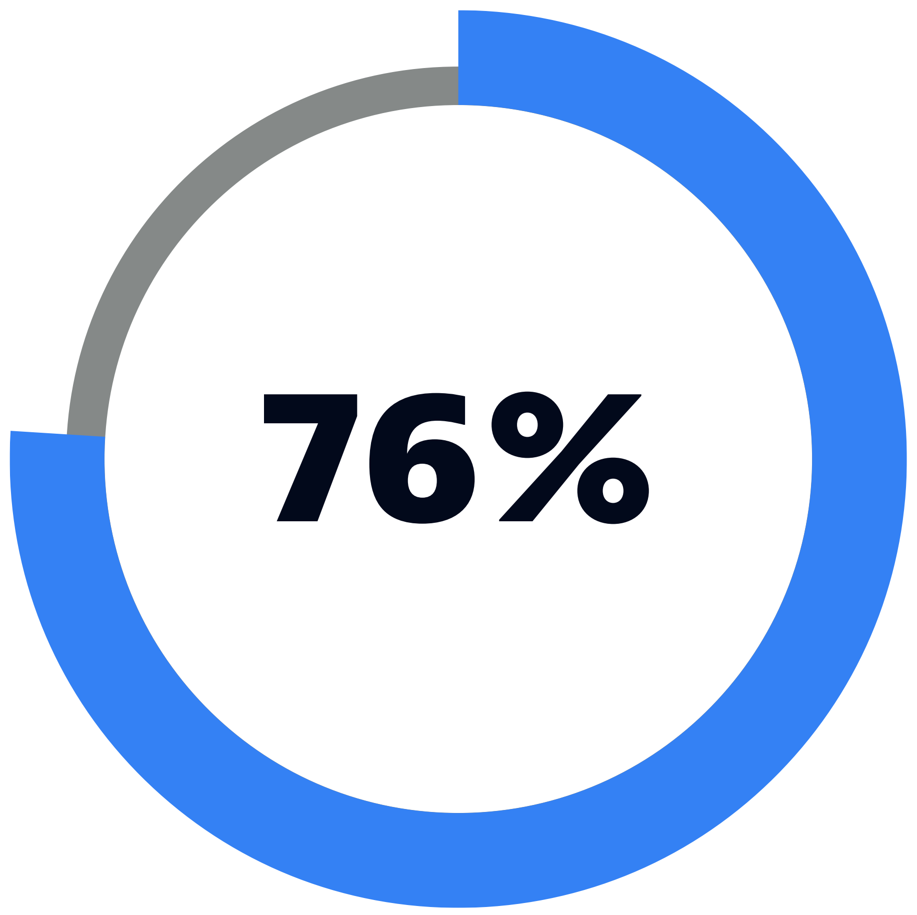


CHAPTER 1

You can’t bank on layered security strategies



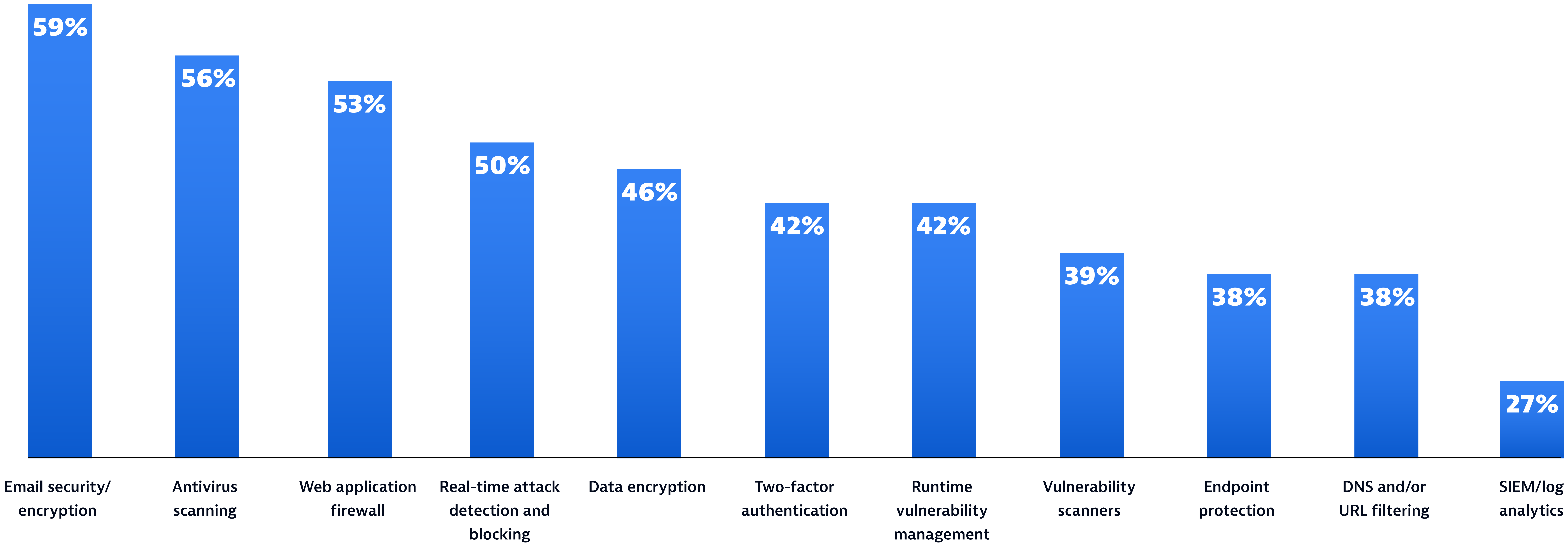
of financial services organizations have a layered cybersecurity posture, supported by five or more different types of security solutions.



of chief information security officers (CISOs) in the financial services sector say that despite having a robust, multilayered security posture, there are still gaps that allow vulnerabilities into production.

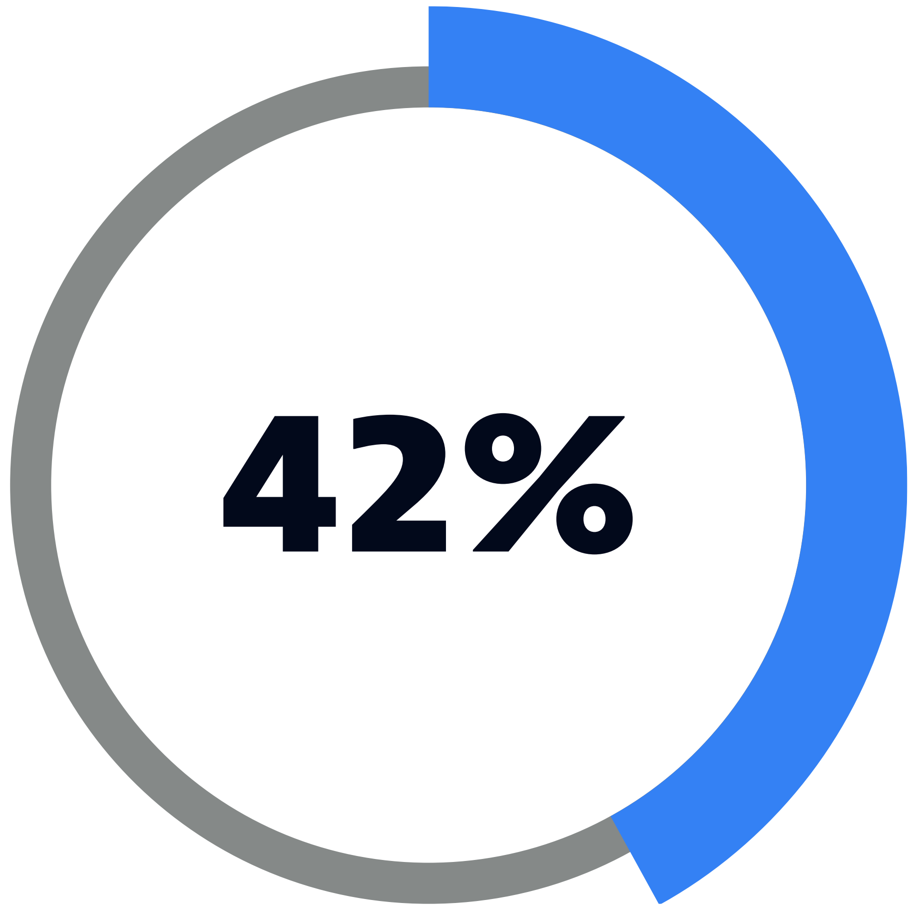
You can’t bank on layered security strategies

The most common security solutions organizations use are the following:

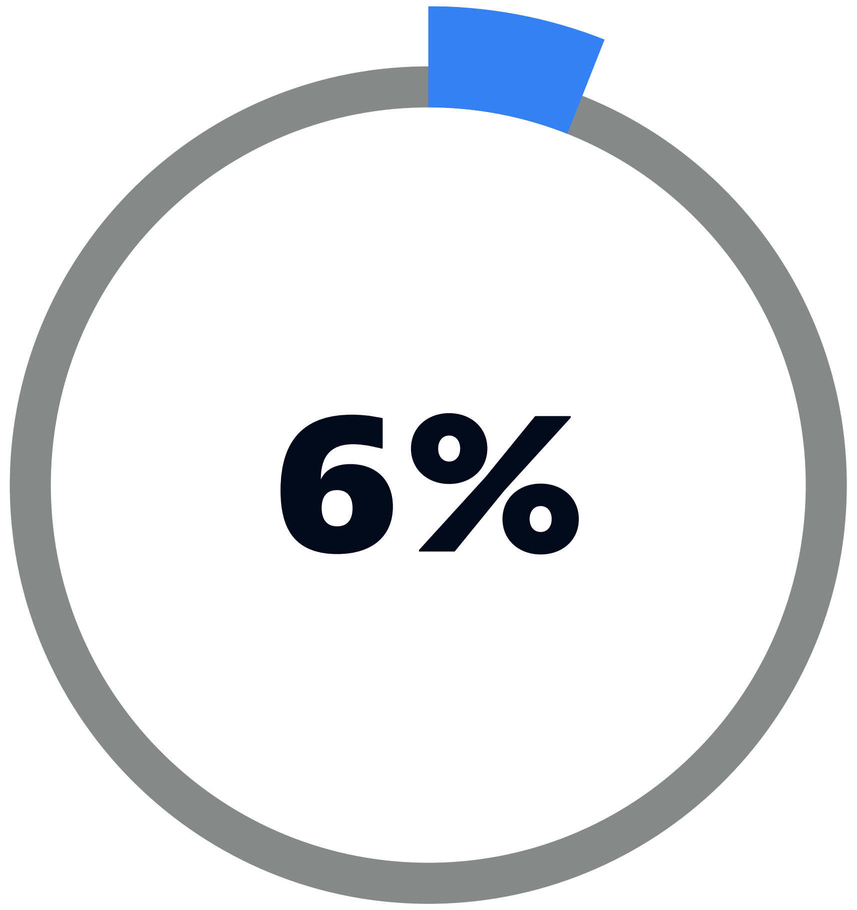


CHAPTER 1

You can’t bank on layered security strategies



of organizations have runtime vulnerability management capabilities.

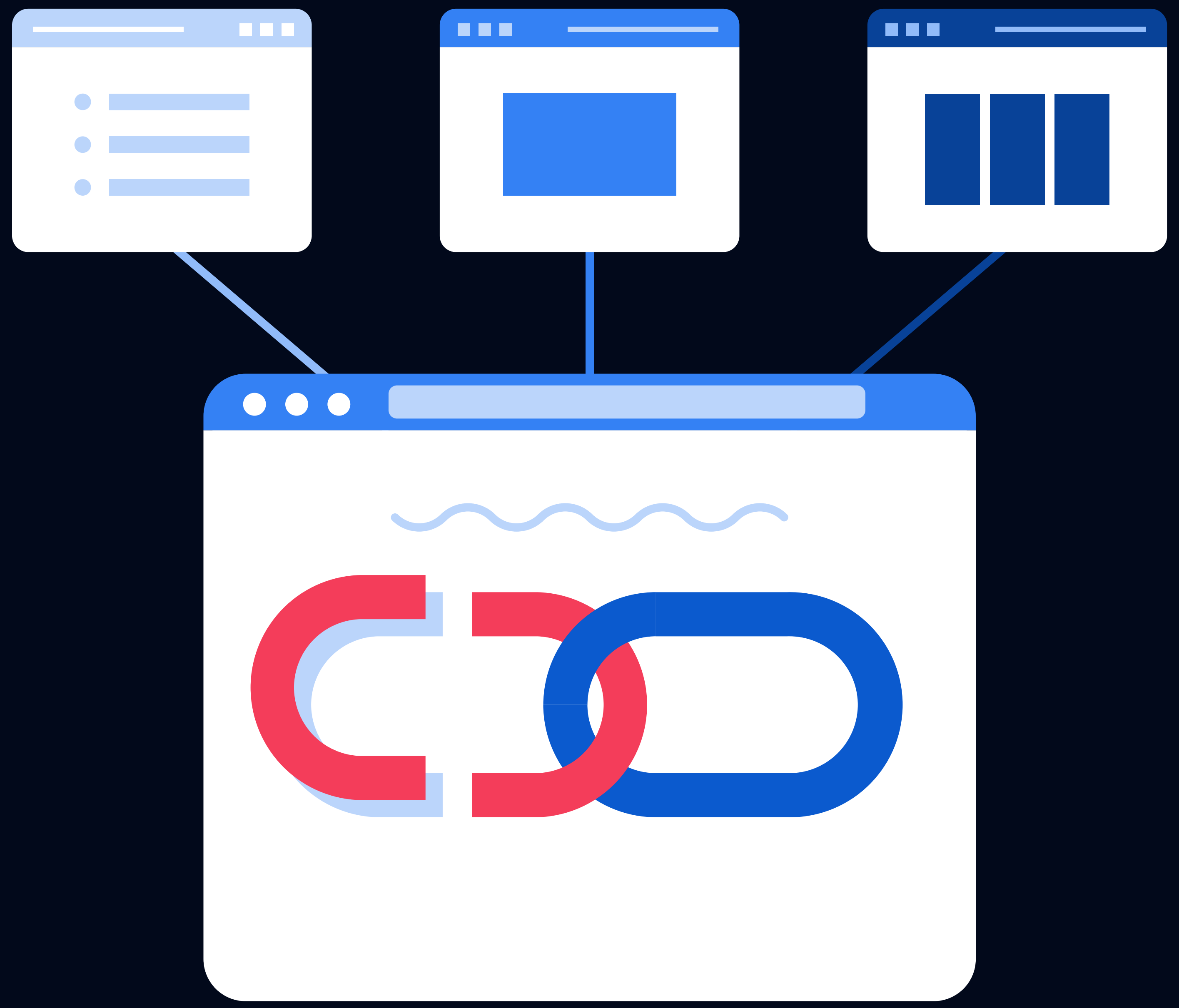


of financial services organizations have real-time visibility into runtime vulnerabilities in containerized production environments.

CHAPTER 2

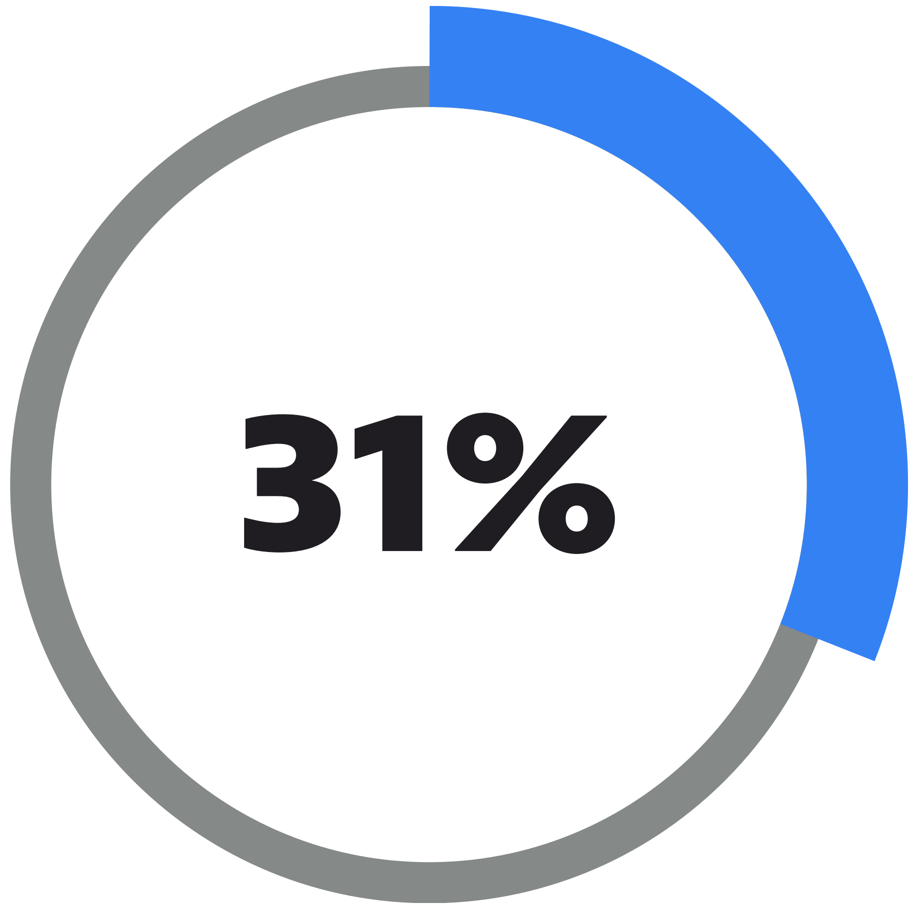
Open source software code can leave the bank vault unlocked

Financial services organizations are increasingly turning to open source code to accelerate innovation. However, these third-party libraries also introduce significant security risks, as they regularly contain vulnerabilities. With the emergence of Log4Shell in December 2021, and Spring4Shell just a few months later, identifying and remediating these vulnerabilities were difficult. Even if organizations can access a complete list of all code libraries running in production, assessing the impact of any vulnerabilities they contain and prioritizing which need to be resolved first has surpassed human capability.

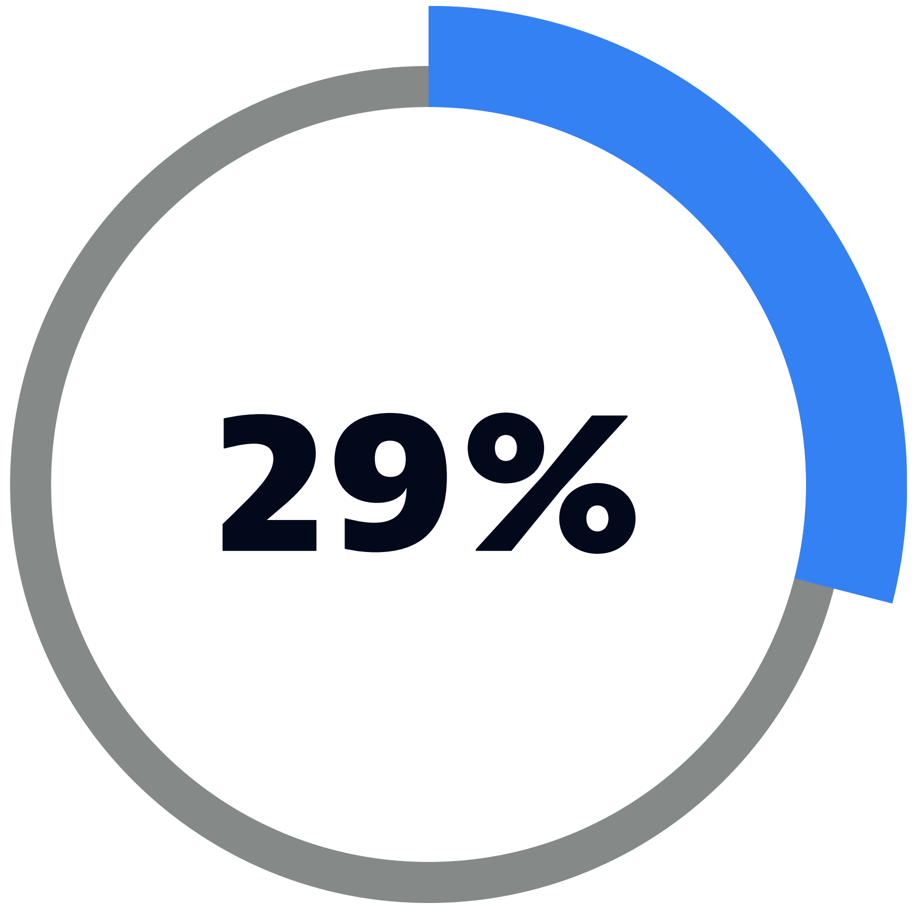


CHAPTER 2

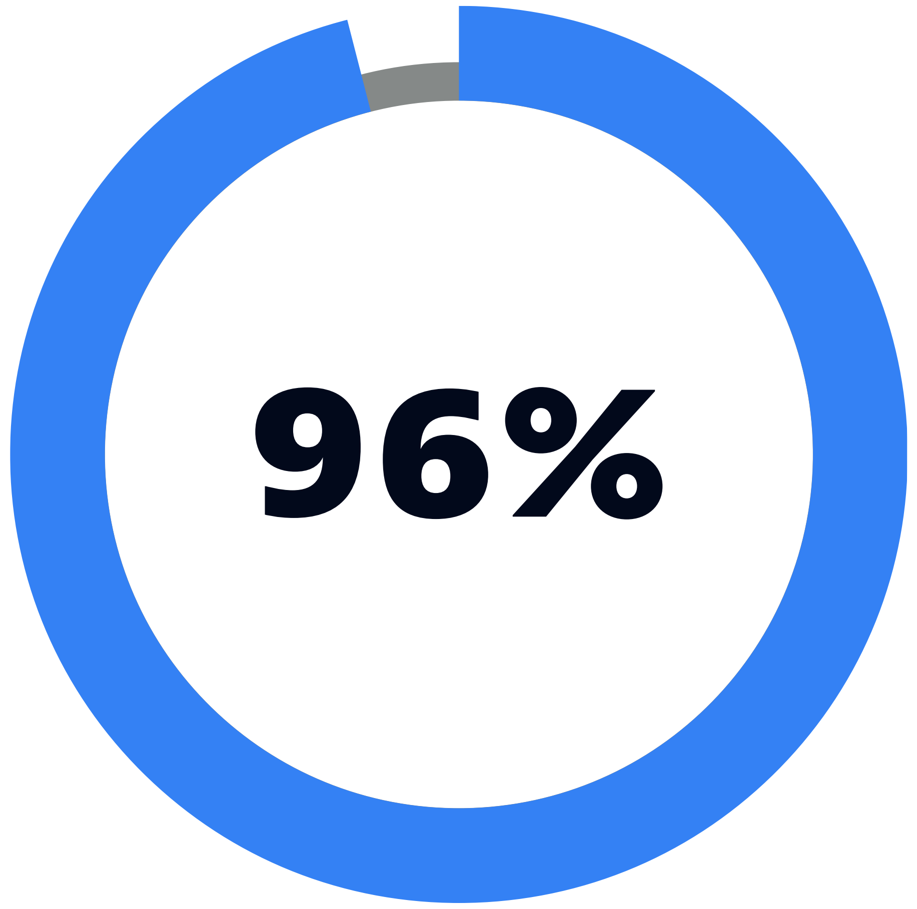
Open source software code can leave the bank vault unlocked



of security teams can access a fully accurate, continuously updated report of every application and code library running in production in real time.



of security teams admit they do not always know which third-party code libraries they have running in production.



of organizations say they faced risk exposure from Log4Shell, and 38% cited their risk as “high” or “severe.”

Key challenges security teams experienced in handling the response to Log4Shell included the following:

58%	Speed of development makes it difficult to prevent vulnerabilities from returning
52%	Volume of false positives or low-impact alerts make it difficult to prioritize which exposures to resolve first
47%	Limited collaboration between security and development teams delayed our response
46%	Significant manual effort to evaluate our risk exposure
35%	Limited or delayed insight into what is running in production
34%	Limited context within alerts to identify the risk impact

Most common responses in security teams when new major vulnerabilities such as Log4Shell are discovered include the following:

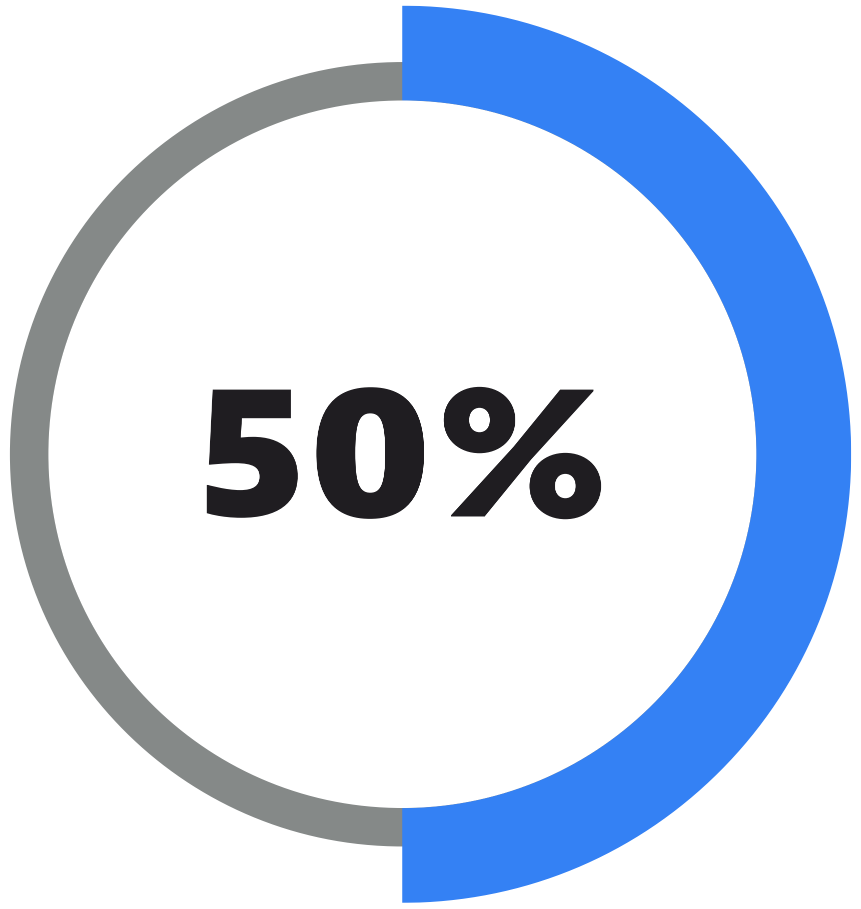
57%	Major increase in remediation tickets for development teams
52%	Significant increase in manual war rooms
47%	Tier-2 or -3 vulnerabilities are ignored while the focus is on the crisis
44%	Teams having to work around the clock
30%	Feeling of being overwhelmed
22%	Sense of panic

CHAPTER 2

Open source software code can leave the bank vault unlocked

56 hours

were spent on average by security teams responding to the Log4j vulnerability.



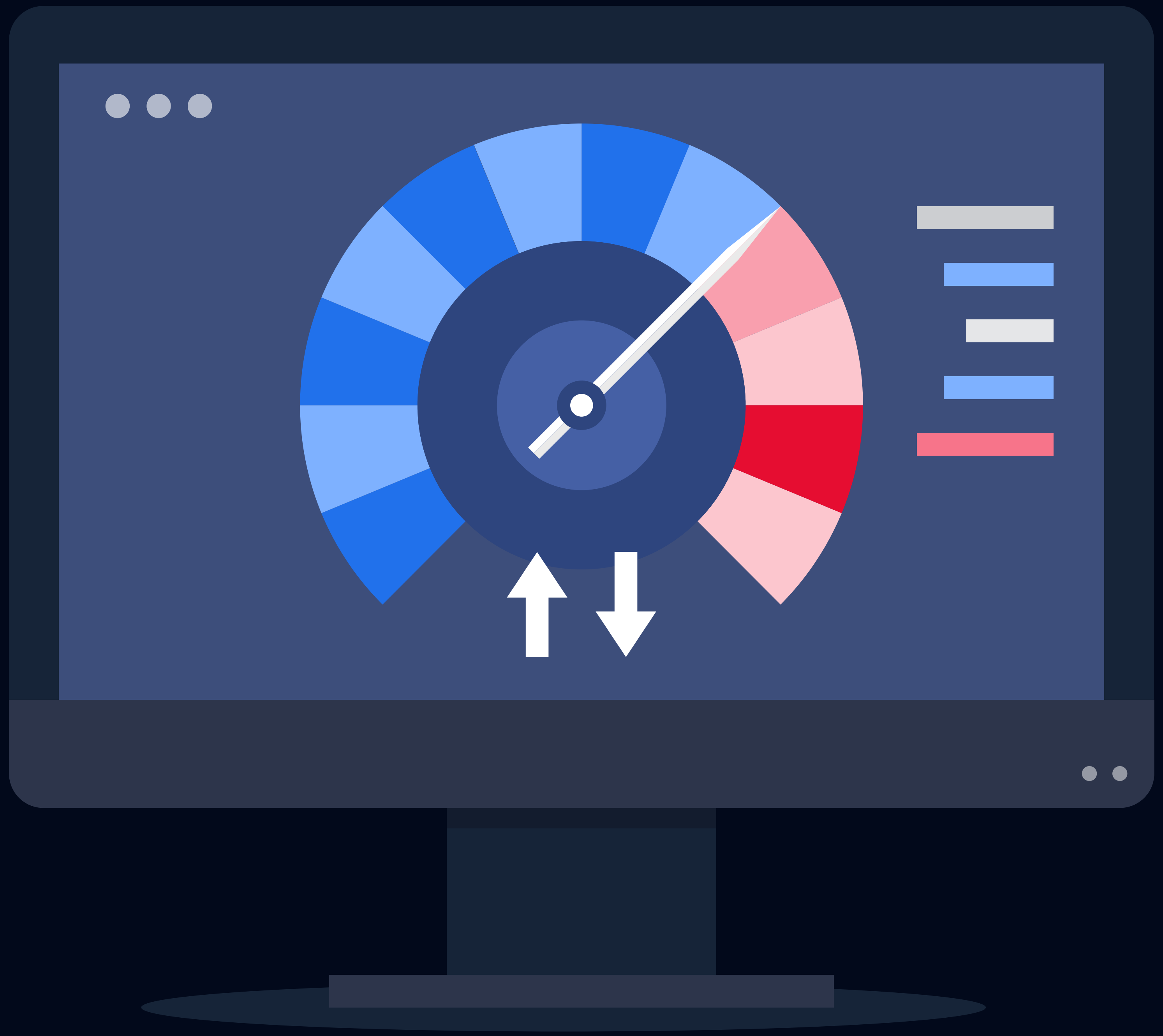
50%

of CISOs are fully confident their teams could identify and resolve all instances of Log4Shell in their environment.

CHAPTER 3

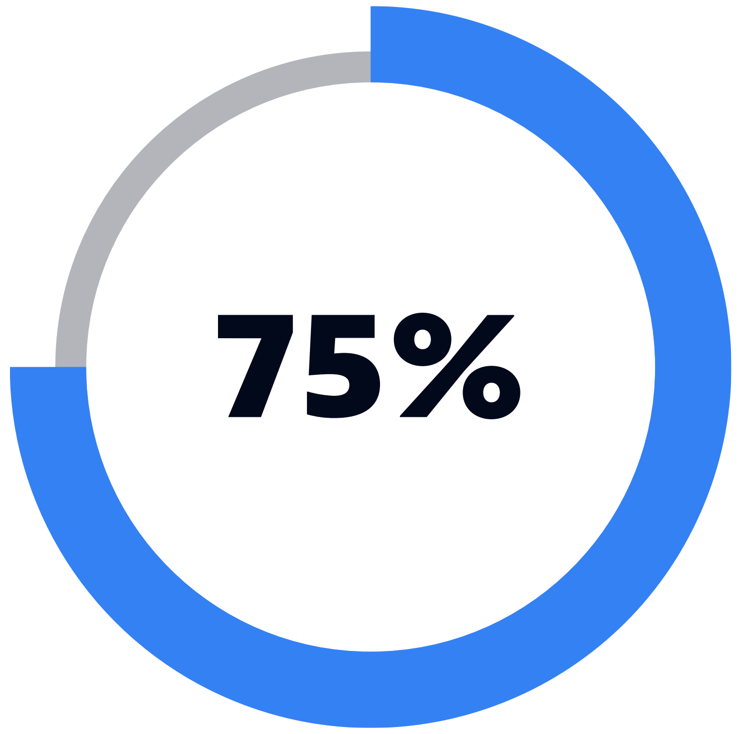
Increased speed brings greater risk for financial services

The drive for faster transformation across the financial services industry is also prompting organizations to adopt Agile practices such as DevSecOps, to remove traditional bottlenecks that can tax understaffed security teams. DevSecOps empowers developers within financial services organizations to secure their own code, so businesses can release new digital banking, investment, and insurance services faster. However, this practice is still maturing, and many developers lack the resources to take greater accountability for security. It's also not enough to just shift security visibility "left" to development; there's also a need to shift "right" to ensure that applications run securely in production. Without this, vulnerabilities that have leaked into production could go undetected and remain open to exploitation, putting customers' financial data at unacceptable risk.

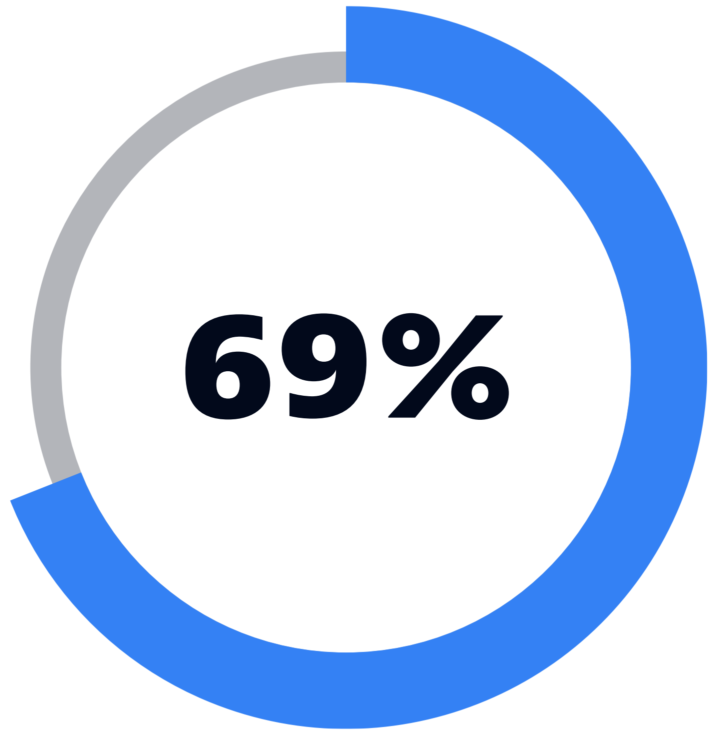


CHAPTER 3

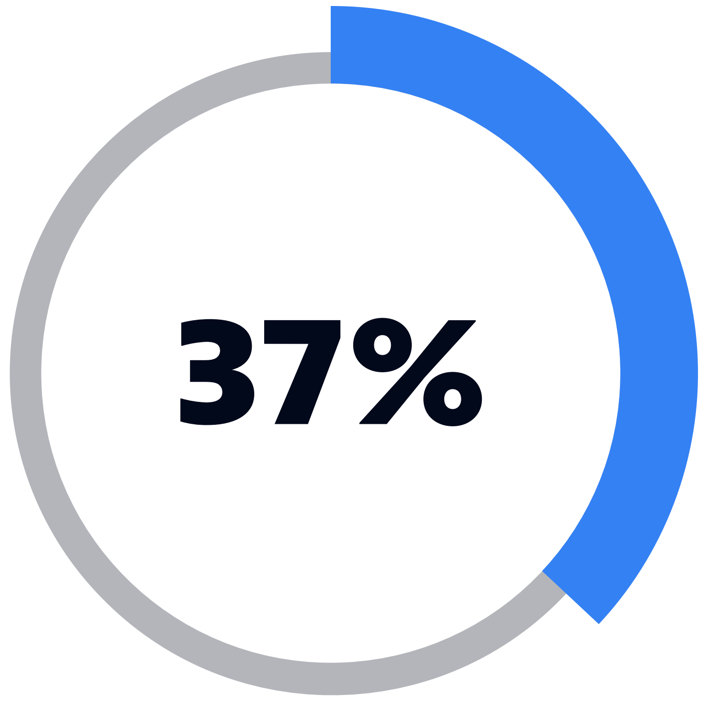
Increased speed brings greater risk for financial services



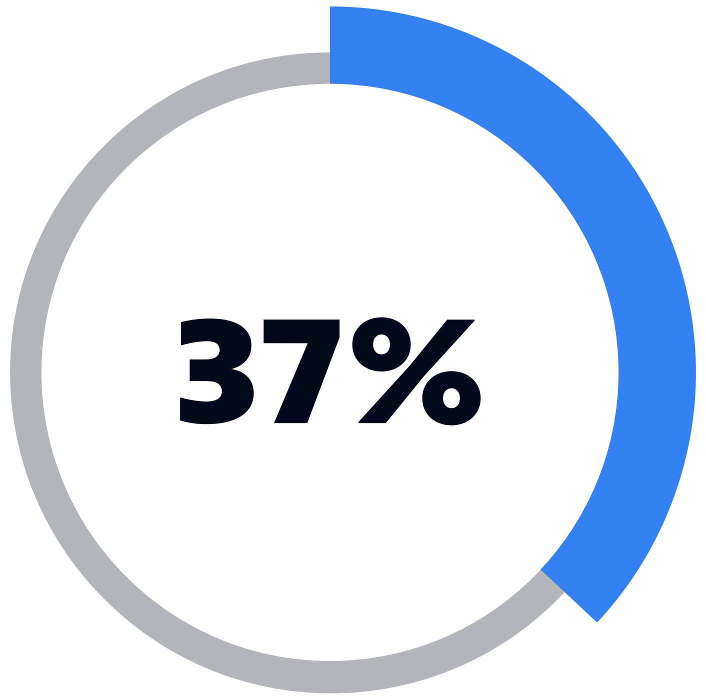
of CISOs say vulnerability management within financial services organizations has become more difficult as the need to accelerate digital transformation has increased.



of CISOs say developers don't always have time to scan for vulnerabilities in their code and apply a fix before it moves into production.



of CISOs are fully confident that applications have been fully tested for vulnerabilities before going live in production.

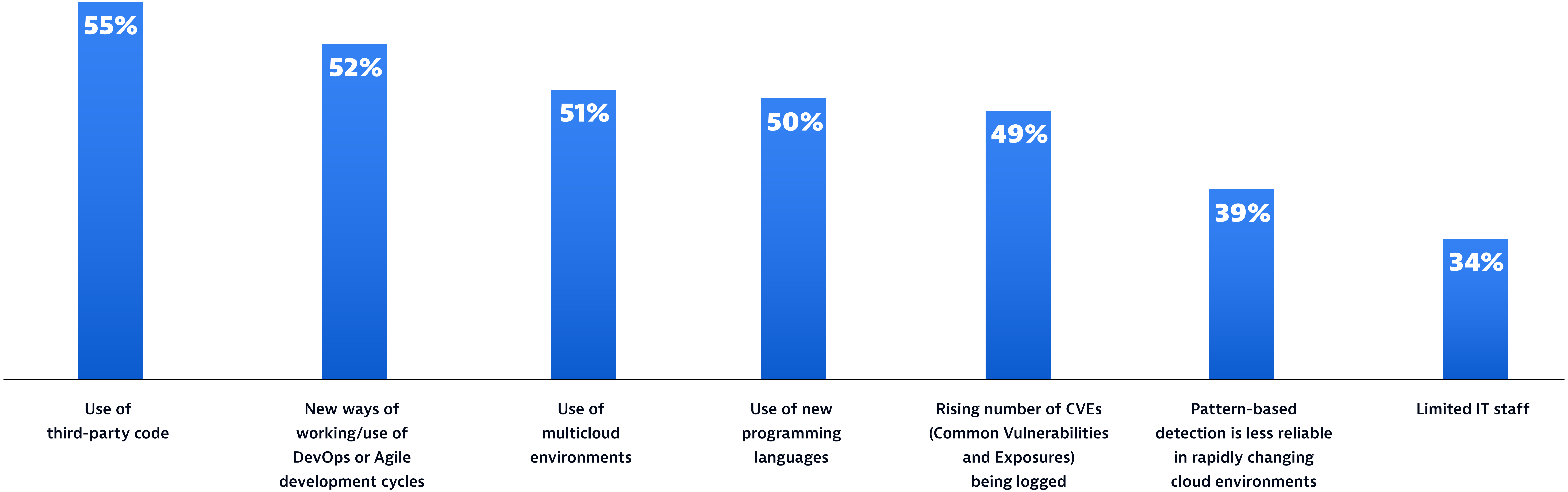


of organizations have a mature DevSecOps culture, where the majority of teams have integrated security practices across the software development lifecycle (SDLC).

CHAPTER 3

Increased speed brings greater risk for financial services

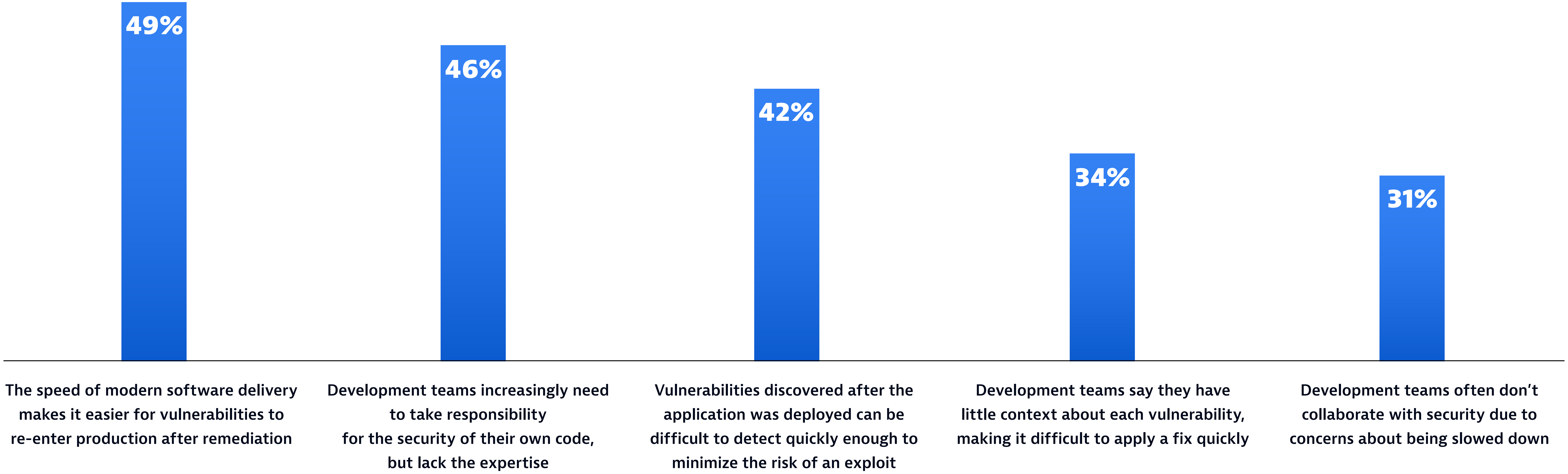
CISOs identify factors that make it more difficult to identify and resolve application vulnerabilities such as the following:



CHAPTER 3

Increased speed brings greater risk for financial services

The most common problems CISOs encounter when addressing application vulnerabilities include the following:



CHAPTER 4

Relentless alerts prevent financial security teams from counting the serious threats

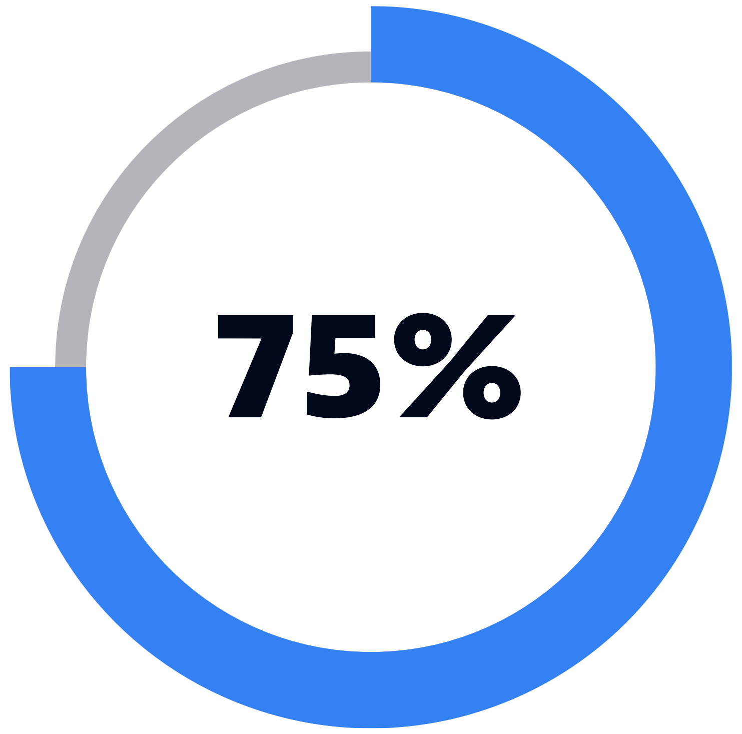
Many security solutions offer only a static view at a single point in time but lack the runtime context needed to understand the difference between a minor risk and a potentially catastrophic exposure. As a result, security teams within banks, payment providers, and other financial services providers are bombarded with thousands of alerts, many of which are false positives, duplicates, or low priority. This makes it difficult for teams to see through the noise and focus on what matters, and efforts to respond manually become impossible.

2,200-plus

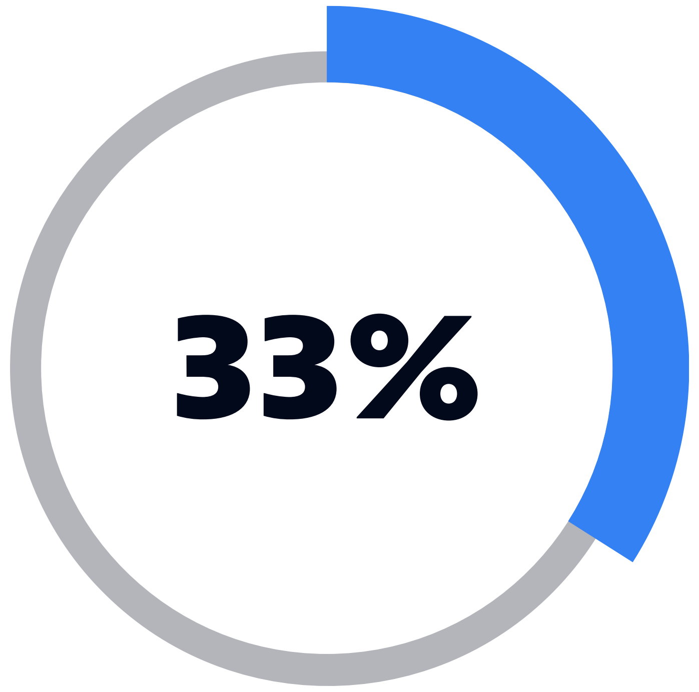
On average, financial services organizations receive more than 2,200 alerts to potential application security vulnerabilities each month.

CHAPTER 4

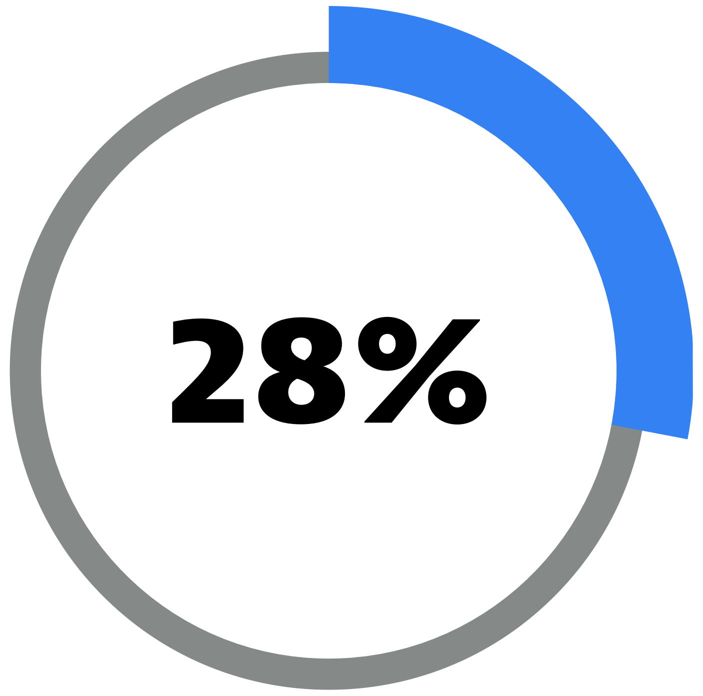
Relentless alerts prevent financial security teams from counting the serious threats



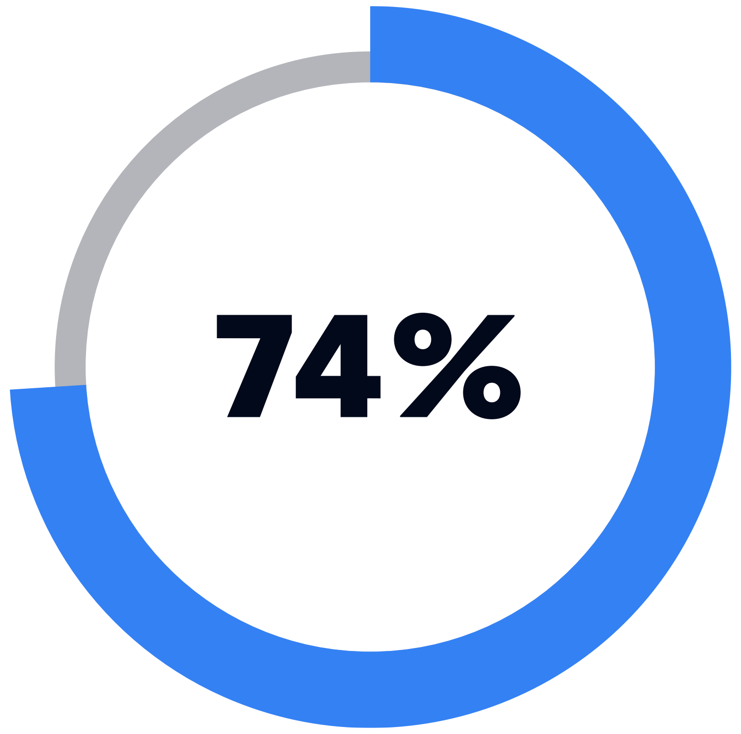
of CISOs say that most security alerts and vulnerabilities are false positives that don’t require action because they are not true exposures.



of application security vulnerability alerts organizations receive each day require actioning, compared with 42% last year.



is the average percentage of time application security teams waste on vulnerability management tasks that could be automated.



of CISOs say the volume of alerts makes it difficult to prioritize vulnerabilities based on risk and impact.

CHAPTER 5

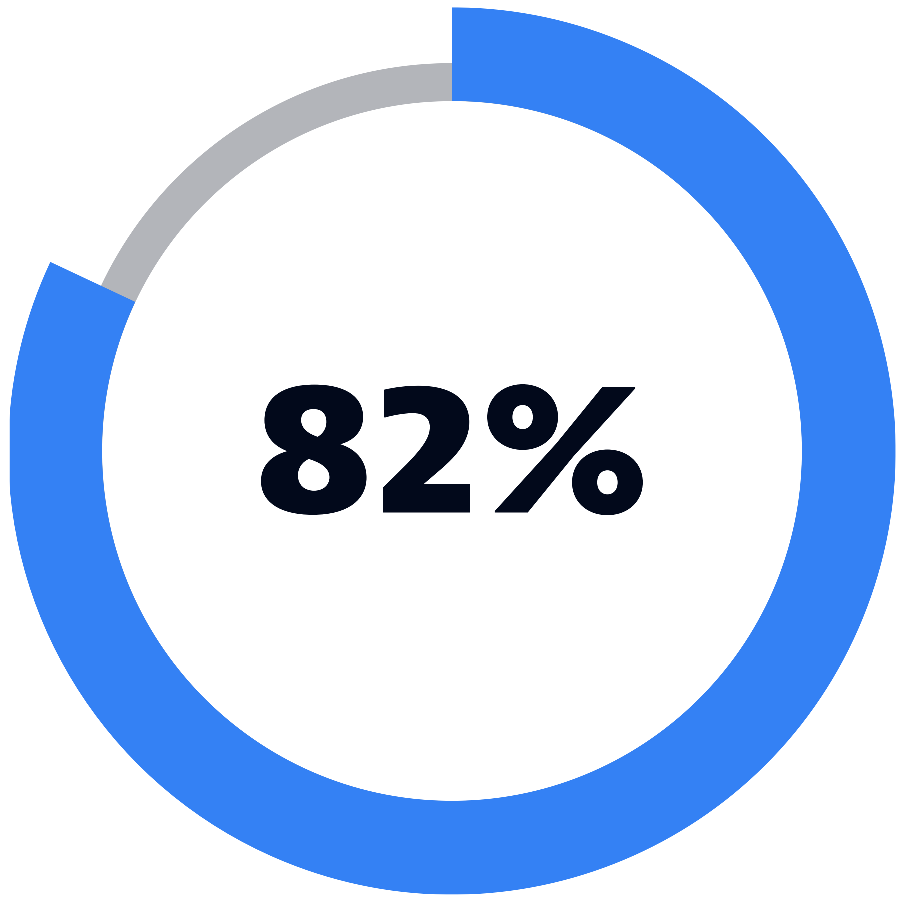
Balance automation, observability, and security for true success

To drive effective vulnerability management in the age of cloud-native delivery, financial services providers must treat security as a shared responsibility across the business. This is best enabled by converging observability and security solutions, so development, operations, and security teams have the context needed to understand how their applications are connected and where the vulnerabilities lie.

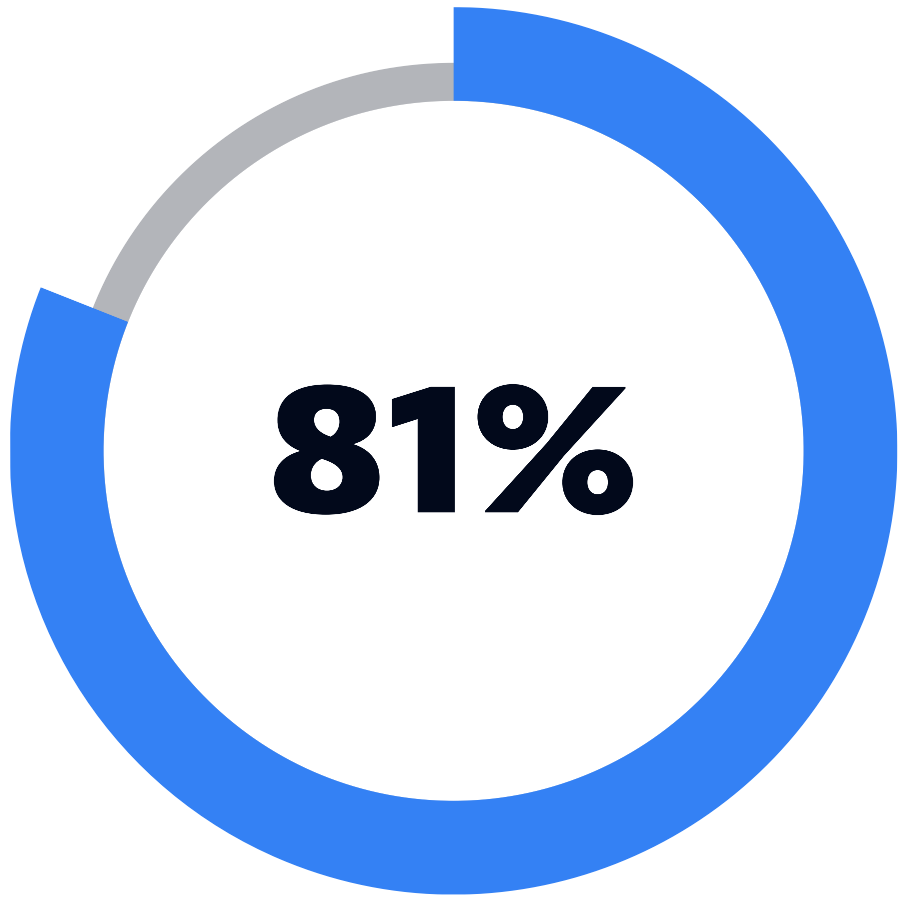
This equips security teams within financial services organizations with runtime vulnerability management capabilities, so they can continuously look at what's running in production and identify vulnerabilities that could be exploited to get at customers' cash, or compromise data that could put them at risk of being defrauded. With automation and AI embedded in these solutions, organizations can access precise, real-time answers that help teams prioritize which vulnerabilities need to be resolved first, based on the potential impact to the organization and its customers.

CHAPTER 5

Balance automation, observability, and security for true success



of CISOs agree that security must be a shared responsibility across the software delivery lifecycle, from development to production.

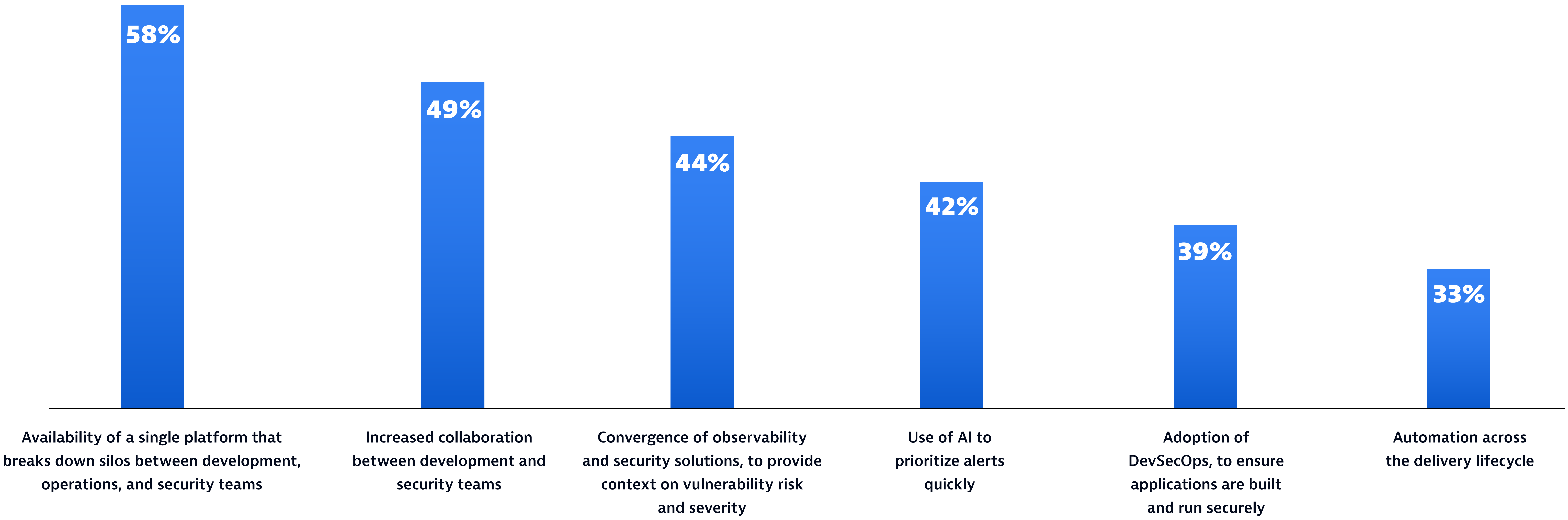


of CISOs say that automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions.

CHAPTER 5

Balance automation, observability, and security for true success

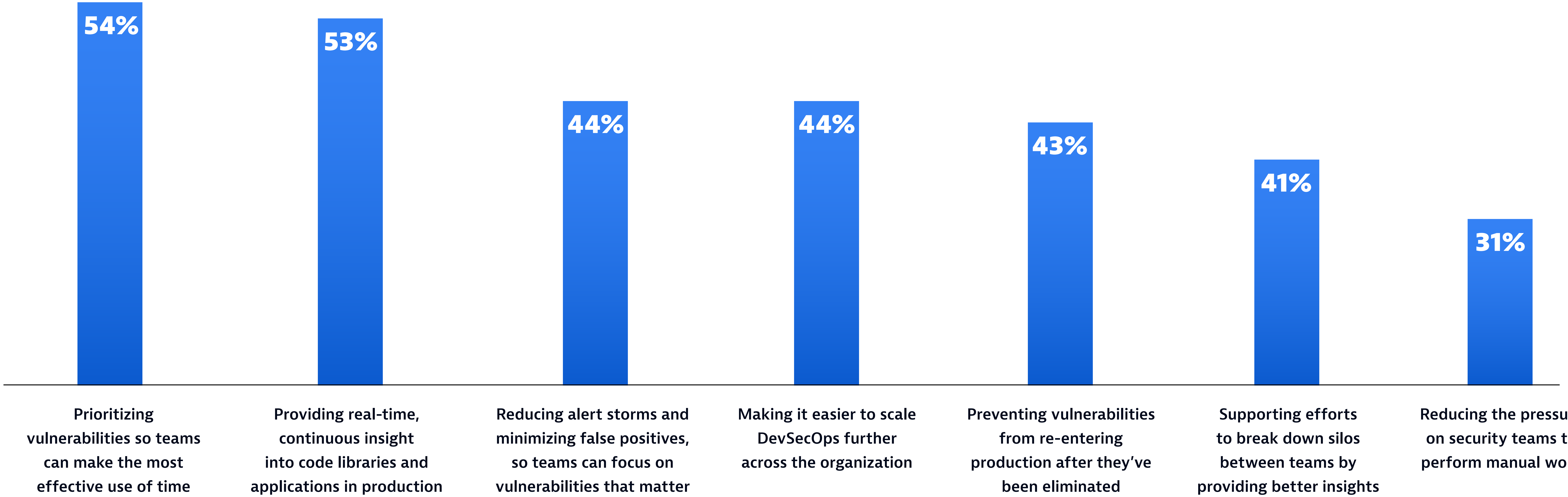
Financial services CISOs say the following factors will be most critical to ensuring application security vulnerabilities can be identified, prioritized, and resolved quickly and effectively in the future:



CHAPTER 5

Balance automation, observability, and security for true success

CISOs say the biggest benefits of increasing the use of AI and automation in security practices include the following:



The Dynatrace difference

Optimized for cloud-native applications, containers, and Kubernetes, Dynatrace® Application Security automatically and continuously detects vulnerabilities in applications, libraries, and code at runtime. It also provides real-time detection and blocking to protect against injection attacks that exploit critical vulnerabilities, such as Log4Shell. It removes blind spots and helps ensure development teams aren't wasting time chasing false positives, and it provides the C suite with confidence in the security of their organizations' applications.

Dynatrace Application Security delivers:

Precise identification and prioritization of vulnerabilities

Providing teams with a clear understanding of the most important vulnerabilities to address and eliminating the time they spend chasing false positives.

Proactive remediation of vulnerabilities

Achieved through integration into DevOps toolchains, including collaboration and issue tracking offerings such as Atlassian Jira, Slack, and ServiceNow.

Automatic attack detection and blocking

Delivering runtime application self-protection for key Open Web Application Security Project (OWASP) threats, including SQL injections and command injections.

Report methodology

This report is based on a global survey of 325 chief information security officers from the financial services sector, representing large enterprises with more than 1,000 employees, conducted by Coleman Parkes and commissioned by Dynatrace in April 2022. The sample included respondents in the U.S., U.K., France, Germany, Spain, Italy, the Nordics, the Middle East, Australia, India, Singapore, Malaysia, Brazil, and Mexico.

Automatic and intelligent observability for hybrid multiclouds

We hope this eBook has inspired you to take the next step in your digital journey.

Dynatrace is committed to providing enterprises with the data and intelligence they need to be successful with their enterprise cloud and digital transformation initiatives, no matter how complex.

Learn more

For more information, please visit www.dynatrace.com/platform for assets, resources, and a **free 15-day trial.**

dynatrace

About Dynatrace

Dynatrace (NYSE: DT) exists to make the world's software work perfectly. Our unified software intelligence platform combines broad and deep observability and continuous runtime application security with the most advanced AIOps to provide answers and intelligent automation from data at enormous scale. This enables innovators to modernize and automate cloud operations, deliver software faster and more securely, and ensure flawless digital experiences. That is why the world's largest organizations trust the Dynatrace® platform to accelerate digital transformation.

Curious to see how you can simplify your cloud and maximize the impact of your digital teams? Let us show you. Sign up for a free 15-day Dynatrace trial.

blog **@dynatrace**