2022 CISO Research Report: Retail Sector

Observability and security must converge to close the gap in vulnerability management.

Introduction

The rise of omnichannel customer experiences and the explosive growth in online shopping have transformed the retail industry. These dynamics have required retailers around the world to adopt new technologies and software development processes to deliver the modern shopping experiences that customers expect and that are required to maintain a competitive edge.

To improve their digital agility, retailers are now adopting dynamic hybrid and multicloud environments, cloud-native architectures, and open source code libraries. Despite delivering key business benefits, these technologies have introduced new challenges.

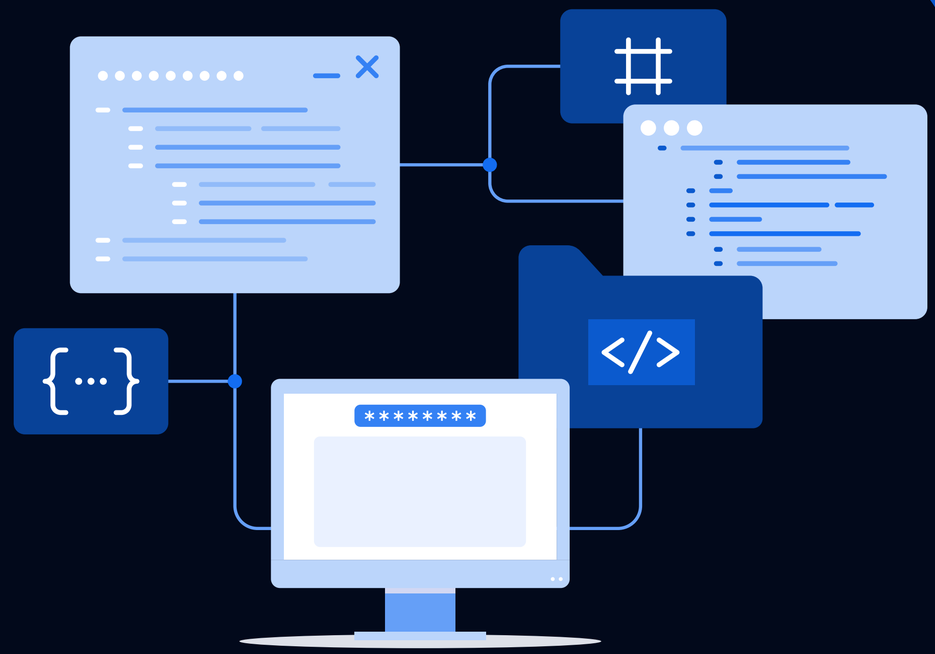
Across the retail sector, the process of developing, testing, securing, and releasing applications and digital services has become more complicated, increasing the opportunities for vulnerabilities to enter the development lifecycle. The Log4j vulnerability that emerged in 2021 demonstrated the severity of this problem, as it highlighted a serious gap in the security posture of countless retail organizations.

Despite most businesses in the sector boasting a robust cybersecurity strategy, there are still gaps around vulnerability management that retailers must urgently address. This report explores these challenges and highlights how the convergence of observability and security can enable more effective vulnerability management as well as attack detection and blocking across the retail sector.

What's inside

CHAPTER 1

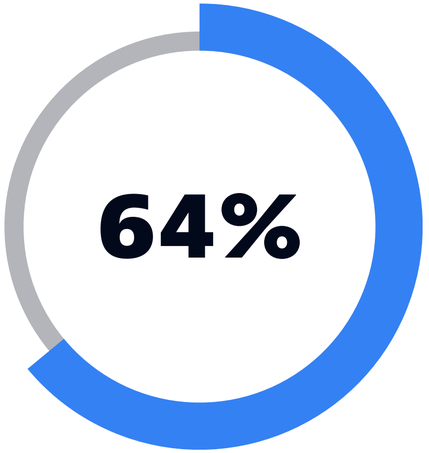
Layered security is not a one-stop shop



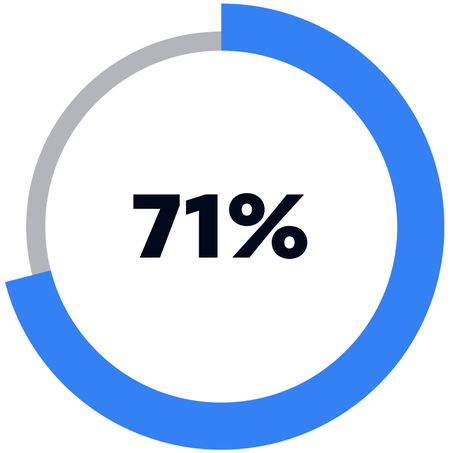
Modern cloud environments deliver numerous business benefits for teams working across IT, development, and security within the retail sector, but they also bring challenges. The growing use of microservices, Kubernetes, and serverless computing improves scalability and reliability, but it also creates complexity for which many solutions weren't designed. Even with the most robust and layered cybersecurity posture, many retail businesses have no visibility into their dynamic, containerized applications. Additionally, they often struggle to access the necessary context to distinguish a potential vulnerability from a critical exposure in their code base. As a result, managing the security of their applications at runtime is increasingly difficult, allowing more vulnerabilities to escape into production and put customer transaction data at risk.

CHAPTER 1

Layered security is not a one-stop shop



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

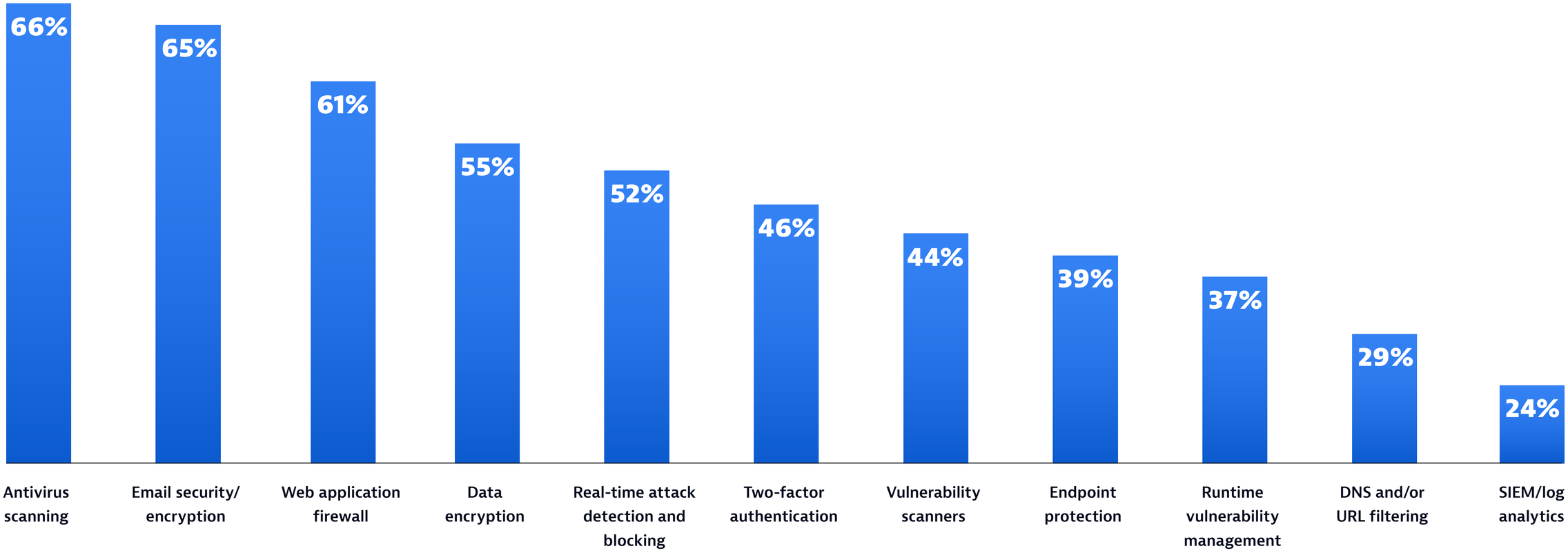


of retail chief information security officers (CISOs) say that despite having a robust, multilayered security posture, gaps still allow vulnerabilities into production.

CHAPTER 1

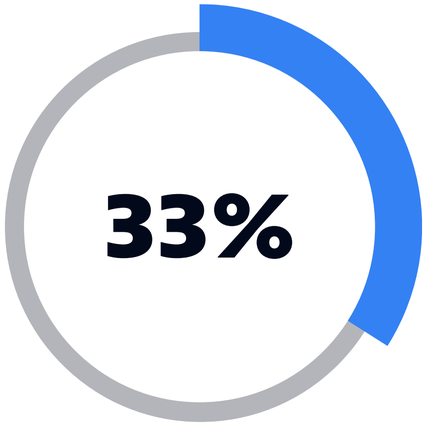
Layered security is not a one-stop shop

The most common security solutions organizations use include the following:

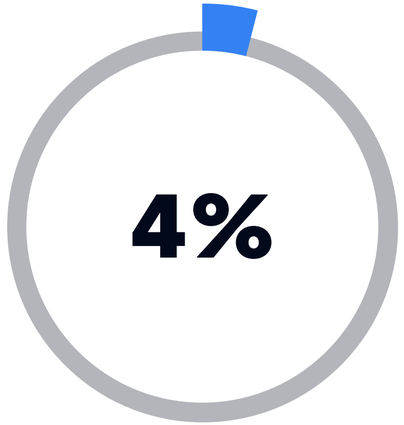


CHAPTER 1

Layered security is not a one-stop shop



of retailers have runtime vulnerability management capabilities.



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

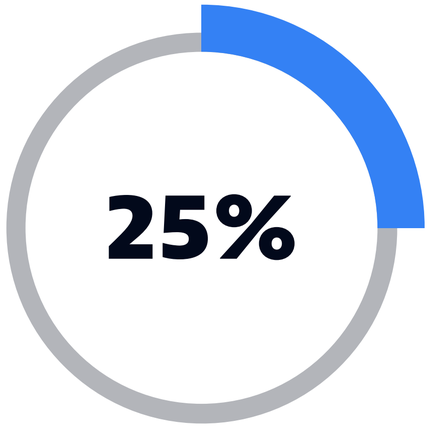
CHAPTER 2

Open source code can leave the front door unlocked

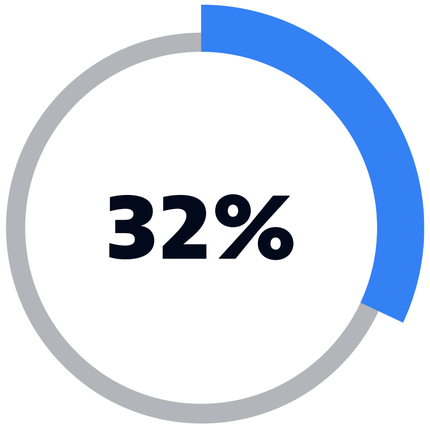
Retail businesses are increasingly turning to open source code to accelerate innovation. These third-party libraries eliminate the need for developers to start every digital transformation from scratch. However, they also introduce significant security risks, as they regularly contain vulnerabilities. As we saw with the discovery of Log4Shell in December 2021, identifying and remediating these vulnerabilities is becoming more challenging as the number of dependencies within applications grows. Even if organizations could access a complete list of all code libraries running in production, determining the impact of any vulnerabilities and prioritizing which to resolve first have gone beyond human capability.

CHAPTER 2

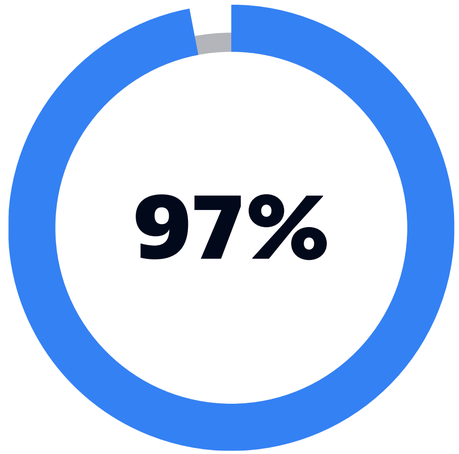
Open source code can leave the front door unlocked



of retail 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 retail organizations say they faced risk exposure from Log4Shell, and 35% cited their risk as “high” or “severe.”

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

64% Speed of development makes it difficult to prevent vulnerabilities from returning

58% Volume of false positives or low-impact alerts make it difficult to prioritize which exposures to resolve first

44% Significant manual effort to evaluate our risk exposure

36% Limited collaboration between security and development teams delayed our response

30% Limited or delayed insight into what is running in production

25% Limited context within alerts to identify the risk impact

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

68% Huge increase in remediation tickets for development teams

53% Significant increase in manual war rooms

37% Teams that have to work around the clock

38% Tier-2 or -3 vulnerabilities are ignored during a crisis

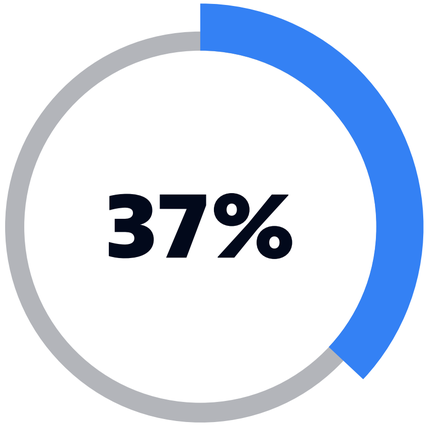
34% Teams that feel overwhelmed

22% Sense of panic

CHAPTER 2

Open source code can leave the front door unlocked

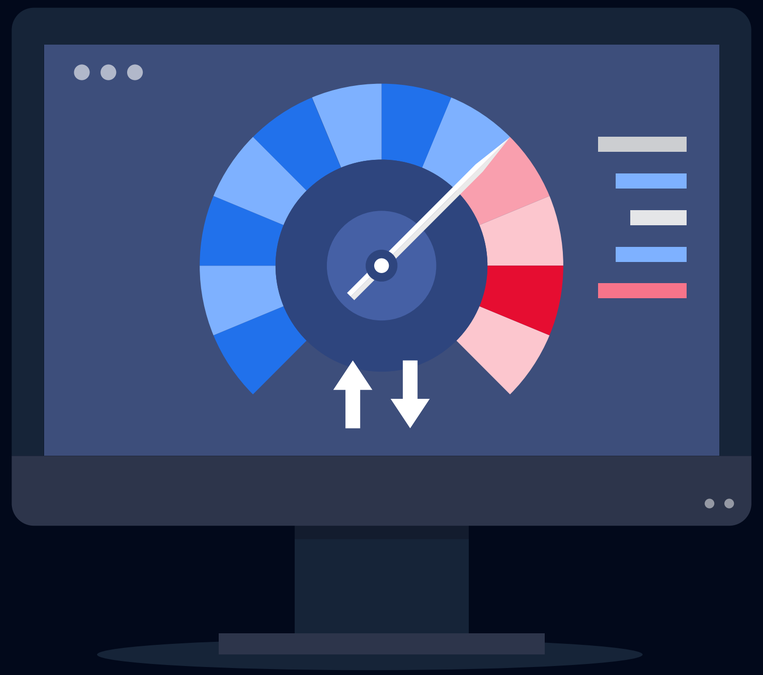
On average, security teams within the retail sector spent 48 hours responding to the Log4j vulnerability.



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

CHAPTER 3

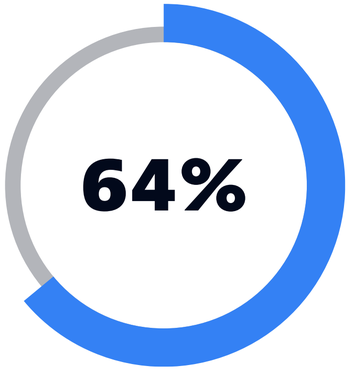
Speed is not always key for the retail sector



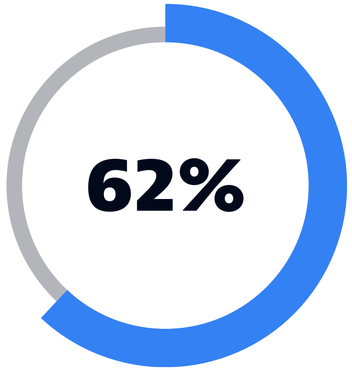
The drive for faster transformation across all areas of retail and ecommerce is also leading more organizations to adopt Agile practices, such as DevSecOps. This framework enables organizations to release new services faster by having developers test their own code for vulnerabilities. However, this practice is still maturing. Many developers within retail organizations lack the resources to take greater accountability for security. It's also not enough to shift security visibility "left" to development, as there's also a need to shift "right" to ensure that applications run securely in production. Without shifting right, vulnerabilities that have leaked into production will go undetected and remain open to exploitation.

CHAPTER 3

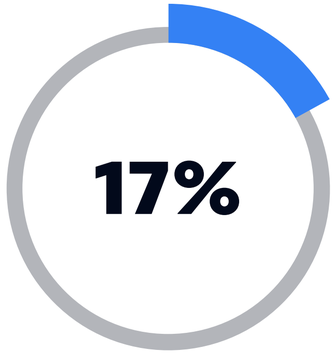
Speed is not always key for the retail sector



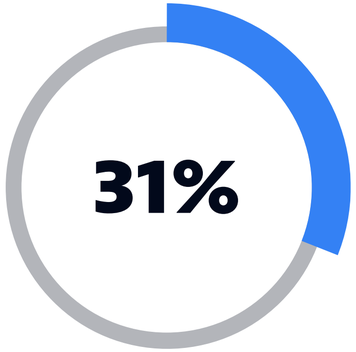
of CISOs within the retail sector say vulnerability management has become more difficult as the need to accelerate digital transformation has increased.



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

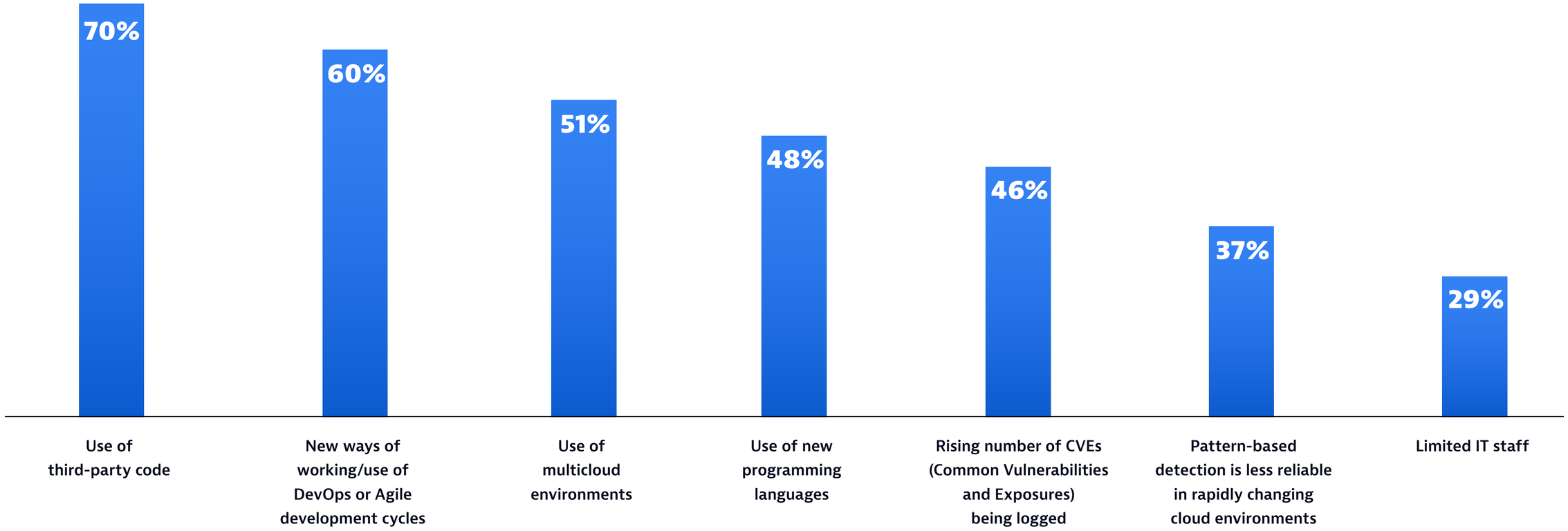


of organizations have a mature DevSecOps culture, where the majority of teams have integrated security practices across the SDLC.

CHAPTER 3

Speed is not always key for the retail sector

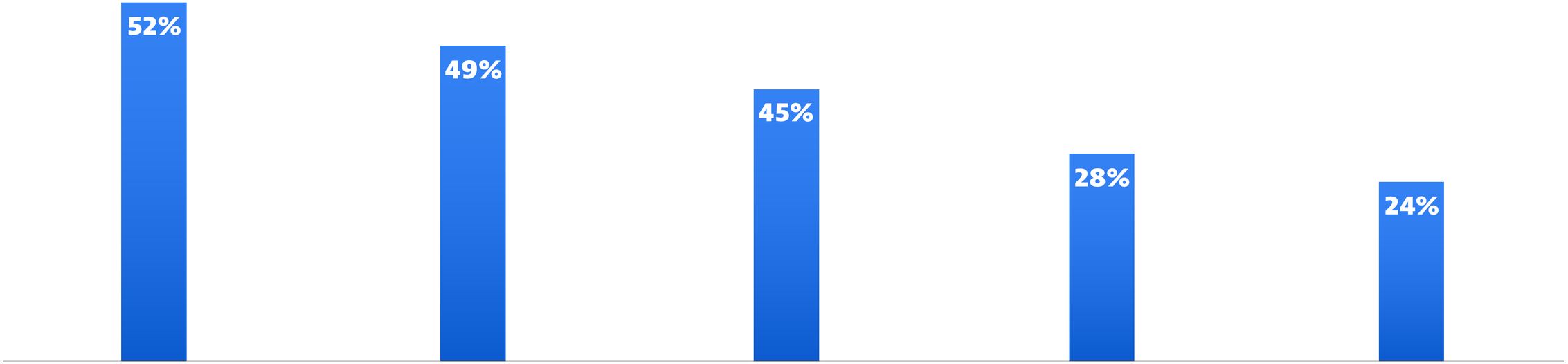
CISOs identify factors that make it more difficult to identify and resolve application vulnerabilities as the following:



CHAPTER 3

Speed is not always key for the retail sector

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



The speed of modern software delivery makes it easier for vulnerabilities to re-enter production after remediation

Development teams increasingly need to take responsibility for the security of their own code, but lack the expertise

Vulnerabilities discovered after the application was deployed can be difficult to detect quickly enough to minimize the risk of an exploit

Development teams say they have little context about each vulnerability, making it difficult to apply a fix quickly

Development teams often don't collaborate with security due to concerns about being slowed down

CHAPTER 4

Relentless alerts prevent security teams from locating real threats

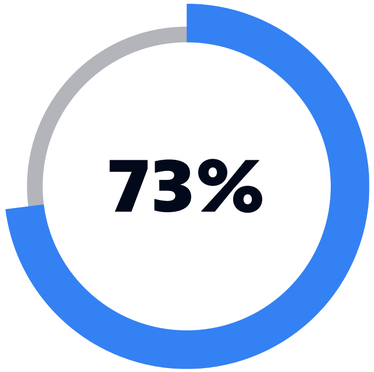
Many security solutions offer only a static view at a single point in time, or they lack the context to understand the difference between a minor risk and a potentially catastrophic exposure. As a result, retail security teams are bombarded with thousands of alerts, many of which are false positives, duplicates, or low priority. Seeing through the noise and focusing on what matters becomes difficult, and efforts to respond manually become impossible.

1,700-plus

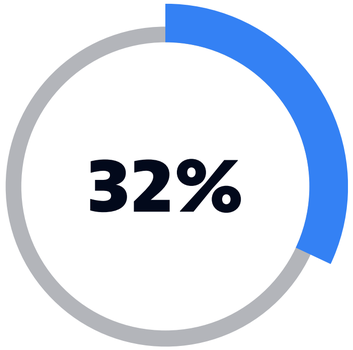
Retail organizations receive more than 1,700 alerts to potential application security vulnerabilities each month.

CHAPTER 4

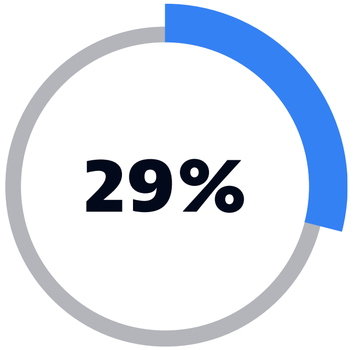
Relentless alerts prevent security teams from locating real threats



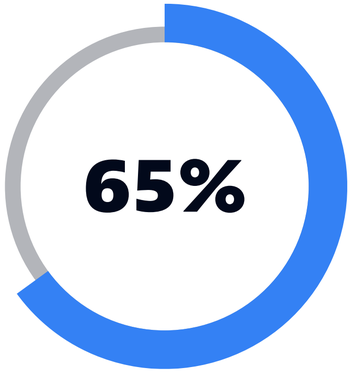
of CISOs say most security alerts and vulnerabilities are false positives that don't require action because they are not true exposures.



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.

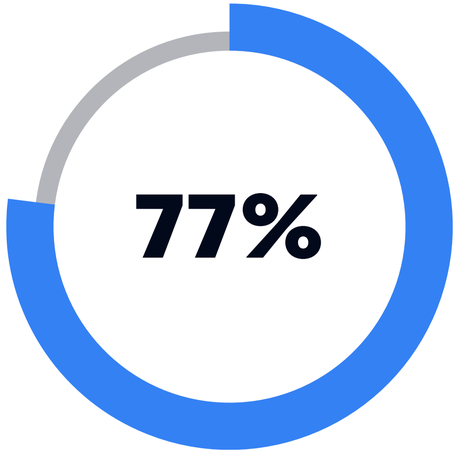
CHAPTER 5

To succeed, retailers must combine automation, observability, and security

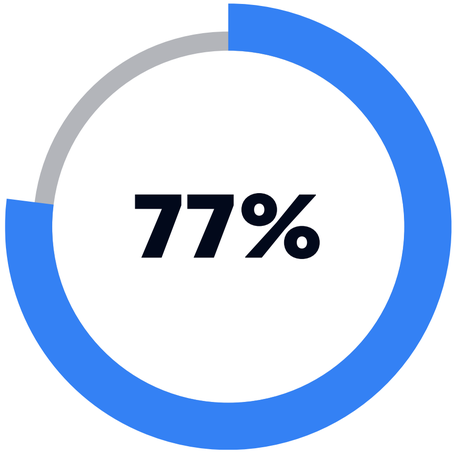
Regardless of whether the retailers specialize in affordable groceries or luxury fashion, the best practice for effective vulnerability management in the age of cloud-native delivery is to treat it as a shared responsibility. By converging observability and security solutions, teams across development, operations, and security gain the necessary context to understand how their applications are connected and where vulnerabilities lie. Equipping security teams with runtime vulnerability management capabilities enables them to continuously look at what is running in production and identify any vulnerabilities that could affect customers or internal users. 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 potential impact.

CHAPTER 5

To succeed, retailers must combine automation, observability, and security



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

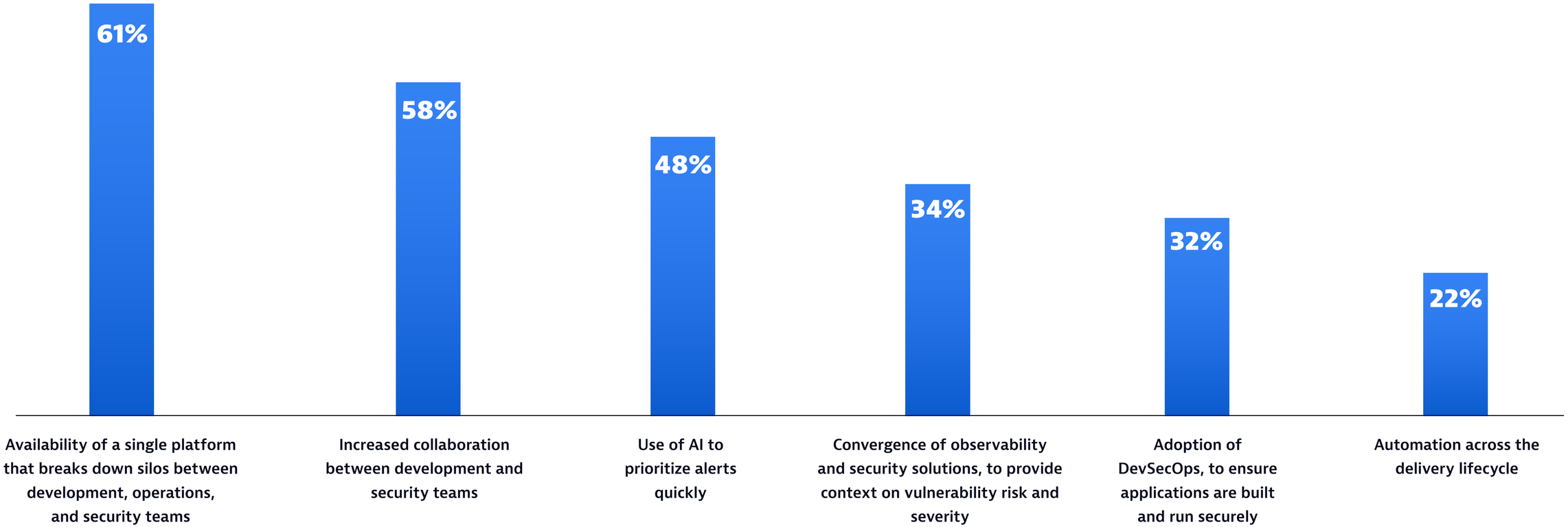


of CISOs say that automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions.

CHAPTER 5

To succeed, retailers must combine automation, observability, and security

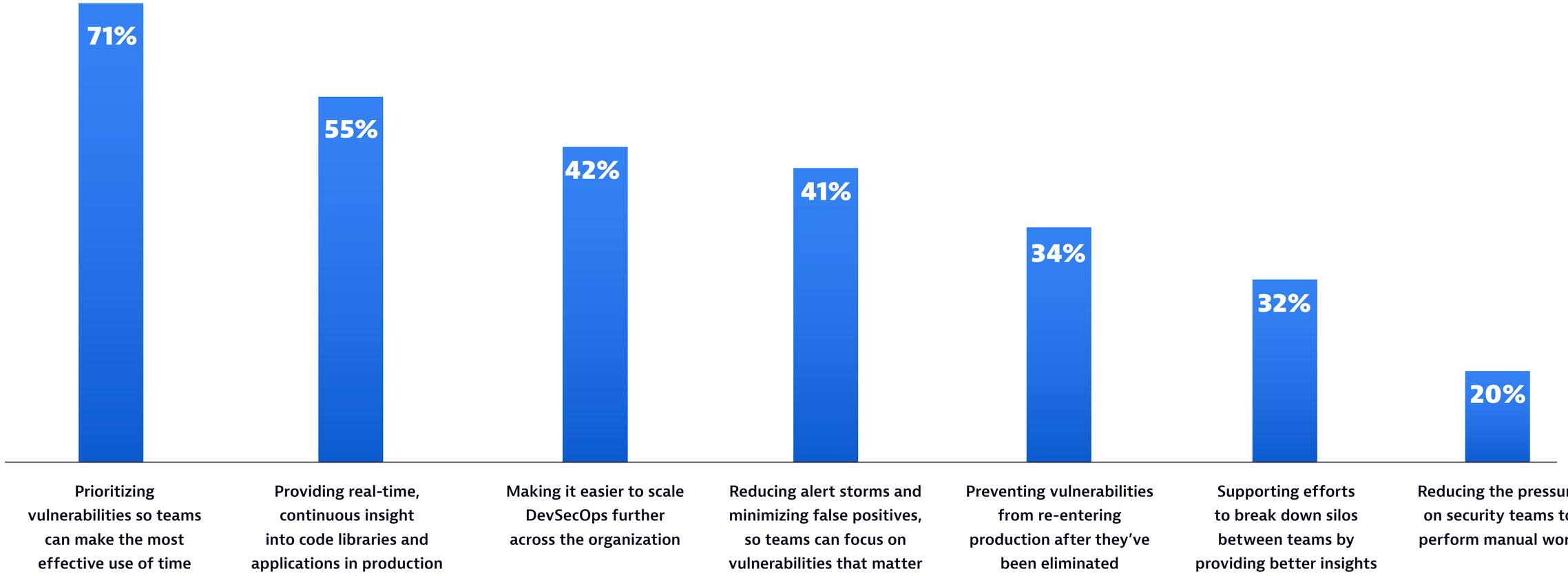
Retail CISOs say the following factors will be most critical to ensuring application security vulnerabilities can be identified, prioritized, and resolved quickly and effectively in the future:



CHAPTER 5

To succeed, retailers must combine automation, observability, and security

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. Dynatrace Application Security removes blind spots and helps ensure development teams aren't wasting time chasing false positives. Finally, it provides the C suite with confidence in the security of their organizations' applications.

Dynatrace Application Security delivers:

Precise identification and prioritization of vulnerabilities

Dynatrace provides teams with a clear understanding of the most important vulnerabilities to address and eliminates the time spent chasing false positives.

Proactive remediation of vulnerabilities

Integration into DevOps toolchains, including Atlassian Jira, Slack, and ServiceNow, ensures swift resolution.

Automatic attack detection and blocking

Dynatrace delivers 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 retail chief information security officers, 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**

08.03.22 18143_EBK_cs