dynatrace

2022 CISO Research Report

Observability and security must converge
to enable effective vulnerability management.

Introduction

Modern cloud-native delivery has made it increasingly difficult for organizations to reduce and manage enterprise risk throughout the software development lifecycle. The process of developing, testing, securing, and releasing applications and software updates has been complicated by use of multicloud environments, multiple coding languages, and open source libraries. While these factors enable organizations to innovate faster, they also compound opportunities for vulnerabilities to enter the development lifecycle.

Log4Shell, a vulnerability that emerged in live applications in December 2021, was the poster child for this problem, and highlighted a major gap in many organizations' current security postures. This vulnerability affected most organizations, including those with a robust, layered cybersecurity strategy.

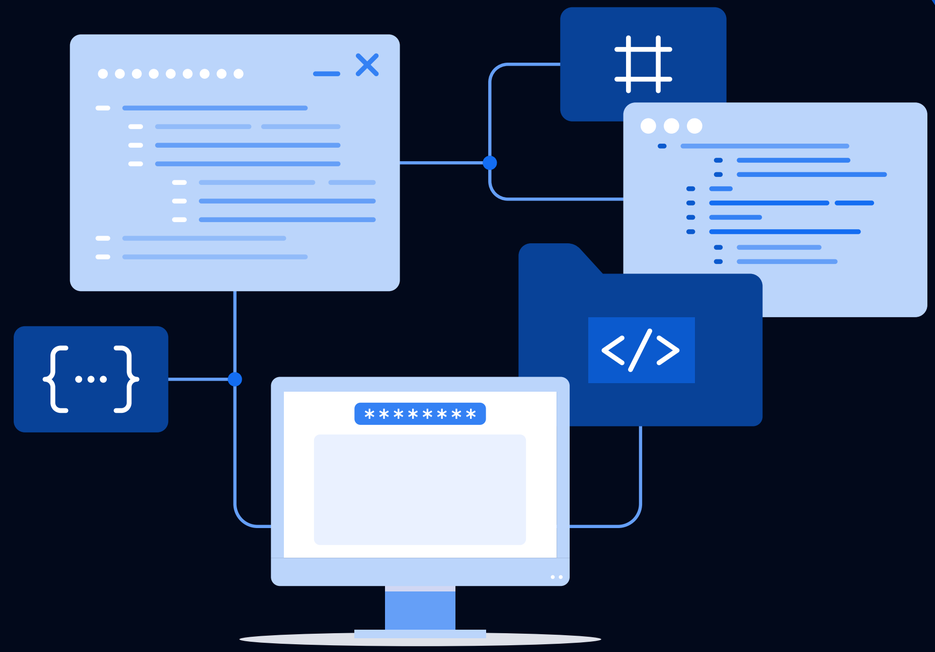
Security teams are also increasingly stretched thin, and it's more difficult for them to prioritize efforts effectively. With so many common vulnerabilities and exposures (CVEs) logged daily, it's impossible to identify and patch all vulnerabilities quickly enough to maintain a secure posture. This report explores these challenges and highlights how IT pros can converge observability and security can close the gap in vulnerability management.

What's inside

CHAPTER 1

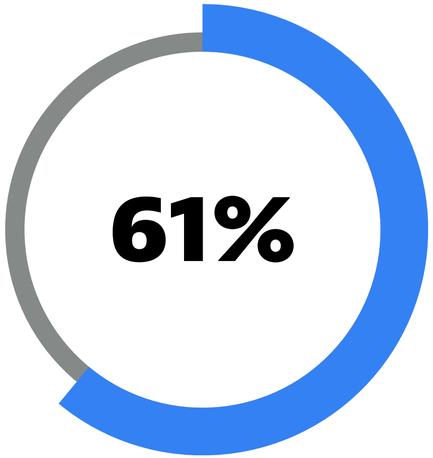
Even layered security strategies contain gaps

The rise of modern cloud environments has created a conundrum for IT pros. 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.

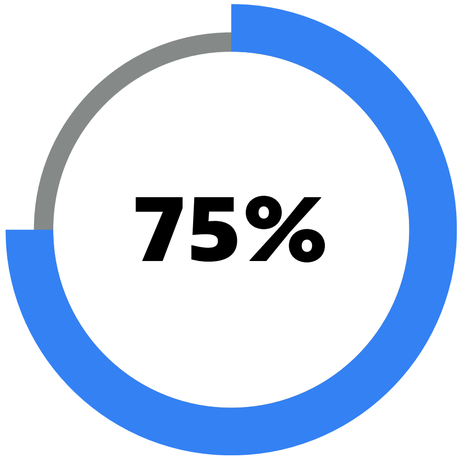


CHAPTER 1

Even layered security strategies contain gaps



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

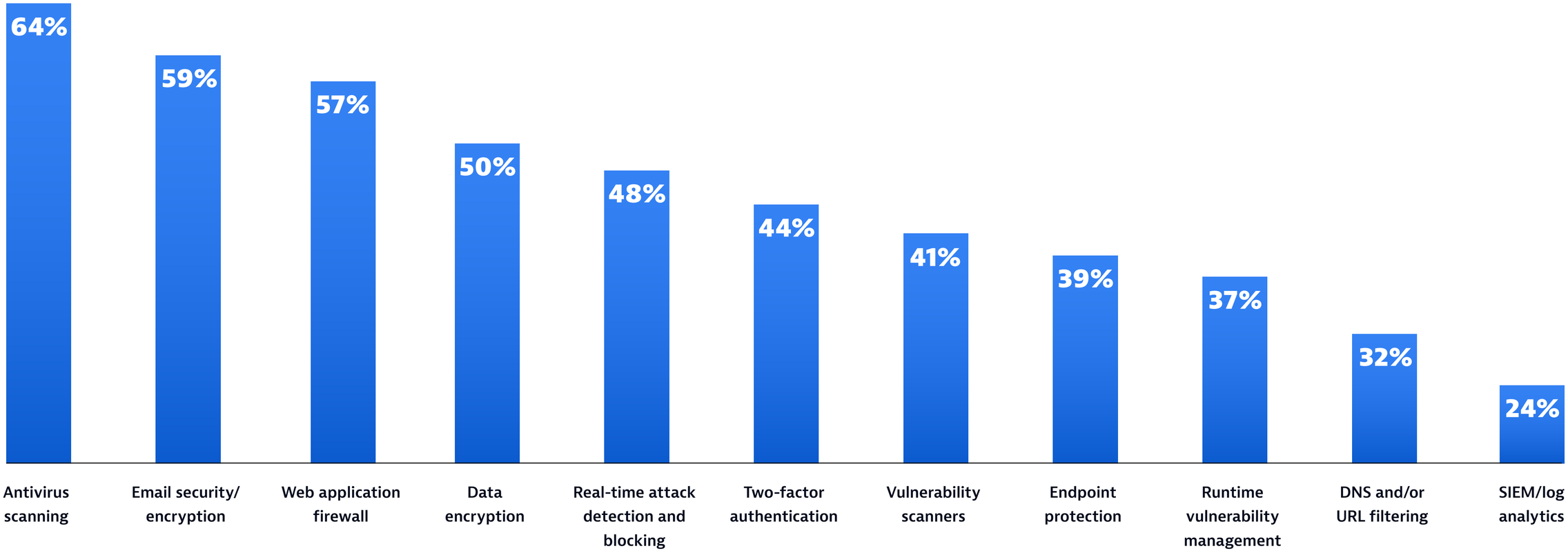


of CISOs say that despite having a robust, multi-layered security posture, there are still gaps that allow vulnerabilities into production.

CHAPTER 1

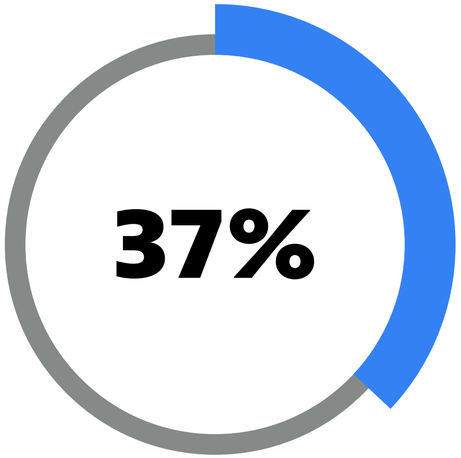
Even layered security strategies contain gaps

The most common security solutions organizations use include the following:

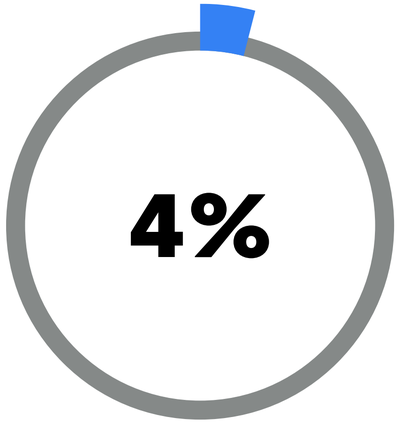


CHAPTER 1

Even layered security strategies contain gaps



of organizations have runtime vulnerability management capabilities.



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

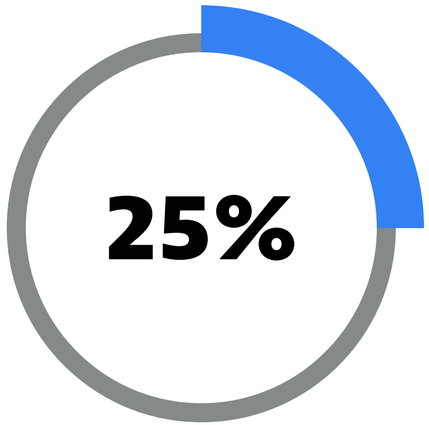
CHAPTER 2

Open source software code can leave the back door unlocked

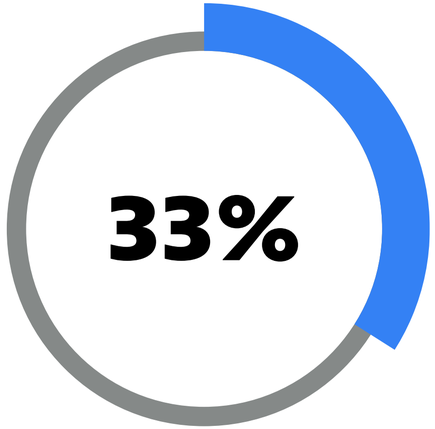
Organizations are increasingly turning to open source code to accelerate innovation. However, these third-party libraries also introduce significant security risks, as they regularly contain vulnerabilities. With the emergence of Log4Shell in December 2021, and Spring4Shell just a few months later, identifying and remediating these vulnerabilities weredifficult. Even if they 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 gone beyond human capability.

CHAPTER 2

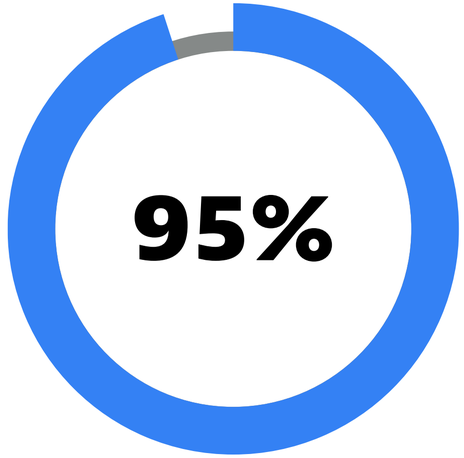
Open source software code can leave the back door unlocked



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 35% cited their risk as ‘high’ or ‘severe’.

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

59% Speed of development makes it difficult to prevent vulnerabilities from returning

53% Volume of false positives or low-impact alerts make it difficult to prioritize which exposures to resolve first

43% Significant manual effort to evaluate our risk exposure

41% Limited collaboration between security and development teams delayed our response

34% Limited or delayed insight into what is running in production

30% Limited context within alerts to identify the risk impact

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

59% Major increase in remediation tickets for development teams

53% Significant increase in manual war rooms

43% Teams having to work around the clock

40% Tier-2 or -3 vulnerabilities are ignored while the focus is on the crisis

31% Feeling of being overwhelmed

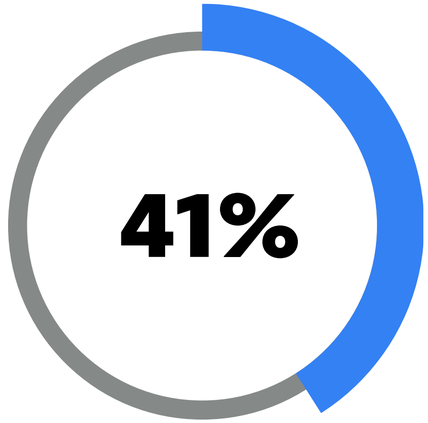
22% Sense of panic

CHAPTER 2

Open source software code can leave the back door unlocked

The most common security solutions organizations use are the following:

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

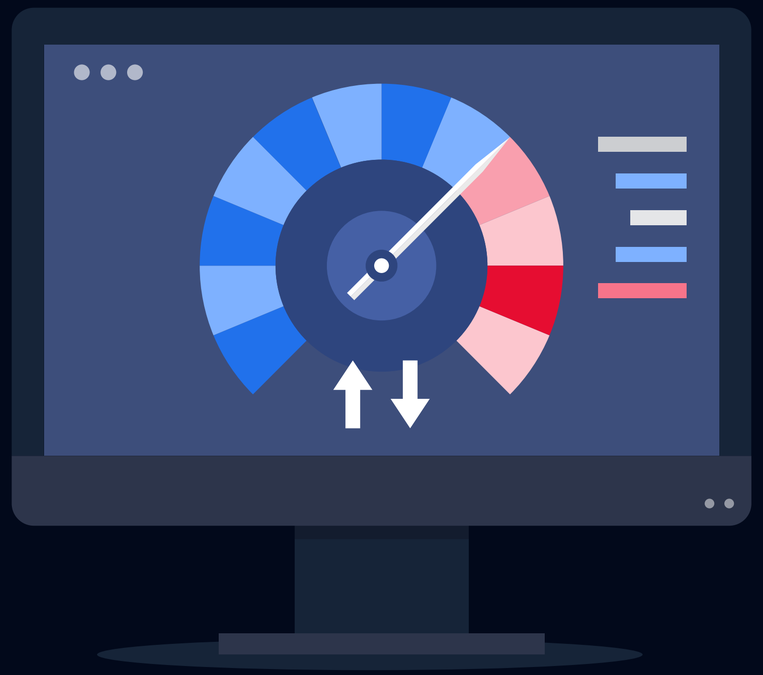


of CISOs are fully confident their teams could identify and resolve all instances of Log4Shell in their environment.

CHAPTER 3

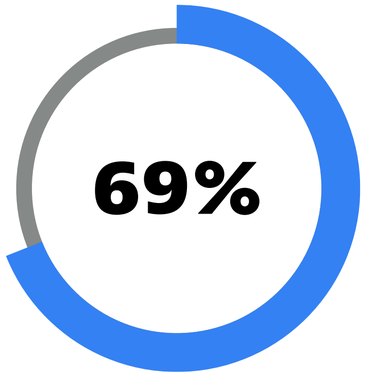
Increased speed brings greater risk

The drive for faster transformation is also prompting organizations to adopt Agile practices such as DevSecOps, to remove traditional bottlenecks that can tax understaffed security teams. DevSecOps empowers developers to secure their own code, so organizations can release new services faster. However, this practice is still maturing, and many developers lack the resources to take more accountability for security. It's also not enough to just shift responsibility '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 run the risk of going undetected and so remain open to exploitation.

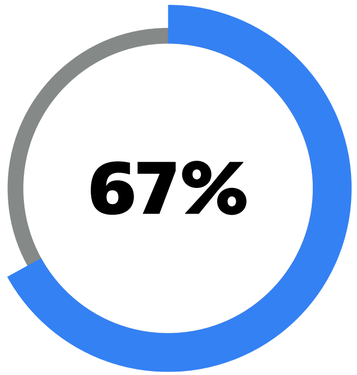


CHAPTER 3

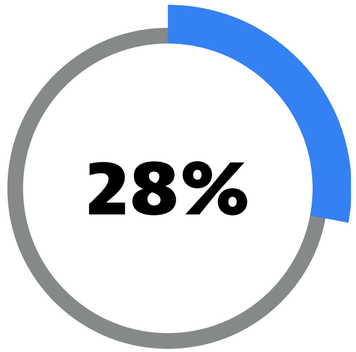
Increased speed brings greater risk



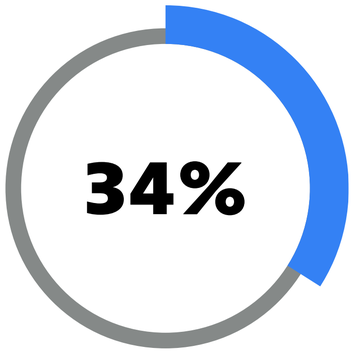
of CISOs say vulnerability management has become more difficult as the need to accelerate digital transformation has increased



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

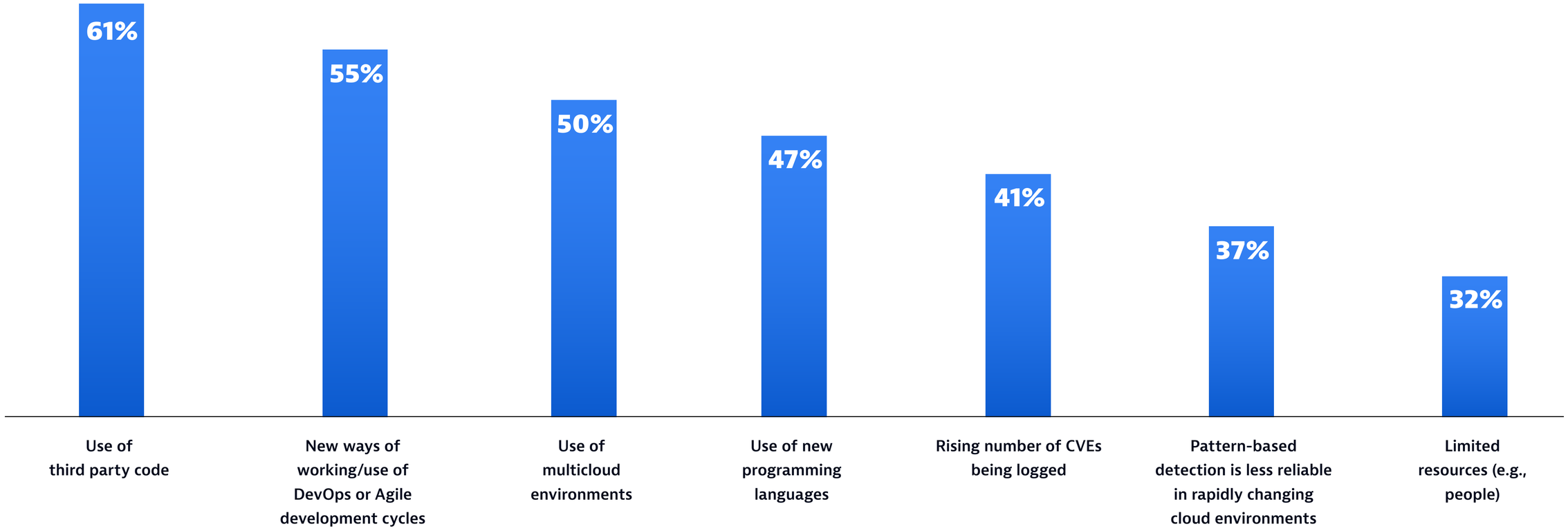


of organizations have a mature DevSecOps culture, where the majority of teams have integrated security practices across the software development lifecycle (SDLC).

CHAPTER 3

Increased speed brings greater risk

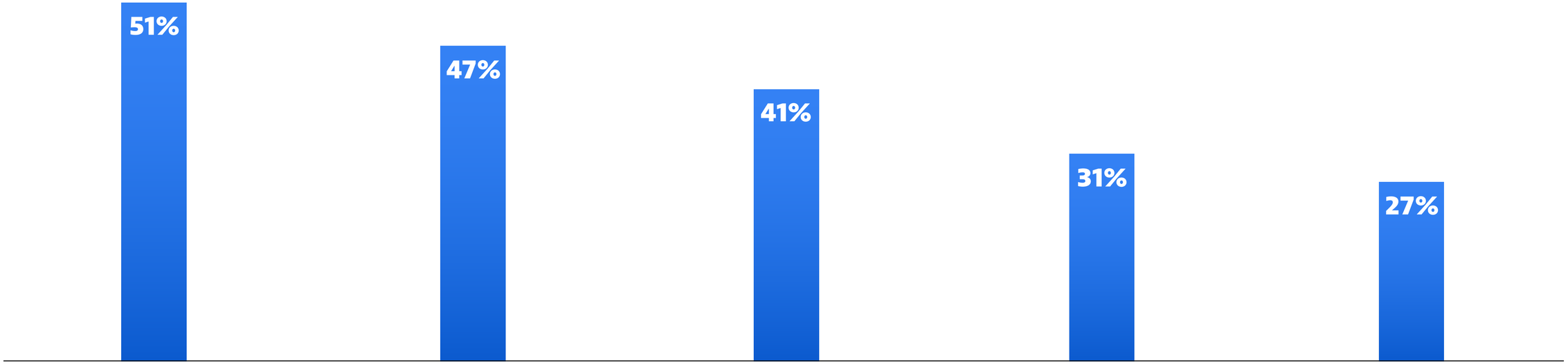
CISOs identify factors that make it more difficult to pinpoint and resolve application vulnerabilities such as the following:



CHAPTER 3

Increased speed brings greater risk

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



CHAPTER 4

Relentless alert storms blind security teams to the real threats

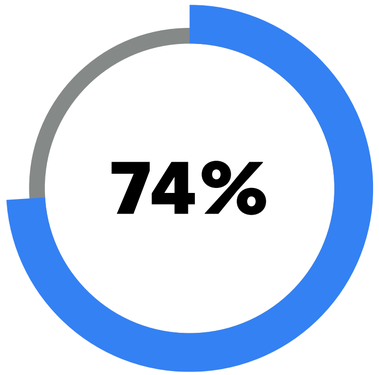
Many security solutions offer only a static view at a single point in time but lack the runtime context needed to understand the difference between a minor risk and a potentially catastrophic exposure. As a result, security teams are bombarded with thousands of alerts, many of which are false positives, 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.

2,027

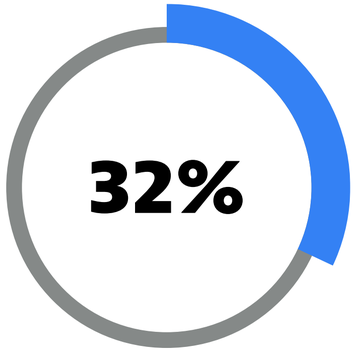
On average, organizations receive more than 2,000 alerts to potential application security vulnerabilities each month.

CHAPTER 4

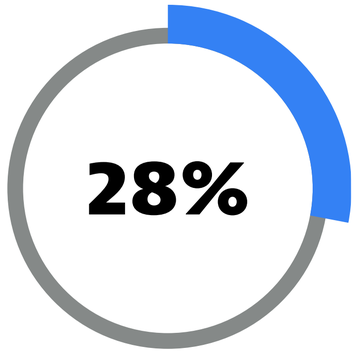
Relentless alert storms blind security teams to the real threats



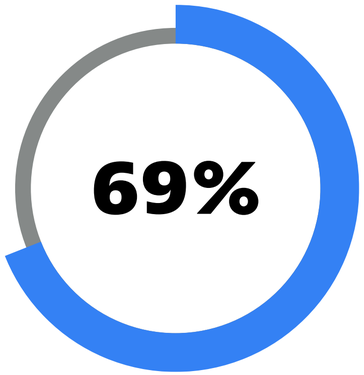
of CISOs say that most security alerts and vulnerabilities are false positives that don't require action because they are not true exposures.



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



is the average proportion of their time that 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.

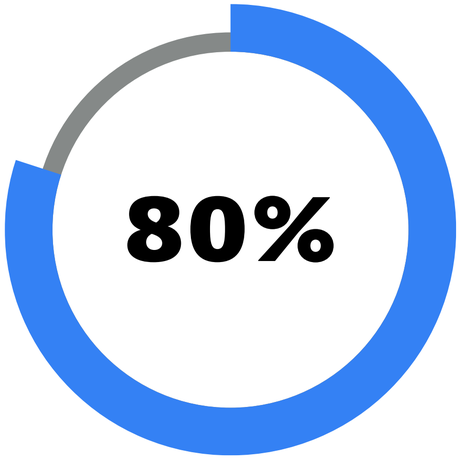
CHAPTER 5

The convergence of automation, observability, and security is key to success

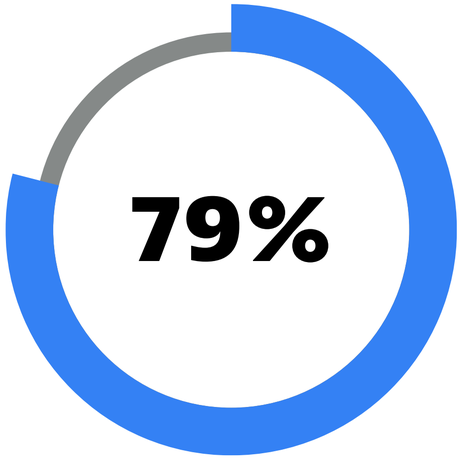
To drive effective vulnerability management in the age of cloud-native delivery, security must be a shared responsibility. This is best enabled by converging observability and security solutions, so development, operations, and security teams have the context needed to understand how their applications are connected and where the vulnerabilities lie. This equips security teams with runtime vulnerability management capabilities, so they can continuously look at what's running in production and identify 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 the potential impact.

CHAPTER 5

The convergence of automation, observability, and security is key to success



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

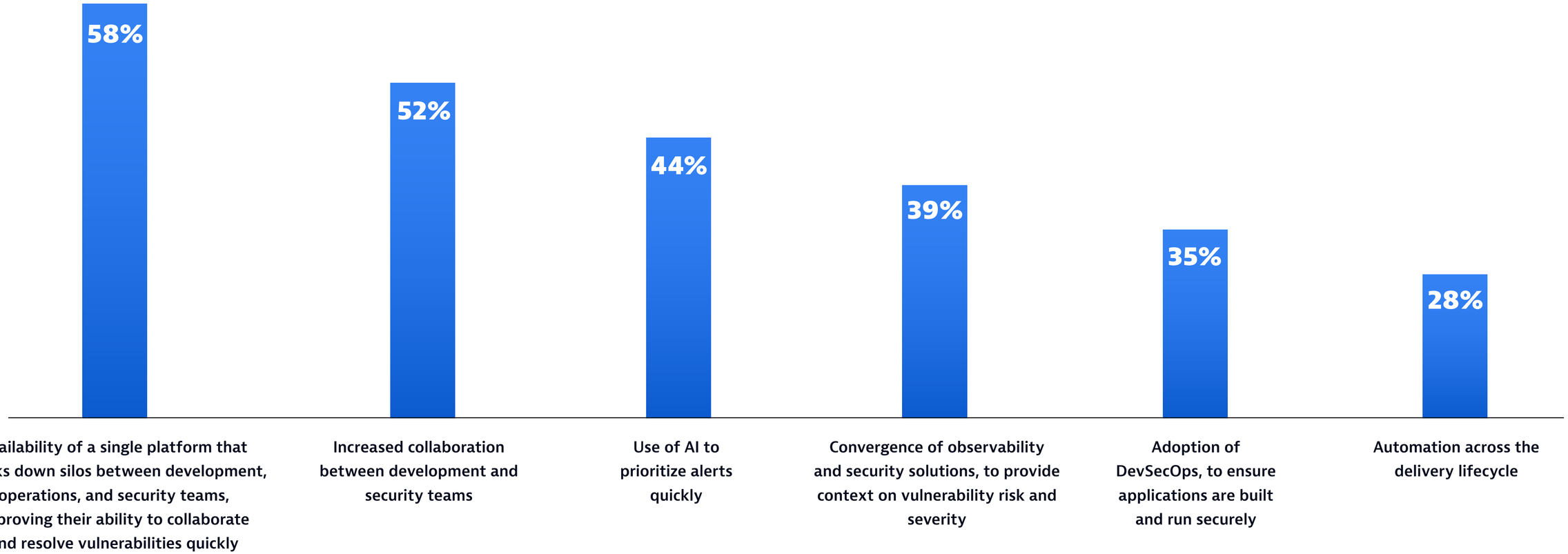


of CISOs say that automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions.

CHAPTER 5

The convergence of automation, observability, and security is key to success

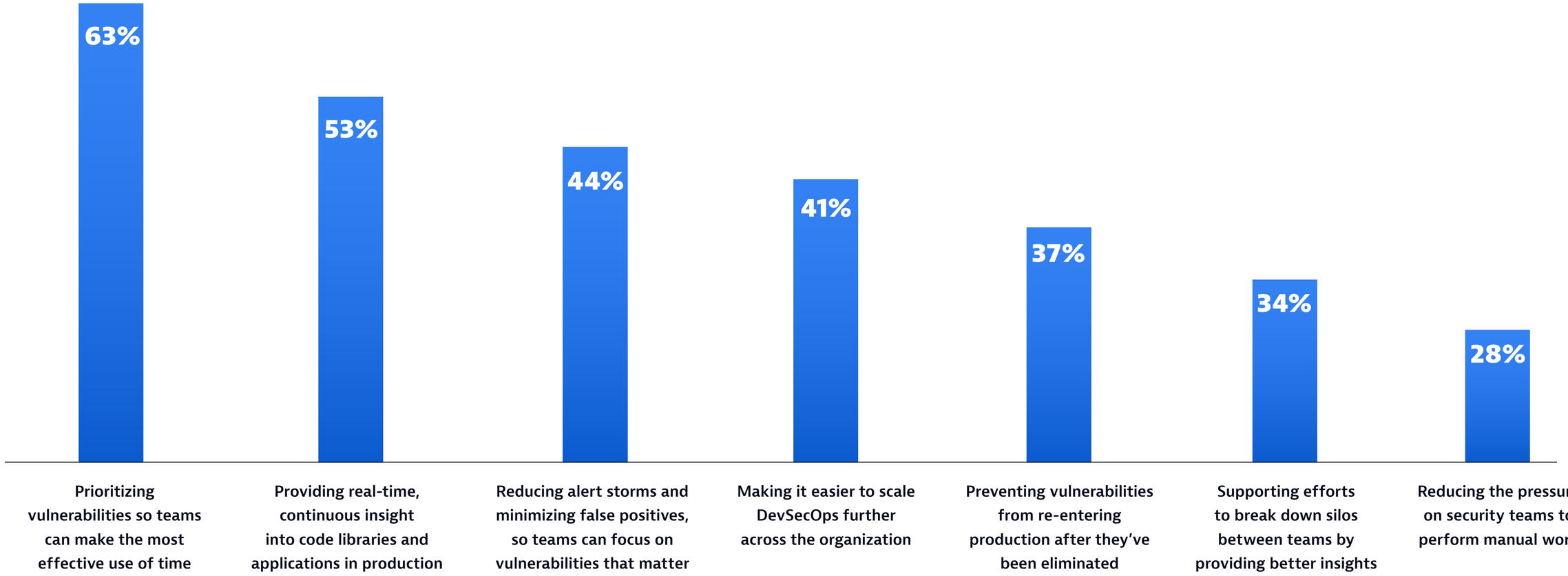
Factors that CISOs say will be most critical to ensuring application security vulnerabilities can be identified, prioritized, and resolved quickly include the following:



CHAPTER 5

The convergence of automation, observability, and security is key to 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. It removes blind spots and helps ensure development teams aren't wasting time chasing false positives, and it provides the Csuite 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.

Methodology

This report is based on a global survey of 1,300 CISOs in large organizations with more than 1,000 employees, conducted by Coleman Parkes and commissioned by Dynatrace in April 2022. The sample included 200 respondents in the U.S.; 100 each in the U.K., France, Germany, Spain, Italy, the Nordics, the Middle East, Australia, and India; and 50 each in Singapore, Malaysia, Brazil, and Mexico.

Global Data Summary: U.S. & Latin America

Sample includes 200 respondents from the U.S. and 50 respondents from each of Brazil and Mexico.

Section 1

Country	Organizations have a layered cybersecurity posture	CISOs say there are still gaps that allow vulnerabilities into production	Organizations have runtime vulnerability management capabilities	Organizations have real-time visibility into runtime vulnerabilities in containerized environments
U.S.	63%	76%	36%	2%
Brazil	76%	74%	44%	16%
Mexico	76%	78%	54%	0%

Security solutions organizations most commonly use	U.S.	Brazil	Mexico
Antivirus scanning	71%	70%	72%
Email security / encryption	60%	66%	64%
Web application firewall (WAF)	57%	74%	72%
Data encryption	58%	62%	66%
Real-time attack detection and blocking	50%	54%	60%
Two-factor authentication (2FA)	46%	40%	42%
Vulnerability scanners	42%	42%	52%
Endpoint protection	32%	38%	50%
Runtime vulnerability management	36%	44%	54%
DNS and/or URL filtering	27%	44%	44%
SIEM / log analytics	28%	24%	32%

Global Data Summary: U.S. & Latin America

Sample includes 200 respondents from the U.S. and 50 respondents from each of Brazil and Mexico.

Section 2

Country	Security teams that can access an accurate, continuously updated report of every application and code library in production in real time	Security teams that admit they don't always know which third-party code libraries they have running in production	Organizations that say they faced risk exposure from Log4Shell	Organizations that say they faced 'high' or 'severe' risk exposure from Log4Shell	Average number of hours security teams spent responding to the Log4j vulnerability	CISOs that are fully confident their teams could identify and resolve all instances of Log4Shell in their environment
U.S.	28%	28%	94%	42%	54	47%
Brazil	30%	22%	92%	24%	36	45%
Mexico	30%	24%	94%	14%	45	51%

Challenges security teams experienced in handling the response to Log4Shell	U.S.	Brazil	Mexico
Speed of development makes it difficult to prevent vulnerabilities coming back	61%	59%	72%
Volume of false positives or low impact alerts make it difficult to prioritize which exposures to resolve first	53%	48%	66%
Significant manual effort to evaluate our risk exposure	47%	35%	51%
Limited collaboration between security and development teams delayed our response	40%	28%	43%
Limited or delayed insight into what is running in production	35%	24%	28%
Limited context within alerts to identify the risk impact	26%	28%	19%

Most common behaviors in security teams when major new vulnerabilities such as Log4Shell are discovered	U.S.	Brazil	Mexico
Huge increase in remediation tickets for development teams	68%	58%	70%
Significant increase in manual war rooms	52%	48%	74%
Teams having to work around the clock	42%	38%	36%
Tier-2 or 3 vulnerabilities are ignored while the focus is on the crisis	40%	36%	36%
Feeling of being overwhelmed	32%	40%	34%
Sense of panic	28%	16%	26%

Global Data Summary: U.S. & Latin America

Sample includes 200 respondents from the U.S. and 50 respondents from each of Brazil and Mexico.

Section 3

Country	CISOs say vulnerability management has become more difficult as the need to accelerate digital transformation has increased	CISOs say developers don't always have time to scan for vulnerabilities in their code and apply a fix before it moves into production	CISOs are fully confident that applications have been fully tested for vulnerabilities before going live in production	Organizations have a mature DevSecOps culture, where the majority of teams have integrated security practices across the SDLC
U.S.	68%	66%	28%	32%
Brazil	74%	64%	16%	54%
Mexico	62%	66%	14%	28%

Factors that make it more difficult to identify and resolve application vulnerabilities	U.S.	Brazil	Mexico
Use of third-party / open-source code	62%	74%	96%
New ways of working / use of DevOps / Agile development cycles	60%	54%	76%
Use of multicloud environments	50%	42%	66%
Use of new programming languages	52%	42%	28%
Rising number of CVEs (Common Vulnerabilities and Exposures) being logged	32%	46%	34%
Pattern-based detection is less reliable in rapidly changing cloud environments	40%	28%	40%
Limited resources (e.g., people)	39%	28%	20%

Most common problems CISOs encounter when addressing application vulnerabilities	U.S.	Brazil	Mexico
The speed of modern software delivery makes it easier for vulnerabilities to re-enter production after remediation	52%	40%	50%
Development teams increasingly need to take responsibility for the security of their own code, but lack the expertise	50%	32%	56%
Vulnerabilities discovered after the application was deployed can be difficult to detect quickly enough to minimize the risk of an exploit	38%	38%	56%
Development teams say they have little context about each vulnerability, making it difficult to apply a fix quickly	40%	22%	26%
Development teams often don't collaborate with security due to concerns about being slowed down	25%	28%	20%

Global Data Summary: U.S. & Latin America

Sample includes 200 respondents from the U.S. and 50 respondents from each of Brazil and Mexico.

Section 4

Country	Average number of alerts to potential application security vulnerabilities organizations receive each month	CISOs say most security alerts and vulnerabilities are false positives that don't require action because they are not true exposures	Average percentage of application security vulnerability alerts organizations receive each day that require actioning (2022)	Average percentage of application security vulnerability alerts organizations receive each day that required actioning (2021)	Average proportion of time application security teams spend on vulnerability management tasks that could be automated	CISOs say the volume of alerts makes it difficult to prioritize vulnerabilities based on risk and impact
U.S.	2251	76%	33%	47%	29%	72%
Brazil	2278	76%	25%	46%	30%	72%
Mexico	983	92%	24%	36%	29.5%	58%

Global Data Summary: U.S. & Latin America

Sample includes 200 respondents from the U.S. and 50 respondents from each of Brazil and Mexico.

Section 5

Country	CISOs agree security must be a shared responsibility across the software delivery lifecycle, from development to production	CISOs say automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions
U.S.	78%	79%
Brazil	86%	90%
Mexico	88%	82%

Factors CISOs say will be most critical to ensuring application security vulnerabilities can be identified, prioritized, and resolved quickly and effectively in the future	U.S.	Brazil	Mexico
Availability of a single platform that breaks down silos between development, operations, and security teams, improving their ability to collaborate and resolve vulnerabilities quickly	60%	56%	80%
Increased collaboration between development and security teams	62%	60%	64%
Use of AI to prioritize alerts quickly	47%	50%	58%
Convergence of observability and security solutions, to provide context on vulnerability risk and severity	35%	44%	30%
Adoption of DevSecOps, to ensure applications are built and run securely	32%	38%	28%
Automation across the delivery lifecycle	24%	24%	14%

Biggest benefits CISOs identify in increasing the use of AI and automation in security practices	U.S.	Brazil	Mexico
Prioritizing vulnerabilities so teams can make the most effective use of time	68%	82%	80%
Providing real-time, continuous insight into code libraries and applications in production	54%	56%	58%
Reducing alert storms and minimizing false positives, so teams can focus on vulnerabilities that matter	42%	46%	42%
Making it easier to scale DevSecOps further across the organization	40%	42%	50%
Preventing vulnerabilities from re-entering production after they've been eliminated	34%	32%	28%
Supporting efforts to break down silos between teams by providing better insights	27%	28%	24%
Reducing the pressure on security teams to perform manual work	31%	12%	10%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Section 1

Country	Organizations have a layered cybersecurity posture	CISOs say there are still gaps that allow vulnerabilities into production	Organizations have runtime vulnerability management capabilities	Organizations have real-time visibility into runtime vulnerabilities in containerized environments
UK	44%	78%	39%	3%
France	58%	69%	26%	2%
Germany	64%	76%	40%	6%
Spain	61%	76%	40%	7%
Italy	54%	76%	39%	8%
Sweden	73%	70%	39%	0%
Finland	59%	62%	53%	6%
Norway	70%	70%	36%	6%

Security solutions organizations most commonly use	UK	France	Germany	Spain	Italy	Sweden	Norway	Finland
Antivirus scanning	47%	77%	61%	57%	68%	64%	79%	59%
Email security / encryption	51%	59%	65%	44%	54%	79%	64%	79%
Web application firewall (WAF)	46%	62%	54%	56%	57%	48%	61%	44%
Data encryption	41%	57%	41%	45%	37%	33%	61%	38%
Real-time attack detection and blocking	46%	42%	46%	49%	51%	36%	61%	50%
Two-factor authentication (2FA)	39%	37%	39%	47%	43%	55%	55%	47%
Vulnerability scanners	35%	41%	47%	45%	38%	58%	36%	38%
Endpoint protection	42%	48%	43%	38%	34%	55%	33%	47%
Runtime vulnerability management	39%	26%	40%	40%	39%	39%	36%	53%
DNS and/or URL filtering	39%	26%	23%	36%	37%	39%	42%	38%
SIEM / log analytics	25%	19%	25%	30%	23%	33%	27%	18%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Section 2

Country	Security teams that can access an accurate, continuously updated report of every application and code library in production in real time	Security teams that admit they don't always know which third-party code libraries they have running in production	Organizations that say they faced risk exposure from Log4Shell	Organizations that say they faced 'high' or 'severe' risk exposure from Log4Shell	Average number of hours security teams spent responding to the Log4j vulnerability	CISOs that are fully confident their teams could identify and resolve all instances of Log4Shell in their environment
UK	32%	35%	93%	27%	66	46%
France	14%	37%	93%	39%	57	31%
Germany	24%	36%	97%	41%	55	39%
Spain	33%	21%	95%	24%	48	41%
Italy	33%	33%	94%	34%	54	27%
Sweden	25%	39%	100%	33%	63	38%
Finland	17%	45%	97%	50%	39	27%
Norway	19%	26%	97%	30%	38	53%

Challenges security teams experienced in handling the response to Log4Shell	UK	France	Germany	Spain	Italy	Sweden	Norway	Finland
Speed of development makes it difficult to prevent vulnerabilities coming back	52%	69%	54%	48%	51%	61%	56%	64%
Volume of false positives or low impact alerts make it difficult to prioritize which exposures to resolve first	45%	55%	58%	47%	45%	73%	56%	55%
Significant manual effort to evaluate our risk exposure	38%	53%	45%	38%	36%	39%	53%	36%
Limited collaboration between security and development teams delayed our response	46%	38%	44%	41%	34%	42%	34%	64%
Limited or delayed insight into what is running in production	38%	13%	30%	33%	37%	27%	31%	33%
Limited context within alerts to identify the risk impact	34%	22%	27%	33%	24%	27%	41%	33%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Most common behaviors in security teams when major new vulnerabilities such as Log4Shell are discovered	UK	France	Germany	Spain	Italy	Sweden	Norway	Finland
Huge increase in remediation tickets for development teams	47%	62%	65%	62%	54%	70%	67%	47%
Significant increase in manual war rooms	45%	55%	54%	49%	46%	55%	55%	44%
Teams having to work around the clock	47%	41%	34%	30%	39%	42%	39%	59%
Tier-2 or 3 vulnerabilities are ignored while the focus is on the crisis	43%	32%	44%	37%	34%	30%	52%	38%
Feeling of being overwhelmed	27%	18%	31%	21%	23%	33%	30%	32%
Sense of panic	17%	18%	20%	16%	11%	33%	21%	32%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Section 3

Country	CISOs say vulnerability management has become more difficult as the need to accelerate digital transformation has increased	CISOs say developers don't always have time to scan for vulnerabilities in their code and apply a fix before it moves into production	CISOs are fully confident that applications have been fully tested for vulnerabilities before going live in production	Organizations have a mature DevSecOps culture, where the majority of teams have integrated security practices across the SDLC
UK	61%	64%	36%	35%
France	70%	61%	4%	32%
Germany	74%	77%	22%	31%
Spain	67%	66%	40%	45%
Italy	74%	73%	31%	41%
Sweden	60%	67%	21%	36%
Finland	70%	65%	41%	24%
Norway	60%	52%	9%	42%

Factors that make it more difficult to identify and resolve application vulnerabilities	UK	France	Germany	Spain	Italy	Sweden	Norway	Finland
Use of third-party / open-source code	50%	76%	70%	60%	58%	58%	70%	59%
New ways of working / use of DevOps / Agile development cycles	51%	68%	60%	48%	50%	55%	55%	53%
Use of multicloud environments	39%	52%	52%	47%	52%	55%	52%	53%
Use of new programming languages	43%	38%	47%	44%	46%	42%	45%	50%
Rising number of CVEs (Common Vulnerabilities and Exposures) being logged	50%	25%	36%	50%	42%	45%	45%	32%
Pattern-based detection is less reliable in rapidly changing cloud environments	35%	25%	30%	37%	35%	33%	55%	35%
Limited resources (e.g., people)	33%	28%	29%	17%	18%	45%	24%	38%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Most common problems CISOs encounter when addressing application vulnerabilities	UK	France	Germany	Spain	Italy	Sweden	Norway	Finland
The speed of modern software delivery makes it easier for vulnerabilities to re-enter production after remediation	48%	46%	52%	44%	49%	48%	67%	65%
Development teams increasingly need to take responsibility for the security of their own code, but lack the expertise	36%	60%	46%	42%	29%	55%	48%	50%
Vulnerabilities discovered after the application was deployed can be difficult to detect quickly enough to minimize the risk of an exploit	34%	48%	52%	40%	34%	45%	24%	38%
Development teams say they have little context about each vulnerability, making it difficult to apply a fix quickly	32%	20%	21%	29%	27%	24%	36%	24%
Development teams often don't collaborate with security due to concerns about being slowed down	35%	16%	26%	13%	20%	39%	18%	32%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Section 4

Country	Average number of alerts to potential application security vulnerabilities organizations receive each month	CISOs say most security alerts and vulnerabilities are false positives that don't require action because they are not true exposures	Average percentage of application security vulnerability alerts organizations receive each day that require actioning (2022)	Average percentage of application security vulnerability alerts organizations receive each day that required actioning (2021)	Average proportion of time application security teams spend on vulnerability management tasks that could be automated	CISOs say the volume of alerts makes it difficult to prioritize vulnerabilities based on risk and impact
UK	2518	69%	33%	41%	26.5%	70%
France	2032	76%	32%	42%	28%	71%
Germany	1932	71%	34%	37%	31%	74%
Spain	1664	82%	27%	36%	25%	66%
Italy	2044	74%	31%	N/A	24%	68%
Sweden	1557	85%	32%	N/A	27%	67%
Finland	1894	88%	33%	N/A	29%	82%
Norway	2637	79%	33%	N/A	28%	58%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Section 5

Country	CISOs agree security must be a shared responsibility across the software delivery lifecycle, from development to production	CISOs say automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions
UK	73%	80%
France	73%	82%
Germany	87%	90%
Spain	87%	82%
Italy	91%	81%
Sweden	70%	58%
Finland	82%	68%
Norway	70%	67%

Factors CISOs say will be most critical to ensuring application security vulnerabilities can be identified, prioritized, and resolved quickly and effectively in the future	UK	France	Germany	Spain	Italy	Sweden	Norway	Finland
Availability of a single platform that breaks down silos between development, operations, and security teams, improving their ability to collaborate and resolve vulnerabilities quickly	52%	69%	58%	52%	45%	58%	52%	62%
Increased collaboration between development and security teams	45%	62%	46%	39%	40%	61%	64%	50%
Use of AI to prioritize alerts quickly	34%	37%	43%	45%	35%	48%	42%	41%
Convergence of observability and security solutions, to provide context on vulnerability risk and severity	45%	22%	30%	32%	38%	33%	64%	35%
Adoption of DevSecOps, to ensure applications are built and run securely	38%	29%	39%	37%	31%	21%	48%	26%
Automation across the delivery lifecycle	28%	18%	24%	27%	33%	18%	30%	15%

Global Data Summary: Europe

Sample includes 100 respondents from each of the UK, France, Germany, Spain, and Italy, 33 respondents from each of Sweden and Norway, and 34 from Finland.

Biggest benefits CISOs identify in increasing the use of AI and automation in security practices	UK	France	Germany	Spain	Italy	Sweden	Norway	Finland
Prioritizing vulnerabilities so teams can make the most effective use of time	42%	81%	64%	52%	49%	76%	58%	74%
Providing real-time, continuous insight into code libraries and applications in production	42%	61%	49%	48%	48%	61%	70%	76%
Reducing alert storms and minimizing false positives, so teams can focus on vulnerabilities that matter	32%	43%	52%	51%	39%	48%	70%	26%
Making it easier to scale DevSecOps further across the organization	39%	28%	39%	42%	41%	52%	61%	38%
Preventing vulnerabilities from re-entering production after they've been eliminated	35%	33%	35%	36%	33%	21%	30%	35%
Supporting efforts to break down silos between teams by providing better insights	52%	21%	26%	36%	25%	33%	42%	32%
Reducing the pressure on security teams to perform manual work	24%	15%	23%	23%	39%	27%	12%	24%

Global Data Summary: Middle East

Sample includes 25 respondents from each of the UAE, Egypt, Qatar, and Saudi Arabia.

Section 1

Country	Organizations have a layered cybersecurity posture	CISOs say there are still gaps that allow vulnerabilities into production	Organizations have runtime vulnerability management capabilities	Organizations have real-time visibility into runtime vulnerabilities in containerized environments
UAE	52%	64%	28%	4%
Egypt	64%	80%	44%	4%
Qatar	60%	80%	28%	4%
Saudi Arabia	68%	80%	48%	4%

Security solutions organizations most commonly use	UAE	Egypt	Qatar	Saudi Arabia
Antivirus scanning	60%	84%	60%	60%
Email security / encryption	44%	28%	52%	64%
Web application firewall (WAF)	52%	60%	60%	60%
Data encryption	44%	52%	60%	64%
Real-time attack detection and blocking	36%	40%	48%	52%
Two-factor authentication (2FA)	44%	40%	40%	28%
Vulnerability scanners	40%	40%	56%	40%
Endpoint protection	20%	32%	44%	16%
Runtime vulnerability management	28%	44%	28%	48%
DNS and/or URL filtering	36%	12%	44%	40%
SIEM / log analytics	12%	32%	24%	32%

Global Data Summary: Middle East

Sample includes 25 respondents from each of the UAE, Egypt, Qatar, and Saudi Arabia.

Section 2

Country	Security teams that can access an accurate, continuously updated report of every application and code library in production in real time	Security teams that admit they don't always know which third-party code libraries they have running in production	Organizations that say they faced risk exposure from Log4Shell	Organizations that say they faced 'high' or 'severe' risk exposure from Log4Shell	Average number of hours security teams spent responding to the Log4j vulnerability	CISOs that are fully confident their teams could identify and resolve all instances of Log4Shell in their environment
UAE	12%	28%	92%	40%	70	48%
Egypt	16%	36%	100%	24%	44	28%
Qatar	24%	32%	96%	40%	43	50%
Saudi Arabia	8%	52%	96%	40%	55	38%

Challenges security teams experienced in handling the response to Log4Shell	UAE	Egypt	Qatar	Saudi Arabia
Speed of development makes it difficult to prevent vulnerabilities coming back	52%	44%	67%	62%
Volume of false positives or low impact alerts make it difficult to prioritize which exposures to resolve first	39%	48%	67%	67%
Significant manual effort to evaluate our risk exposure	43%	44%	38%	38%
Limited collaboration between security and development teams delayed our response	52%	40%	50%	29%
Limited or delayed insight into what is running in production	43%	32%	33%	42%
Limited context within alerts to identify the risk impact	35%	16%	33%	25%

Most common behaviors in security teams when major new vulnerabilities such as Log4Shell are discovered	UAE	Egypt	Qatar	Saudi Arabia
Huge increase in remediation tickets for development teams	52%	44%	64%	60%
Significant increase in manual war rooms	60%	52%	52%	44%
Teams having to work around the clock	48%	48%	48%	52%
Tier-2 or 3 vulnerabilities are ignored while the focus is on the crisis	44%	32%	40%	56%
Feeling of being overwhelmed	28%	24%	24%	20%
Sense of panic	20%	24%	12%	28%

Global Data Summary: Middle East

Sample includes 25 respondents from each of the UAE, Egypt, Qatar, and Saudi Arabia.

Section 3

Country	CISOs say vulnerability management has become more difficult as the need to accelerate digital transformation has increased	CISOs say developers don't always have time to scan for vulnerabilities in their code and apply a fix before it moves into production	CISOs are fully confident that applications have been fully tested for vulnerabilities before going live in production	Organizations have a mature DevSecOps culture, where the majority of teams have integrated security practices across the SDLC
UAE	72%	60%	28%	32%
Egypt	88%	68%	16%	28%
Qatar	72%	56%	24%	36%
Saudi Arabia	76%	64%	36%	16%

Factors that make it more difficult to identify and resolve application vulnerabilities	UAE	Egypt	Qatar	Saudi Arabia
Use of third-party / open-source code	68%	80%	80%	44%
New ways of working / use of DevOps / Agile development cycles	36%	40%	48%	64%
Use of multicloud environments	48%	48%	56%	36%
Use of new programming languages	40%	64%	60%	44%
Rising number of CVEs (Common Vulnerabilities and Exposures) being logged	44%	36%	44%	44%
Pattern-based detection is less reliable in rapidly changing cloud environments	40%	24%	28%	48%
Limited resources (e.g., people)	28%	24%	44%	24%

Most common problems CISOs encounter when addressing application vulnerabilities	UAE	Egypt	Qatar	Saudi Arabia
The speed of modern software delivery makes it easier for vulnerabilities to re-enter production after remediation	52%	36%	40%	52%
Development teams increasingly need to take responsibility for the security of their own code, but lack the expertise	44%	52%	48%	44%
Vulnerabilities discovered after the application was deployed can be difficult to detect quickly enough to minimize the risk of an exploit	36%	24%	44%	40%
Development teams say they have little context about each vulnerability, making it difficult to apply a fix quickly	24%	36%	32%	24%
Development teams often don't collaborate with security due to concerns about being slowed down	40%	20%	56%	40%

Global Data Summary: Middle East

Sample includes 25 respondents from each of the UAE, Egypt, Qatar, and Saudi Arabia.

Section 4

Country	Average number of alerts to potential application security vulnerabilities organizations receive each month	CISOs say most security alerts and vulnerabilities are false positives that don't require action because they are not true exposures	Average percentage of application security vulnerability alerts organizations receive each day that require actioning (2022)	Average proportion of time application security teams spend on vulnerability management tasks that could be automated	CISOs say the volume of alerts makes it difficult to prioritize vulnerabilities based on risk and impact
UAE	2695	76%	36%	33%	80%
Egypt	1520	60%	36%	36%	80%
Qatar	2060	68%	30%	31%	72%
Saudi Arabia	1735	68%	30%	33%	64%

Global Data Summary: Middle East

Sample includes 25 respondents from each of the UAE, Egypt, Qatar, and Saudi Arabia.

Section 5

Country	CISOs agree security must be a shared responsibility across the software delivery lifecycle, from development to production	CISOs say automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions
UAE	80%	72%
Egypt	76%	72%
Qatar	68%	60%
Saudi Arabia	76%	68%

Factors CISOs say will be most critical to ensuring application security vulnerabilities can be identified, prioritized, and resolved quickly and effectively in the future	UAE	Egypt	Qatar	Saudi Arabia
Availability of a single platform that breaks down silos between development, operations, and security teams, improving their ability to collaborate and resolve vulnerabilities quickly	60%	44%	56%	44%
Increased collaboration between development and security teams	36%	56%	60%	52%
Use of AI to prioritize alerts quickly	40%	52%	48%	32%
Convergence of observability and security solutions, to provide context on vulnerability risk and severity	36%	48%	40%	52%
Adoption of DevSecOps, to ensure applications are built and run securely	36%	28%	56%	36%
Automation across the delivery lifecycle	28%	16%	20%	24%

Biggest benefits CISOs identify in increasing the use of AI and automation in security practices	UAE	Egypt	Qatar	Saudi Arabia
Prioritizing vulnerabilities so teams can make the most effective use of time	60%	44%	60%	52%
Providing real-time, continuous insight into code libraries and applications in production	44%	44%	60%	28%
Reducing alert storms and minimizing false positives, so teams can focus on vulnerabilities that matter	52%	40%	32%	28%
Making it easier to scale DevSecOps further across the organization	44%	40%	40%	36%
Preventing vulnerabilities from re-entering production after they've been eliminated	36%	20%	40%	64%
Supporting efforts to break down silos between teams by providing better insights	28%	44%	24%	28%
Reducing the pressure on security teams to perform manual work	32%	28%	44%	20%

Global Data Summary: Asia Pacific

Sample includes 100 respondents from each of Australia and India, and 50 respondents from each of Singapore and Malaysia.

Section 1

Country	Organizations have a layered cybersecurity posture	CISOs say there are still gaps that allow vulnerabilities into production	Organizations have runtime vulnerability management capabilities	Organizations have real-time visibility into runtime vulnerabilities in containerized environments
Australia	58%	76%	30%	2%
India	62%	79%	30%	3%
Singapore	48%	62%	38%	0%
Malaysia	64%	80%	32%	0%

Security solutions organizations most commonly use	Australia	India	Singapore	Malaysia
Antivirus scanning	58%	62%	56%	56%
Email security / encryption	59%	59%	58%	70%
Web application firewall (WAF)	59%	61%	44%	56%
Data encryption	58%	51%	52%	42%
Real-time attack detection and blocking	52%	58%	36%	36%
Two-factor authentication (2FA)	40%	51%	52%	54%
Vulnerability scanners	29%	36%	42%	38%
Endpoint protection	45%	39%	36%	38%
Runtime vulnerability management	30%	30%	38%	32%
DNS and/or URL filtering	31%	28%	24%	36%
SIEM / log analytics	21%	15%	12%	28%

Global Data Summary: Asia Pacific

Sample includes 100 respondents from each of Australia and India, and 50 respondents from each of Singapore and Malaysia.

Section 2

Country	Security teams that can access an accurate, continuously updated report of every application and code library in production in real time	Security teams that admit they don't always know which third-party code libraries they have running in production	Organizations that say they faced risk exposure from Log4Shell	Organizations that say they faced 'high' or 'severe' risk exposure from Log4Shell	Average number of hours security teams spent responding to the Log4j vulnerability	CISOs that are fully confident their teams could identify and resolve all instances of Log4Shell in their environment
Australia	32%	37%	96%	41%	45	52%
India	20%	30%	96%	43%	52	42%
Singapore	14%	49%	94%	28%	61	31%
Malaysia	18%	36%	96%	40%	40	25%

Challenges security teams experienced in handling the response to Log4Shell	Australia	India	Singapore	Malaysia
Speed of development makes it difficult to prevent vulnerabilities coming back	68%	59%	65%	49%
Volume of false positives or low impact alerts make it difficult to prioritize which exposures to resolve first	55%	54%	43%	51%
Significant manual effort to evaluate our risk exposure	47%	43%	49%	39%
Limited collaboration between security and development teams delayed our response	37%	47%	31%	53%
Limited or delayed insight into what is running in production	35%	48%	43%	31%
Limited context within alerts to identify the risk impact	40%	30%	51%	39%

Most common behaviors in security teams when major new vulnerabilities such as Log4Shell are discovered	Australia	India	Singapore	Malaysia
Huge increase in remediation tickets for development teams	53%	54%	56%	58%
Significant increase in manual war rooms	54%	54%	54%	64%
Teams having to work around the clock	49%	48%	56%	54%
Tier-2 or 3 vulnerabilities are ignored while the focus is on the crisis	50%	40%	40%	52%
Feeling of being overwhelmed	43%	37%	44%	36%
Sense of panic	25%	23%	28%	34%

Global Data Summary: Asia Pacific

Sample includes 100 respondents from each of Australia and India, and 50 respondents from each of Singapore and Malaysia.

Section 3

Country	CISOs say vulnerability management has become more difficult as the need to accelerate digital transformation has increased	CISOs say developers don't always have time to scan for vulnerabilities in their code and apply a fix before it moves into production	CISOs are fully confident that applications have been fully tested for vulnerabilities before going live in production	Organizations have a mature DevSecOps culture, where the majority of teams have integrated security practices across the SDLC
Australia	58%	64%	40%	38%
India	75%	68%	55%	37%
Singapore	64%	74%	22%	18%
Malaysia	74%	74%	18%	18%

Factors that make it more difficult to identify and resolve application vulnerabilities	Australia	India	Singapore	Malaysia
Use of third-party / open-source code	52%	45%	48%	50%
New ways of working / use of DevOps / Agile development cycles	53%	50%	58%	50%
Use of multicloud environments	49%	52%	48%	52%
Use of new programming languages	53%	52%	60%	52%
Rising number of CVEs (Common Vulnerabilities and Exposures) being logged	53%	50%	38%	52%
Pattern-based detection is less reliable in rapidly changing cloud environments	44%	45%	30%	42%
Limited resources (e.g., people)	35%	42%	26%	54%

Most common problems CISOs encounter when addressing application vulnerabilities	Australia	India	Singapore	Malaysia
The speed of modern software delivery makes it easier for vulnerabilities to re-enter production after remediation	50%	56%	58%	58%
Development teams increasingly need to take responsibility for the security of their own code, but lack the expertise	50%	51%	62%	36%
Vulnerabilities discovered after the application was deployed can be difficult to detect quickly enough to minimize the risk of an exploit	44%	39%	38%	58%
Development teams say they have little context about each vulnerability, making it difficult to apply a fix quickly	35%	43%	40%	38%
Development teams often don't collaborate with security due to concerns about being slowed down	28%	42%	26%	38%

Global Data Summary: Asia Pacific

Sample includes 100 respondents from each of Australia and India, and 50 respondents from each of Singapore and Malaysia.

Section 4

Country	Average number of alerts to potential application security vulnerabilities organizations receive each month	CISOs say most security alerts and vulnerabilities are false positives that don't require action because they are not true exposures	Average percentage of application security vulnerability alerts organizations receive each day that require actioning (2022)	Average proportion of time application security teams spend on vulnerability management tasks that could be automated	CISOs say the volume of alerts makes it difficult to prioritize vulnerabilities based on risk and impact
Australia	1777	65%	33%	27%	63%
India	2355	66%	34%	30%	67%
Singapore	1928	68%	31%	29%	60%
Malaysia	1810	66%	36%	26%	78%

Global Data Summary: Asia Pacific

Sample includes 100 respondents from each of Australia and India, and 50 respondents from each of Singapore and Malaysia.

Section 5

Country	CISOs agree security must be a shared responsibility across the software delivery lifecycle, from development to production	CISOs say automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions
Australia	79%	78%
India	87%	81%
Singapore	76%	80%
Malaysia	80%	76%

Factors CISOs say will be most critical to ensuring application security vulnerabilities can be identified, prioritized, and resolved quickly and effectively in the future	Australia	India	Singapore	Malaysia
Availability of a single platform that breaks down silos between development, operations, and security teams, improving their ability to collaborate and resolve vulnerabilities quickly	50%	66%	68%	64%
Increased collaboration between development and security teams	55%	41%	46%	50%
Use of AI to prioritize alerts quickly	52%	55%	32%	36%
Convergence of observability and security solutions, to provide context on vulnerability risk and severity	52%	45%	36%	64%
Adoption of DevSecOps, to ensure applications are built and run securely	34%	40%	38%	40%
Automation across the delivery lifecycle	51%	42%	28%	36%

Biggest benefits CISOs identify in increasing the use of AI and automation in security practices	Australia	India	Singapore	Malaysia
Prioritizing vulnerabilities so teams can make the most effective use of time	65%	66%	62%	64%
Providing real-time, continuous insight into code libraries and applications in production	54%	56%	52%	46%
Reducing alert storms and minimizing false positives, so teams can focus on vulnerabilities that matter	49%	46%	46%	42%
Making it easier to scale DevSecOps further across the organization	41%	45%	42%	48%
Preventing vulnerabilities from re-entering production after they've been eliminated	45%	53%	38%	40%
Supporting efforts to break down silos between teams by providing better insights	52%	37%	58%	36%
Reducing the pressure on security teams to perform manual work	36%	44%	26%	40%

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**

05.31.22 17322_EBK_jw