illumio

The 2025 Global Cloud Detection and Response Report

The State of Observability in the Breach Containment Era



Contents

PART 1

Introduction 3

PART 2

Summary of key findings 5

Visibility and context challenges 6

Alert volume and prioritization 7

Lateral movement risk 8

Tooling limitations 8

Security confidence and risk reduction 9

PART 3

Question-by-question analysis 10

Visibility and context challenges 11

Alert volume and prioritization 16

Lateral movement risk 23

Tooling limitations 27

Security confidence and risk reduction 31

PART 4

Conclusion 33

APPENDIX

Methodology and participant profile 35

PART 1

Introduction

Security teams can't protect what they can't see or understand. And today, it's less than ever.

As organizations adopt hybrid infrastructure and cloud-native applications, visibility is shrinking while complexity grows.

Security teams are often left without a clear picture of what's running, where it's vulnerable, or how it's being accessed. This is making early threat detection and rapid response increasingly difficult.

Teams are overwhelmed by high alert volumes, limited context, and rising uncertainty. False positives waste time. Lateral movement often goes undetected. Without knowing what's happening inside their network, even mature security programs are at risk of missing what matters most.

To better understand these challenges, Illumio commissioned independent research firm Vitreous World to survey 1,124 senior cybersecurity and IT decision-makers across 14 industries and 7 countries. The research set out to uncover how organizations are managing detection and response in the cloud, what's working, and where gaps remain.

This report explores five critical areas:

- Visibility and contextual understanding
- Alert volume, triage, and prioritization
- Detection of lateral movement
- Limitations in tooling and technology
- Security team confidence and risk reduction

The findings reveal a consistent story: security teams are doing their best in complex environments, but persistent challenges remain.

This report offers a global view into the current state of detection and response and a roadmap for leaders looking to improve visibility, reduce risk, and strengthen resilience.



PART 2

Summary of key findings

Cloud security is getting more attention — and more budget — than ever. But are organizations actually getting better at seeing and stopping threats?

While confidence is high in some areas, there are still major blind spots, alert overload is burning teams out, and too much network traffic is flying under the radar without the context needed to respond quickly or effectively.

This section breaks down the key takeaways from our research, including the numbers that matter and the story they tell. You'll get insight into what's working, where security teams are struggling, and how leaders are thinking about the future.



Visibility and context challenges

In cybersecurity, seeing isn't the same as understanding. Modern environments are sprawling and fast-moving, making it difficult to know what's really happening across the hybrid cloud.

The problem isn't just seeing traffic but understanding it. Too often, alerts lack the context needed to separate signal from noise. This leaves teams chasing false positives and missing lateral movement.

Cloud security spending climbs, but monitoring confidence shows gaps

Most IT and cybersecurity leaders expect an increase in cloud security budgets over the next year (91% net: increase). Significant increases are common across all markets, except in Japan, where a higher proportion expect budgets to remain unchanged.

Leaders are most confident in monitoring north-south traffic (net: 82%), encrypted traffic (net: 81%), and hybrid workload communications (net: 80%). Confidence is slightly lower for east-west traffic (net: 77%) and activity within containerized environments (net: 75%). Japan consistently reports lower confidence.

Security leaders trust their tools even while false positives persist

Leaders generally trust their detection capabilities. They have high agreement that current CDR/XDR solutions detect anomalous traffic (net: 84%) and feel they have full visibility of traffic anomalies across cloud and on-premises environments (net agree: 83%). There is also strong reliance on multiple tools to achieve comprehensive hybrid visibility (net agree: 87%).

False positives remain an issue (net: 58%), but confidence in detecting lateral movement and breaches is strong (86%).

Over a third of network traffic lacks context, fueling incident response challenges

On average, 37.9% of network traffic lacks enough context for confident investigation and response. The U.S. and Australia report the highest levels (41.0% and 40.3% respectively), while Brazil and Japan report the lowest (34.0% and 34.9% respectively).

Nearly all leaders (net: 93%) reported challenges in responding to security incidents over the past 12 months, mainly tool/technology-related (net: 42%) or human/process-based (net: 39%). Top issues include insufficient resources (14%), difficulty correlating cloud and on-premises data (13%), and limited context from alerts (12%). Market-specific differences show Japan with the highest resource challenges and France struggling most with data correlation.

Alert volume and prioritization

Security teams are drowning in alerts, with thousands flooding dashboards every day. Most leaders say their teams can't keep up, and the backlog lets real threats slip through the cracks.

False positives make the problem worse, draining hours each week and distracting teams from investigating genuine risks. The result is burnout, costly downtime, and reputational damage when uninvestigated alerts turn into incidents.

Thousands of daily alerts leave security teams overwhelmed

On average, teams receive 2,020.3 daily alerts from detection systems. Germany (2,416.1) and France (2,336.1) report the highest daily alerts, while Japan (1,060.9) and Brazil (1,504.7) report the lowest.

Two-thirds of leaders (net: 67%) report receiving more alerts than their team can investigate. The U.S. (net: 79%), Australia (net: 83%), and Germany (net: 73%) exceed the global average, while Japan (net: 31%) and Brazil (net: 61%) are below average.

Top strategies to reduce alert fatigues are better alert prioritization based on risk and context (29%), improved integration of detection/response tools (29%) and more skilled analysts/staff (28%).

Uninvestigated alerts lead to breaches, with costly fallout

Nearly all leaders (net: 92%) report that uninvestigated alerts have caused real security incidents. Most occur rarely (44%) or sometimes (30%), with the highest 'rarely' rates in Brazil (55%) and Japan (51%).

On average, it takes 12.1 hours to detect the issue. Shortest detection times are in Japan (10.3 hours) and Brazil (10.9 hours), while longest are in the UK (13.6 hours) and Australia (13.1 hours). 95% (net) of organizations experienced impacts from missed alerts.

Top consequences are team burnout (21%), operational downtime (21%) and reputational damage (17%). Operational downtime is highest in Brazil (28%), reputational damage peaks in Australia (26%).

False positives drain 14 hours a week, distracting teams from real threats

On average, teams spend 14.1 hours per week on false positives. The longest duration was reported in Australia (15.9 hours), the U.S. (15.6 hours), and the UK (15.0 hours). The shortest was in Japan (11.1 hours) and Brazil (12.8 hours).

73% (net) of leaders report that false positives significantly (24%) or moderately (49%) hinder the focus on real threats. The impact is strongest in Australia (net: 85%) and the U.S. (net: 80%) and lowest in Japan (net: 55%) and Brazil (net: 63%).

Leading causes of false positives are lack of network/traffic visibility (21%), tool sprawl (21%), inadequate alert context (20%), and legacy/ineffective detection tech (19%). False positives impact organizations most through increased costs or wasted resources (25%) and missed/delayed responses to genuine threats (21%).

Lateral movement risk

Lateral movement is the process of attackers moving through your network, escalating privileges, compromising assets, and expanding their foothold. It's one of the most dangerous stages of an attack, and most organizations admit it's already happening in their environments.

While detection tools catch some incidents in real time, many are only uncovered during or after an attack. This leaves hours of downtime and costly losses in their wake.

Alert fatigue, blind spots in east-west traffic, and missing context make these threats especially hard to spot. The result is that even well-resourced teams struggle to contain attackers once they're inside the network.

90% of leaders report lateral movement incidents, but detection success varies widely

Most IT and cybersecurity leaders (net: 90%) have detected a security incident involving lateral movement within the past 12 months. Detection success varies: 54% were identified by detection tools during the attack, 31% during the incident but not due to detection tools, and 6% only afterward.

The U.S., UK, Brazil, and Australia report stronger tool-driven detection, whereas Japan had the highest rate (20%) of undetected incidents. Most IT and cybersecurity leaders (net: 95%) reported that their teams investigate potential lateral movement during an incident or alert review: 30% always investigate, 46% do so often when signs of compromise appear and 19% only sometimes investigate.

Lateral movement incidents drive hours of downtime and six-figure losses

Organizations who detected lateral movements during an incident reported an average of 7.1 hours of operational downtime. This impact was most severe in the U.S. (9.8 hours) and Australia (8.0 hours), while Brazil experienced the shortest downtime at 5.9 hours.

The financial toll of downtime linked to lateral movement incidents averaged USD 227,264.20 across organizations. Australia reported the highest average cost (USD 355,292.00), followed by Germany (USD 289,375.00). By comparison, Brazil (USD 139,651.20) and Japan (USD 143,939.40) saw the lowest cost estimates.

Alert fatigue and context gaps leave lateral movement detection elusive

Detecting lateral movement remains challenging. Leaders cite alert fatigue and lack of actionable insight as the top barriers.

Over a third (37%) reported being overwhelmed by too many alerts, particularly in Brazil (49%) and France (41%). Another 34% said they could see connections but lacked the context needed for action, while 31% struggled with visibility into east-west traffic, a particular pain point in Australia (45%).

Other recurring issues included difficulties correlating behaviors across cloud and on-premises (31%) and uncertainty in interpreting data (31%). Only a small minority (8%) said they faced no significant operational challenges, highlighting the complexity of addressing lateral movement.

Tooling limitations

Detection and response tools are everywhere, but effectiveness doesn't always match adoption.

Most organizations run multiple platforms to cover gaps, yet nearly all still report limitations, from alert fatigue and missing context to slow response times and incomplete hybrid coverage. These shortfalls leave security teams struggling to prioritize alerts and contain fast-moving threats.

Leaders see AI and automation as the way forward, promising sharper detection, faster response, and fewer manual workloads.

Detection and response tools fall short in the cloud

Most organizations use multiple cloud detection and response tools, with adoption rates from 79% (CNAPP) to 87% (NDR/CDR and XDR/MDR). Effectiveness rates vary from 67% (CNAPP) to 78% (NDR/CDR).

Nearly all organizations (net: 92%) face limitations with their current cloud detection and response capabilities in the cloud, rising to 97% (net) in Australia. The main challenges include alert fatigue (39%) and insufficient context to prioritize alerts (39%).

Other issues include slow value realization (34%), gaps in hybrid coverage (34%), limited lateral movement visibility (30%), lack of automated response (26%) and complexity of use (23%). Only 7% report no limitations.

Security leaders bet on AI to cut workloads and catch more threats

Organizations see AI and machine learning as most valuable in enhancing threat detection and improving operational efficiency. Key areas of impact include increasing threat detection accuracy (38%), accelerating incident response (34%), reducing manual workloads (32%), automating triage and prioritization (32%), detecting zero-day threats (32%) and identifying behavioral anomalies (32%).

AI and automation lead future security priorities

Organizations use a mix of automated, manual, and team-based approaches to respond to alerts in the cloud. About 28% respond automatically with predefined actions, 27% investigate in-platform but act via other tools, 25% rely on IT/DevOps teams and 18% respond manually in real time.

Future security priorities focus on AI/ML adoption, detection and automation: increasing AI/ML-driven capabilities (34%), improving cloud detection and response (34%), reducing mean time to detect/respond (33%) and automating threat triage/investigation (31%).

Security confidence and risk reduction

Confidence can be a double-edged sword in cybersecurity. Most leaders say they feel secure in their ability to detect and contain cloud threats. But confidence alone doesn't guarantee resilience.

Without faster root cause analysis, better correlation across multiple tools, and unified visibility, even confident teams can miss the signals that matter most. The stakes are high: every delay in detection or response increases risk, raises costs, and undermines trust.

Cloud threat confidence runs high, with most leaders feeling secure in detection

Organizations report high confidence in their ability to detect and contain cloud-based threats, with 92%–95% feeling confident across all areas. About half (51%–58%) are very confident in all areas, while 37%–41% are somewhat confident. The strongest confidence is in understanding the full impact of incidents (very confident: 58%) and detecting risks and vulnerabilities (very confident: 57%).

Alert correlation, speed, and visibility top the cloud threat management wishlist

IT and cybersecurity leaders identify several priorities to enhance cloud threat management. Top needs include correlating alerts across multiple sources (28%), faster root cause identification (27%) and unified visibility across environments or more skilled staff (26% each). Other key improvements include better integration between detection and response tools (25%) and improved alert filtering/customization (25%).

PART 3

Question-by-question analysis

Now that we've explored highlights from our research, this section takes a deeper look at the data behind them. Get a detailed view into how today's security teams are navigating detection and response in the cloud.

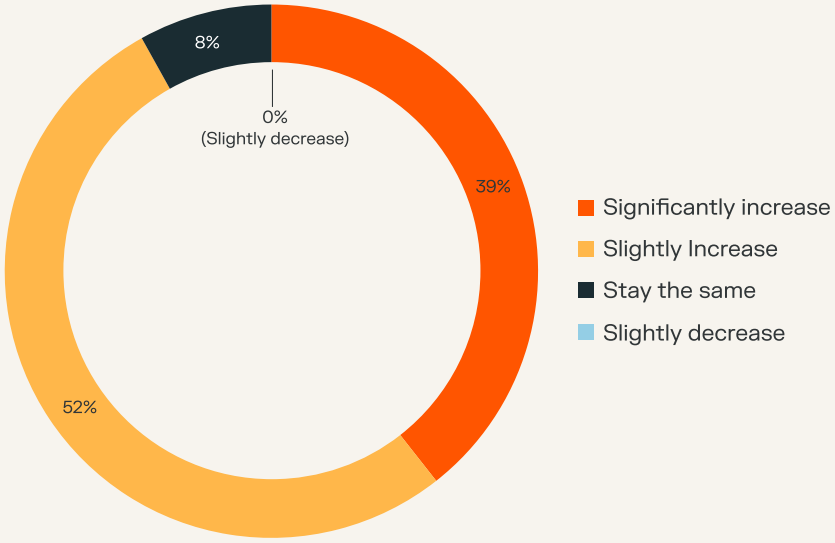
Here's a breakdown of individual survey questions and responses from 1,124 IT and cybersecurity leaders across seven global markets. Each question is accompanied by regional comparisons to provide additional context and insight.

Visibility and context challenges

How do you expect your organization's budget for cloud security to change over the next 12 months?

Most IT and cybersecurity leaders expect their organization's budget for cloud security to increase in the next 12 months (net increase: 91%). Specifically, 39% reported it will increase significantly while 52% expect a slight increase.

Significant increases are more likely in the U.S., Germany, and Brazil, while slight increases are expected in France and Australia. A higher proportion of leaders in Japan reported that budgets will remain the same.



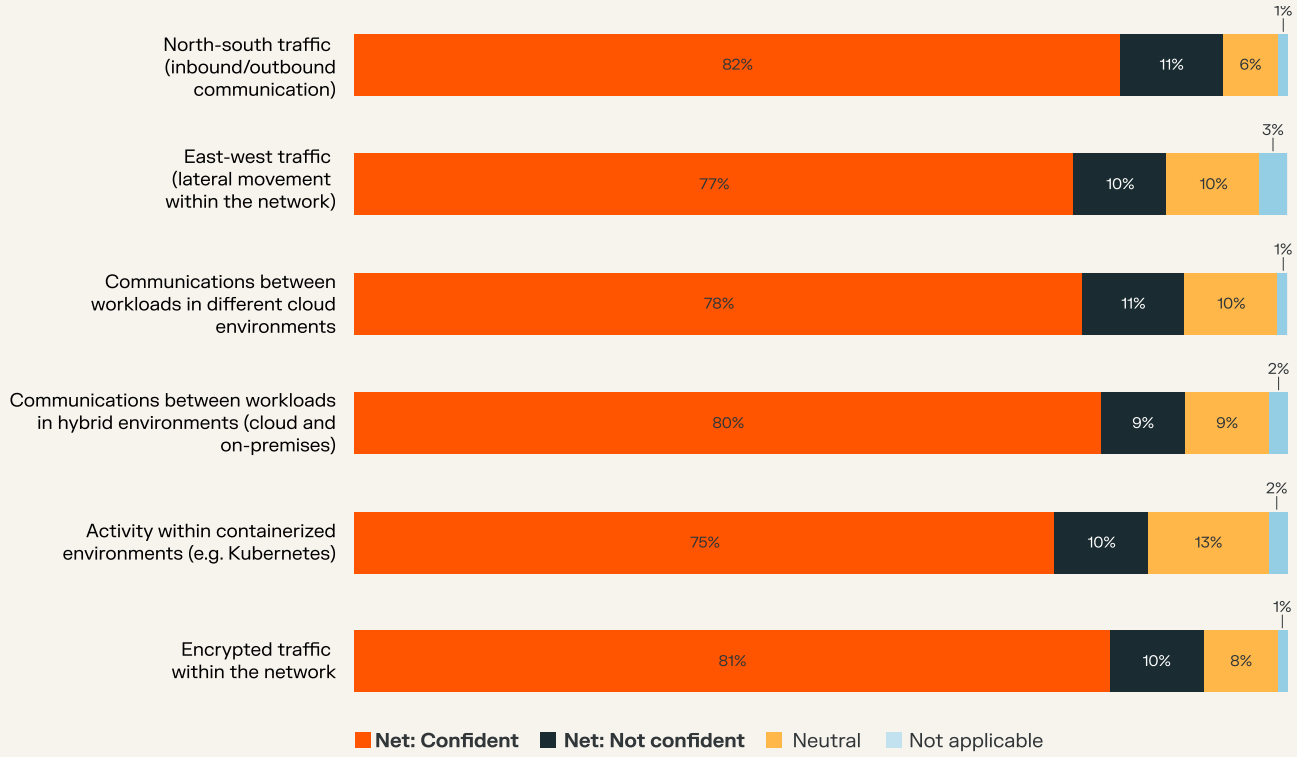
91%

of security leaders expect an increase in cloud security budgets in the next 12 months

Base: all respondents n=1,150

How confident are you in your organization's ability to observe and monitor the following types of network activity across both cloud and on-premises environments?

Overall, IT and cybersecurity leaders are more confident in their organization's ability to observe and monitor north-south traffic (inbound/outbound communication) (net confident: 82%), encrypted traffic within the network (net confident: 81%) and communications between workloads in hybrid environments (cloud and on-premises) (net confident: 80%).



Base: all respondents n=1,150

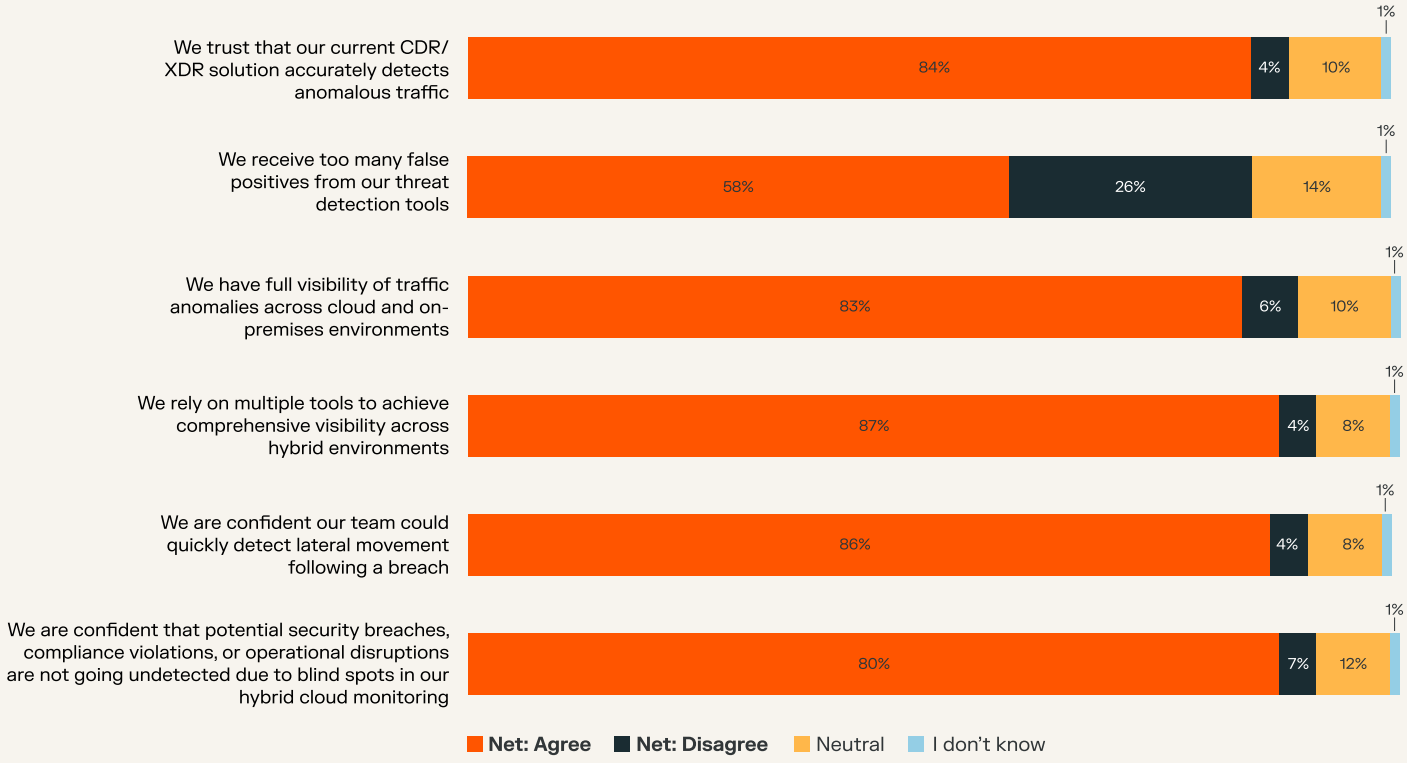
To what extent do you agree or disagree with the following statements?

IT and cybersecurity leaders are generally confident in their detection and response capabilities. Most respondents trust their current CDR/XDR solutions to accurately detect anomalous traffic (net agree: 84%) and feel they have full visibility of traffic anomalies across cloud and on-premises environments (net agree: 83%). There is also strong reliance on multiple tools to achieve comprehensive hybrid visibility (net agree: 87%) and high confidence in the team's ability to quickly detect lateral movement following a breach (net agree: 86%).

While 58% (net agree) of leaders report receiving too many false alerts, most remain confident that hybrid cloud monitoring effectively catches potential breaches and compliance or operational issues (net agree: 80%).

58%

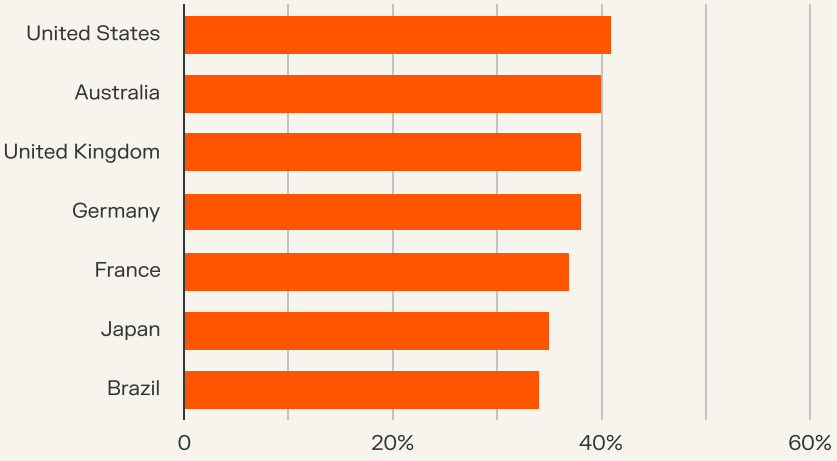
of security teams report receiving too many false alerts



Base: all respondents n=1,150

In your organization's customer-facing or production environments, what percentage of network traffic lacks sufficient context to enable confident investigation and response?

On average, IT and cybersecurity leaders reported that 38% of network traffic lacks sufficient context to support confident investigation and response. Among all markets, the U.S. and Australia reported the highest levels of insufficient context while Brazil and Japan reported the lowest.



38%

of network traffic lacks sufficient context to support confident investigation and response

Base: all respondents n=1,150

Which of the following has been the biggest challenge causing your organization to miss, delay, or struggle with detecting or responding to security incidents in the past 12 months?

Most IT and cybersecurity leaders (net: 93%) faced challenges in the past 12 months, especially in the U.S. and Australia (both scoring net: 97%). Most challenges were tool/technology related (net: 42%), especially in France (net: 53%), the U.S. (net: 48%), Australia (net: 46%) and the UK (net: 45%), or human/process-based (net: 39%). The top 3 challenges were:

- Insufficient resources (e.g., budget, personnel, expertise, training, etc.): 14%. This score increases to 25% in Japan.
- Difficulty correlating data across cloud and on-premises environments: 13%. This score increases to 25% in France.

93%

of IT and security leaders have faced challenges detecting or responding to security incidents in the past 12 months

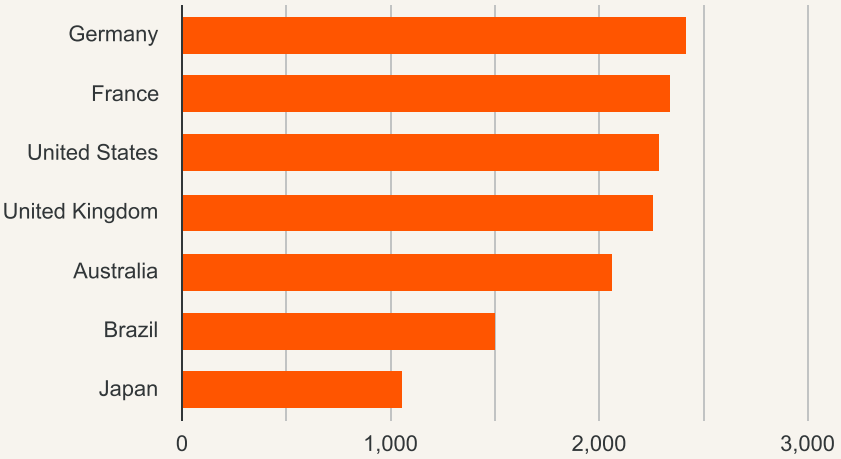


Base: all respondents n=1,150

Alert volume and prioritization

On a typical day, how many security alerts does your team receive from detection systems?

On average, IT and cybersecurity leaders reported that their team receives 2,020 alerts from detection systems on a typical day. Among all markets, Germany and France reported the highest average number of daily alerts, while Japan and Brazil reported the lowest.



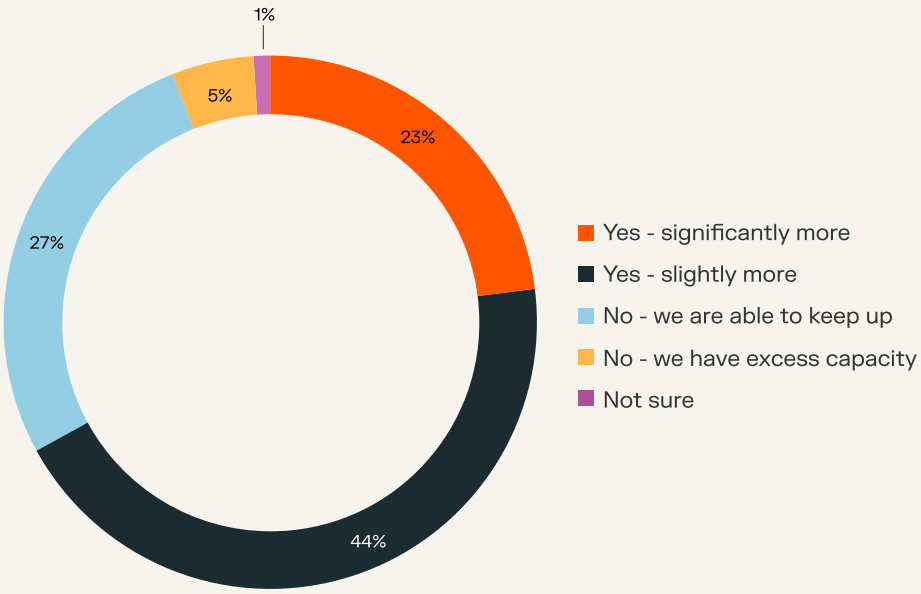
2,020

The average number of alerts security teams receive on a typical day

Base: all respondents n=1,150

Does your team currently receive more security alerts than it can effectively investigate?

Just over two-thirds of IT and cybersecurity leaders (net yes: 67%) reported that their team receive more security alerts than they can effectively investigate. The only markets below the global average are Brazil and Japan, with scores of 61% and 31%. Leaders in these two markets were more likely to report that they do not receive more alerts than they can investigate and that they are able to keep up.



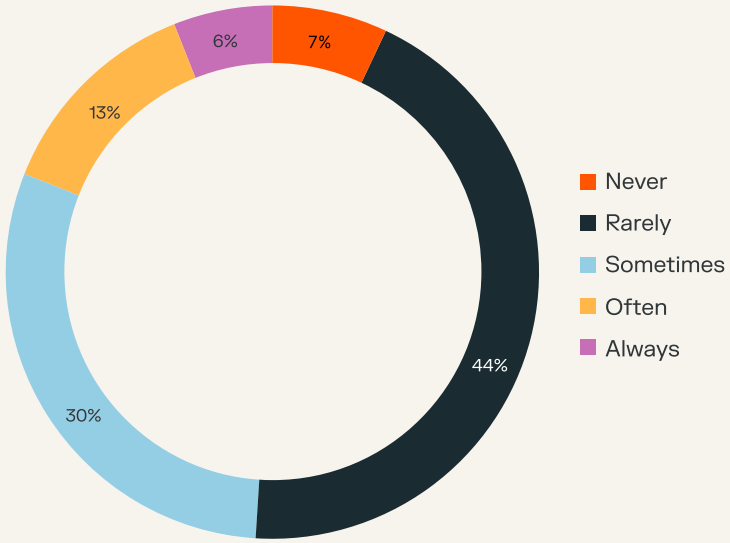
67%

of security teams receive more alerts than they can investigate

Base: all respondents n=1,150

How frequently do missed or uninvestigated alerts result in real security incidents in your organization (e.g., compromise, breach, or material risk)?

Most IT and cybersecurity leaders (net: 92%) reported that missed or uninvestigated alerts have, at some point, led to real security incidents within their organization. These incidents are most commonly reported as occurring sometimes (30%) or rarely (44%). The proportion reporting 'rarely' is higher in certain markets, rising to 47% in France, 51% in Japan, and 55% in Brazil.



92%

of IT and security leaders report that missed or uninvestigated alerts have led to real security incidents

Base: all respondents n=1,150

What is the biggest consequence your organization has experienced due to missed or uninvestigated alerts?

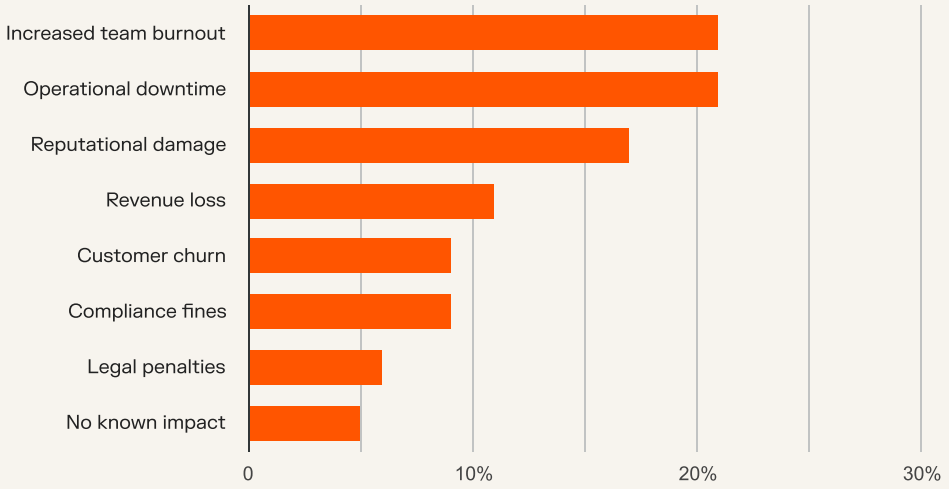
Among the IT and cybersecurity leaders who have experienced missed or uninvestigated alerts, 95% (net) said these incidents had a real impact on their organization, especially in France (net: 99%), Germany (net: 99%), the U.S. (net: 98%), and Australia (net: 98%).

The top three consequences reported were:

- Increased team burnout: 21%
- Operational downtime: 21%. This score increases to 28% in Brazil.
- Reputational damage: 17%. This score increases to 20% in the UK, 22% in France and 26% in Australia.

95%

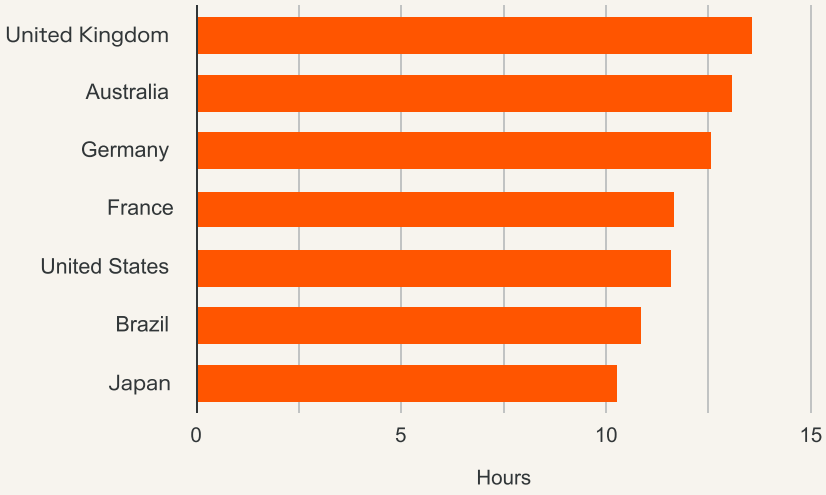
of security teams report that missed or uninvestigated alerts have a real impact on their organization



Base: all who have experienced missed or uninvestigated alerts or aren't sure n=1,068

When an alert is missed and leads to a security incident, how long does it typically take to detect the issue?

On average, it takes 12.1 hours to detect the issue. Detection times vary across markets, taking longer in the UK and Australia and less time in Japan and Brazil.



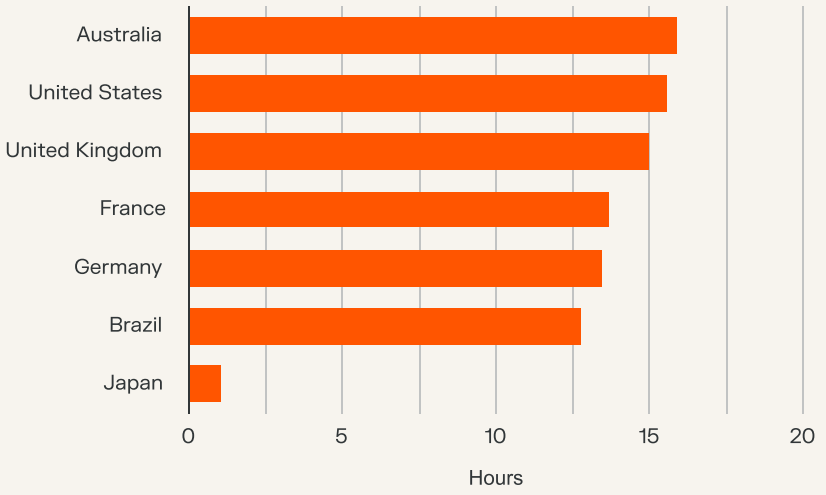
12 hours

The average time it takes to detect a security incident when teams miss an alert

Base: all who have experienced missed or uninvestigated alerts or aren't sure n=1,068

Approximately how many hours per week does your team collectively spend investigating security alerts that turn out to be false positives?

On average, teams spend 14.1 hours per week investigating security alerts that turn out to be false positives. Investigation times vary by market, with longer weekly efforts in the U.S., UK, and Australia, and shorter times in Japan and Brazil.



14 hours

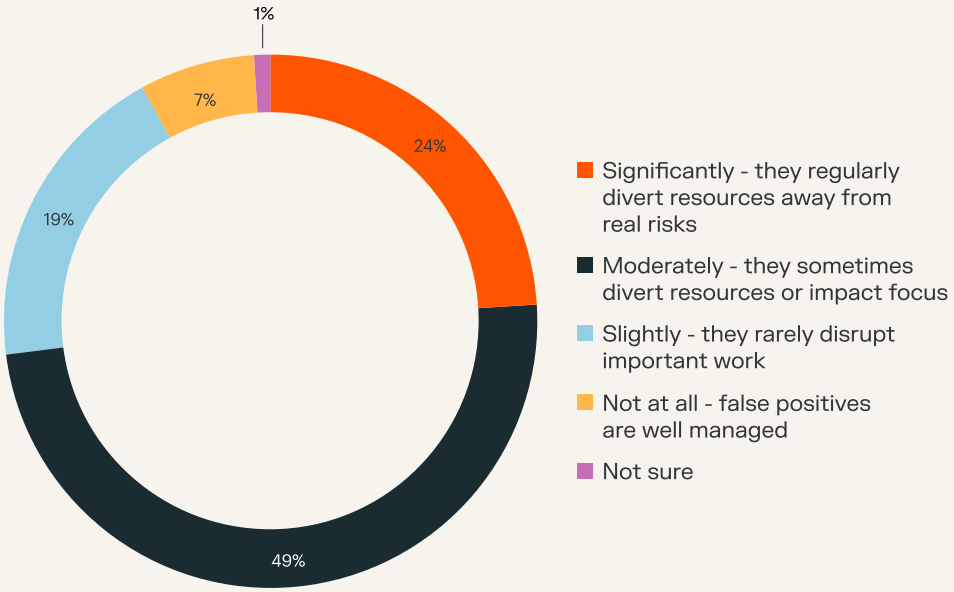
The average time security teams spend investigating alerts each week that turn out to be false positives

Base: all respondents n=1,150

To what extent do false positives impact your security team's ability to focus on real threats or other high-priority work?

Overall, net: 73% of IT and cybersecurity leaders reported that false positives either significantly (24%) or moderately (49%) hurt their security team's ability to focus on real threats or high-priority work, while 26% indicated they are only slightly (19%) or not at all disruptive (7%). Only 1% were unsure.

False positives affect organizations across all markets, although cause less disruption in Brazil and Japan. All market-specific differences are outlined in the following sections:



73%

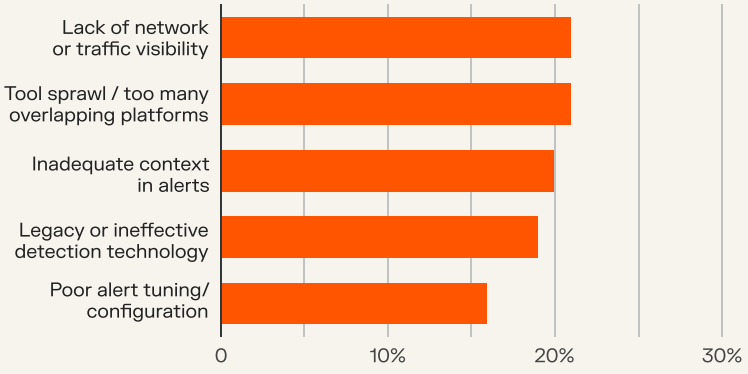
of security leaders agreed that false positives impact their team's ability to focus on real threats or high-priority work

Base: all respondents n=1,150

What is the primary cause of false positives in your environment?

The primary causes of false positives are:

- Lack of network or traffic visibility: 21%. We see the highest score in Germany (28%).
- Tool sprawl / too many overlapping platforms: 21%. We see the highest score in Brazil (27%).
- Inadequate context in alerts: 20%. We see the highest scores in France and the UK (both scoring 24%).
- Legacy or ineffective detection technology: 19%. We see the highest score in France (27%).

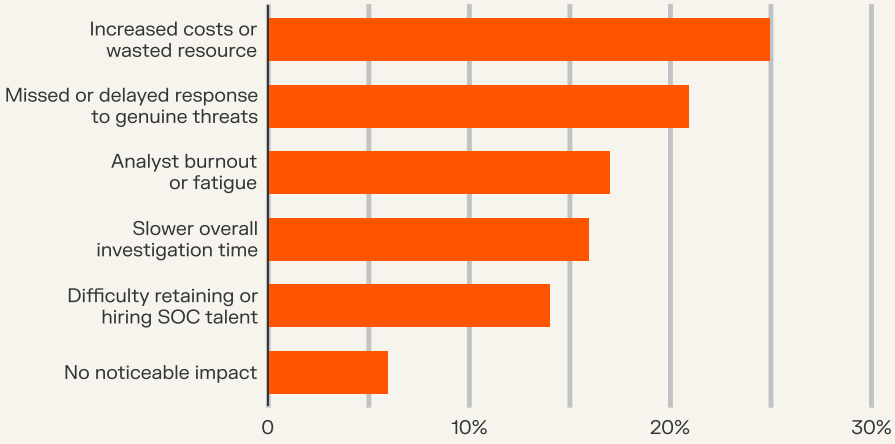


Base: all respondents n=1,150

Which of the following has been the biggest impact your organization has experienced due to the volume of false positives?

The biggest impacts due to the volume of false positives are:

- Increased costs or wasted resource: 25%
- Missed or delayed response to genuine threats: 21%. We see the highest score in Germany (30%).



Base: all respondents n=1,150

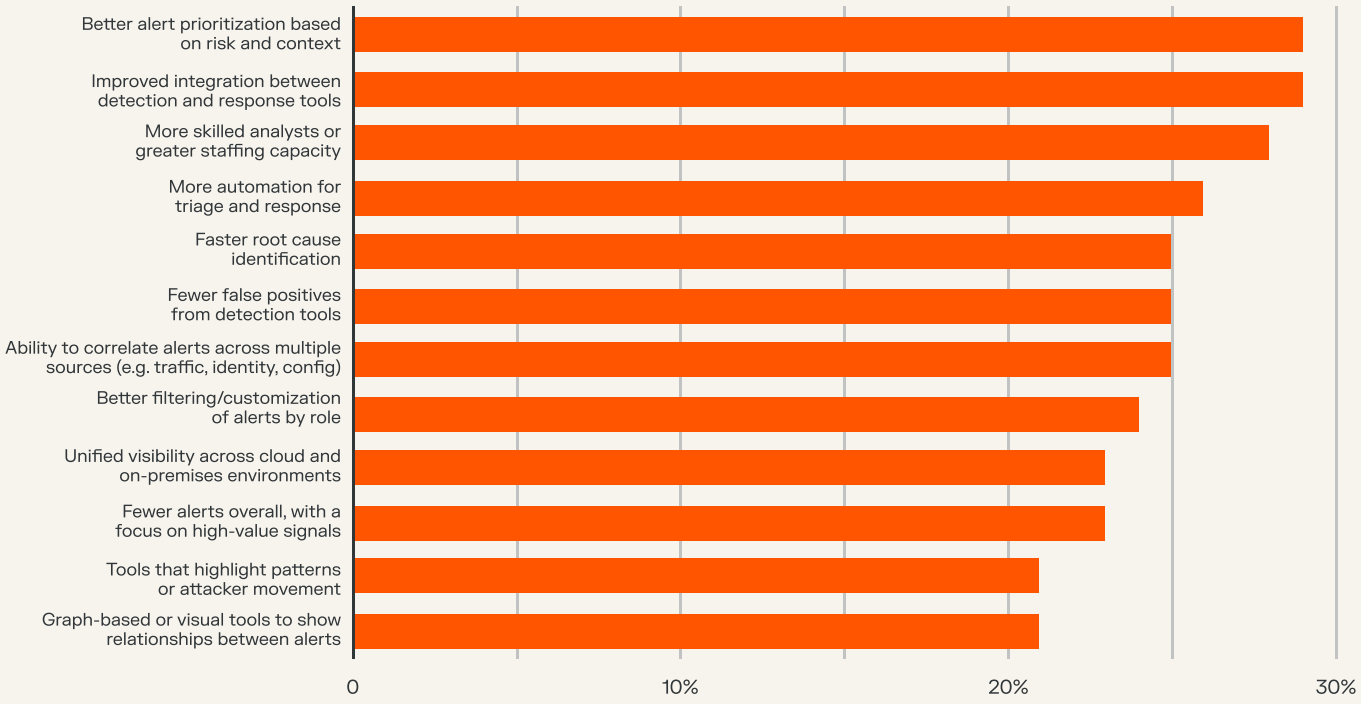
Which of the following would most reduce alert fatigue in your security operations?

The top answers that were more likely ranked in the top 3 are:

- Better alert prioritization based on risk and context: 29%
- Improved integration between detection and response tools: 29%
- More skilled analysts or greater staffing capacity: 28%

29%

of security leaders believe better alert prioritization would reduce their team's alert fatigue

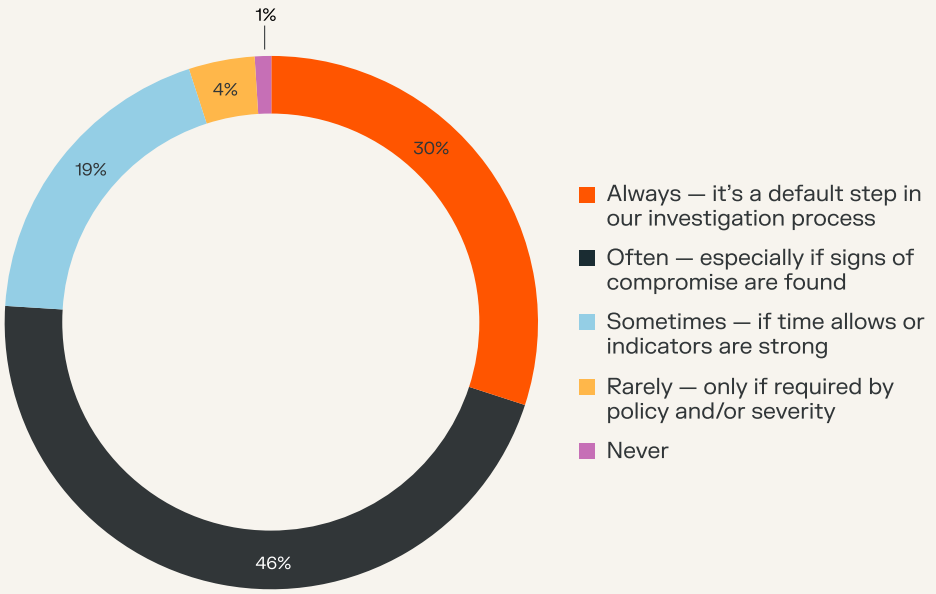


Base: all respondents n=1,150

Lateral movement risk

How often does your team investigate potential lateral movement during an incident or alert review?

Most IT and cybersecurity leaders (net: 95%) reported that their teams investigate potential lateral movement during an incident or alert review: 30% always, 46% often, and 19% sometimes. However, leaders in Japan and Australia are less likely than those in other markets to report doing so always or often.



95%

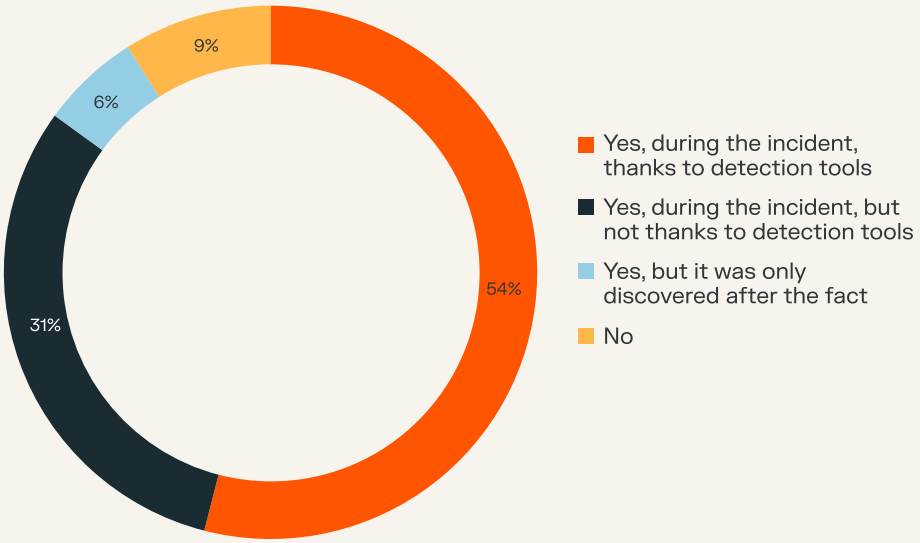
of security teams investigate potential lateral movement during an incident or alert review

Base: all respondents n=1,150

Has your organization detected a security incident involving lateral movement in the past 12 months?

Most IT and cybersecurity leaders (net: 90%) reported having detected a security incident involving lateral movement within the past 12 months. Among them, 54% said the detection occurred during the incident thanks to detection tools, 31% detected it during the incident but not due to such tools, and 6% only identified it after the fact.

Respondents in the U.S., UK, Brazil and Australia were more likely to attribute detection to their tools, whereas a higher number of leaders in France and Germany reported that detection was not tool-driven. Notably, 1 in 5 Japanese leaders (20%) said that they had not detected any incidents involving lateral movement in the past 12 months which is the highest score across all markets.



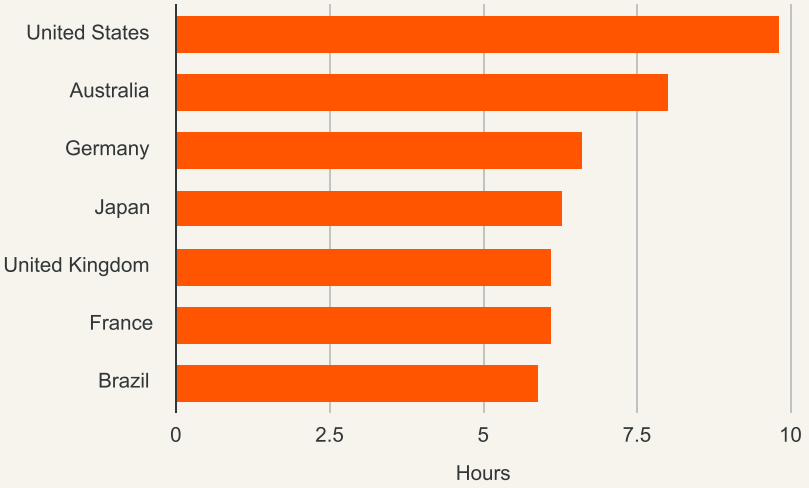
Base: all respondents n=1,150

90%

of security teams detected a security incident involving lateral movement in the last year

How much operational downtime did your organization experience as a result of this incident?

On average, organizations reported 7.1 hours of downtime following a security incident involving lateral movement. U.S. and Australian organizations experienced the longest downtime, while Brazil reported the shortest.



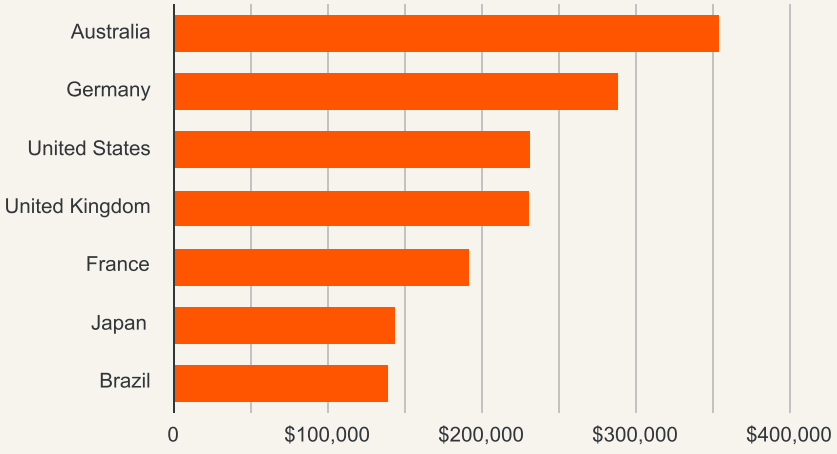
7 hours

The average downtime following a security incident involving lateral movement

Base: all who detected a security incident involving lateral movement in the last year (during the incident) n=972

What was the estimated cost of this downtime?

On average, downtime linked to a security incident involving lateral movement was estimated to cost organizations $227,264.20. Costs were highest in Australia and Germany, while Japan and Brazil reported the lowest averages.



$227,264

The average cost of downtime from security incidents involving lateral movement.

Base: all who detected a security incident involving lateral movement in the last year (during the incident) n=972

Where does your organization face the biggest operational challenges when it comes to detecting lateral movement?

When asked about the biggest operational challenges in detecting lateral movement, IT and cybersecurity leaders most often mentioned alert fatigue and lack of actionable insight. The top challenges ranked in the top three were:

- Too many alerts leading to alert fatigue (low signal-to-noise ratio): 37%. We see the highest scores in France (41%) and Brazil (49%).
- We can see connections but lack context or actionable insight: 34%.
- Limited visibility into east-west traffic: 31%. We see the highest score in Australia (45%).
- Can't correlate behaviors across cloud and on-premises: 31%.
- Unsure how to interpret the data to spot lateral movement: 31%. We see the highest score in Germany (39%).



Base: all respondents n=1,150

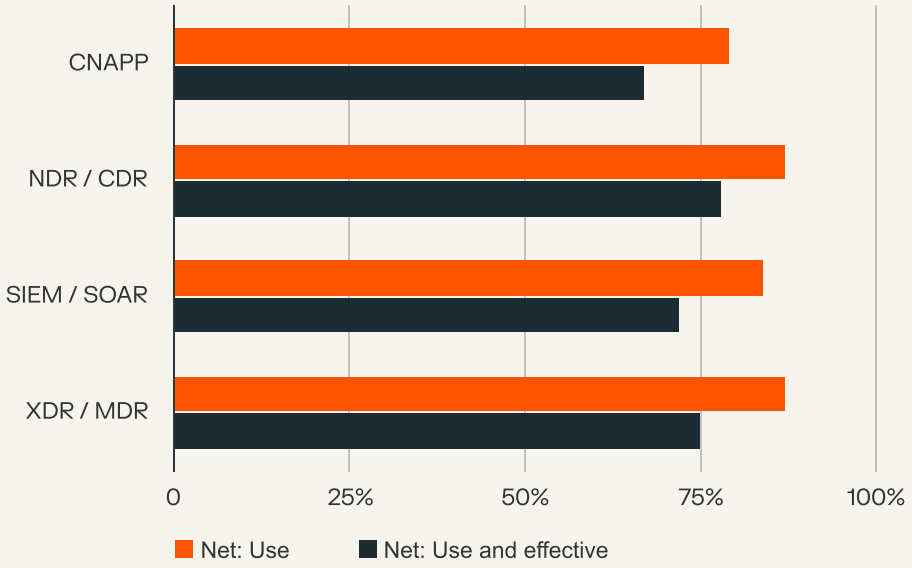
Tooling limitations

Which of the following cloud detection and response tools does your organization currently use, and how would you rate their effectiveness?

Most organizations use a range of cloud detection and response tools, with usage rates between 79% and 87% across all tools: CNAPP (net use: 79%), NDR/CDR (net use: 87%), SIEM/SOAR (net use: 84%), XDR/MDR (net use: 87%) and homegrown tools (net use: 82%).

Overall, while adoption is high, perceived effectiveness varies, with most tools rated somewhat or very effective by the majority of users:

- **Net: Use and effective:** 67% – 78% across all tools, with NDR/CDR highest at 78%
- **Used and very effective:** 28% – 38% across all tools, with XDR/MDR highest at 38%
- **Used and somewhat effective:** 37% – 41% across all tools, with NDR/CDR highest at 41%
- **Used and not effective:** 10% – 12% across all tools

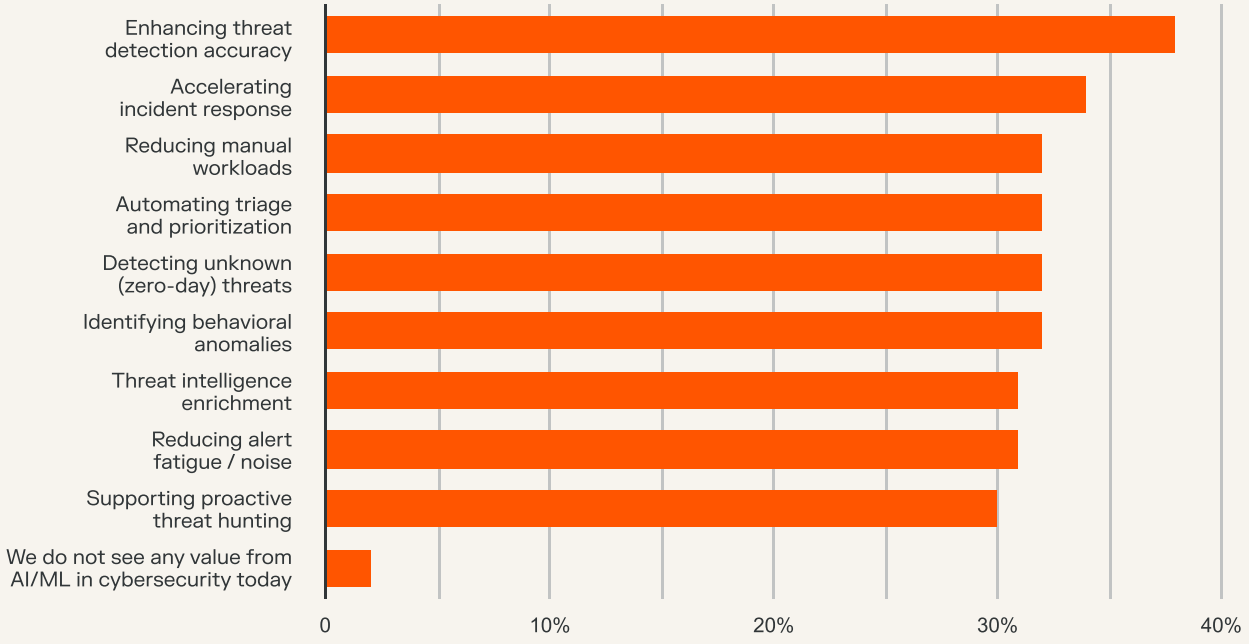


Base: all respondents n=1,150

CNAPP - cloud-native application protection platform
NDR - network detection and response
CDR - cloud detection and response
SIEM - security information and event management
SOAR - security orchestration, automation, and response
XDR - extended detection and response
MDR - managed detection and response

Where does your organization see the greatest value from AI/ML in cybersecurity today?

Organizations see the greatest value of AI/ML in cybersecurity in improving detection and efficiency.



Base: all respondents n=1,150

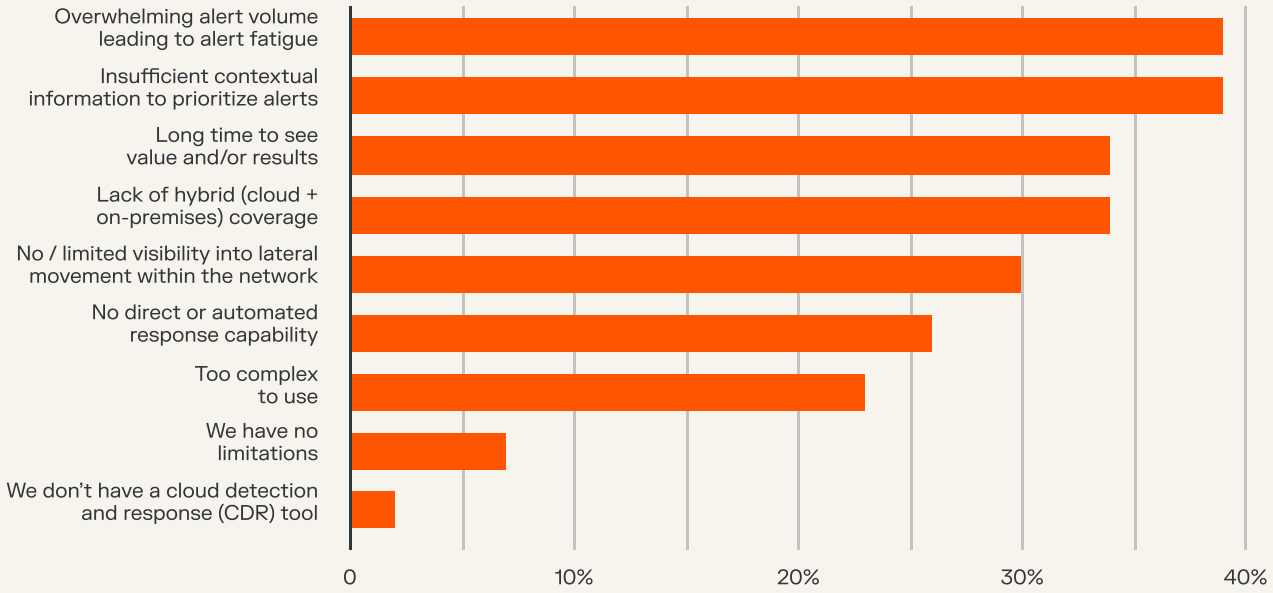
What are the biggest limitations you experience with your current cloud detection and response (CDR) capabilities in the cloud?

Nearly all organizations (net: 92%) reported experiencing limitations with their current cloud detection and response (CDR) capabilities, rising to net: 97% in Australia. The most commonly cited challenges were:

- Overwhelming alert volume leading to alert fatigue: 39%
- Insufficient contextual information to prioritize alerts: 39%

92%

of organizations report experiencing limitations with their current cloud detection and response capabilities

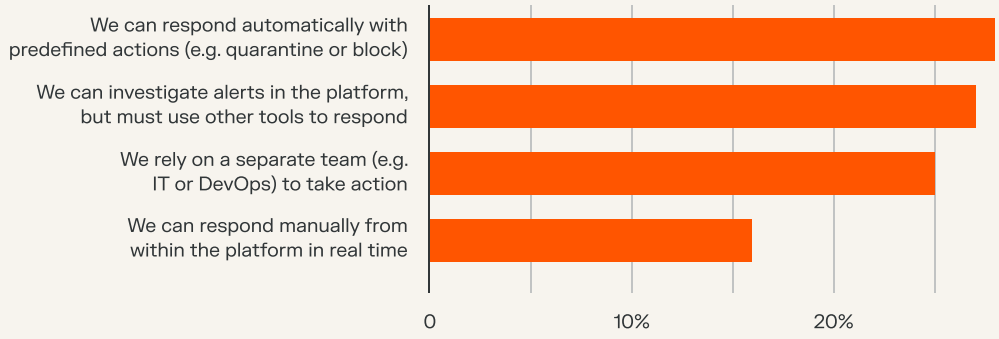


Base: all respondents n=1,150

How is your organization currently able to respond to alerts in the cloud using your detection and response tools?

When asked how their organizations are currently able to respond to alerts in the cloud using detection and response tools, IT and cybersecurity leaders reported a mix of automated, manual, and team-based approaches.

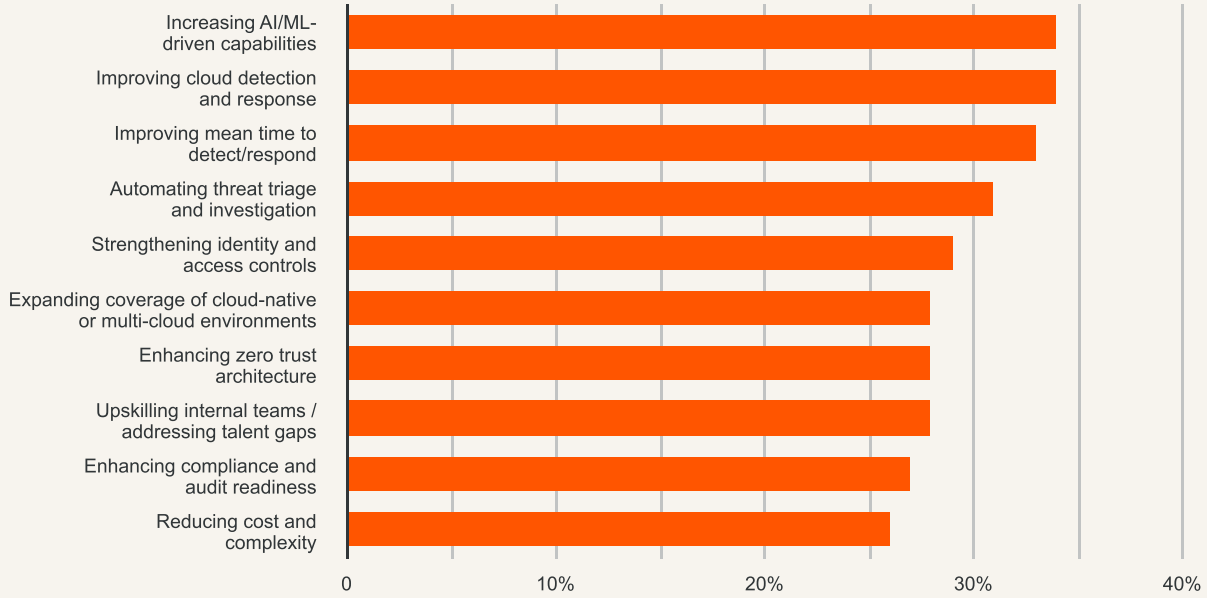
- We can respond automatically with predefined actions (e.g., quarantine or block): 28%
- We can investigate alerts in the platform, but must use other tools to respond: 27%
- We rely on a separate team (e.g., IT or DevOps) to take action: 25%. This score increases to 36% in the UK.
- We can respond manually from within the platform in real time: 18%



Base: all respondents n=1,150

What are your top security priorities for 2026?

Looking ahead to 2026, IT and cybersecurity leaders identified a range of strategic priorities, particularly around enhancing detection and response capabilities, leveraging AI/ML, and automating threat management.



Base: all respondents n=1,150

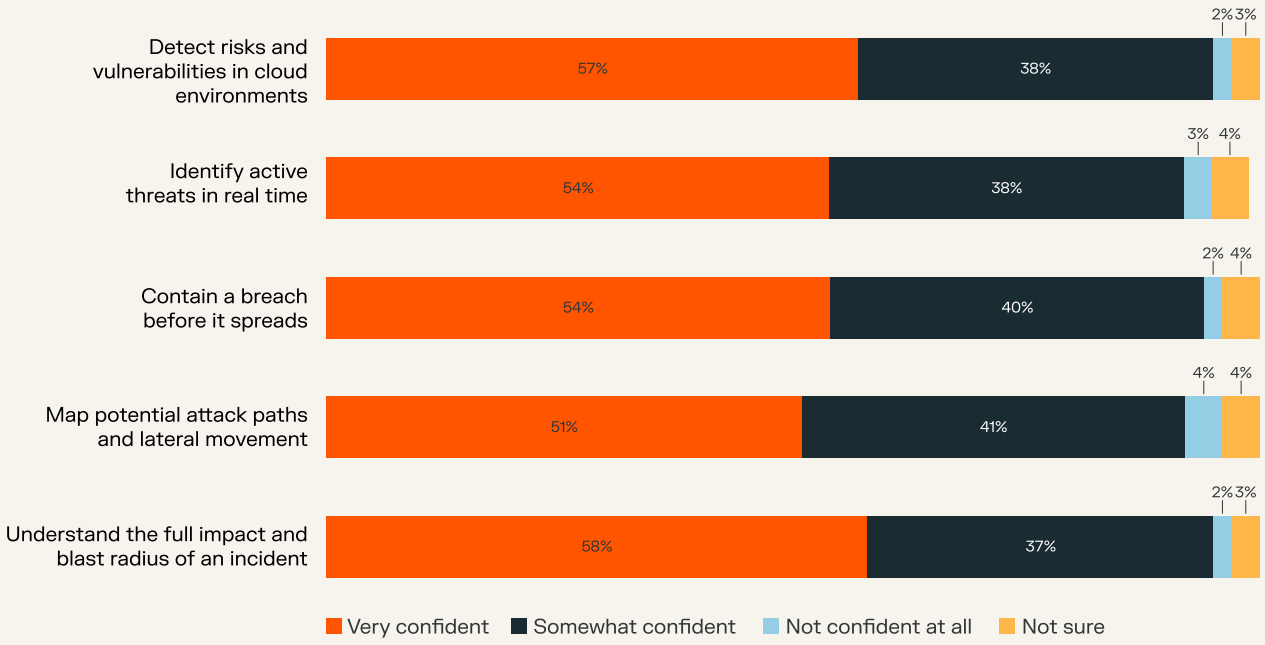
Security confidence and risk reduction

How confident are you in your organization's ability to detect and contain cloud-based threats?

Organizations report confidence in their ability to detect and contain cloud-based threats:

- **Net: confident:** 92% – 95% across all areas
- **Very confident:** 51% – 58% across all areas
- **Somewhat confident:** 37% – 41% across all areas
- Only a small minority are not confident at all (2% – 4%) or unsure (3% – 4%).

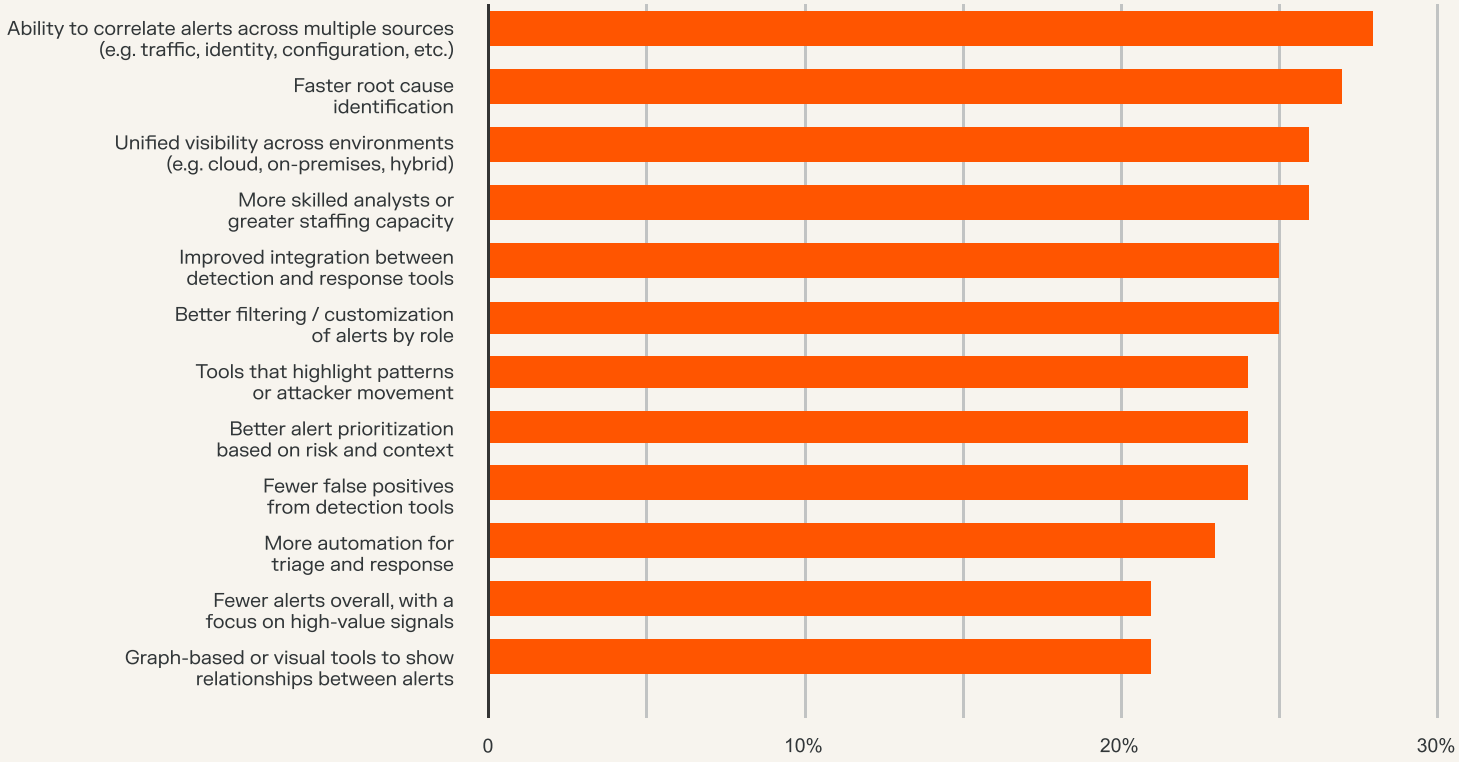
Organizations feel most confident in their ability to understand the full impact of an incident (very confident: 58%) and to detect risks and vulnerabilities in cloud environments (very confident: 57%).



Base: all respondents n=1,150

What would most improve your organization's ability to detect, investigate, and respond to cyber threats before they cause harm to your cloud environments?

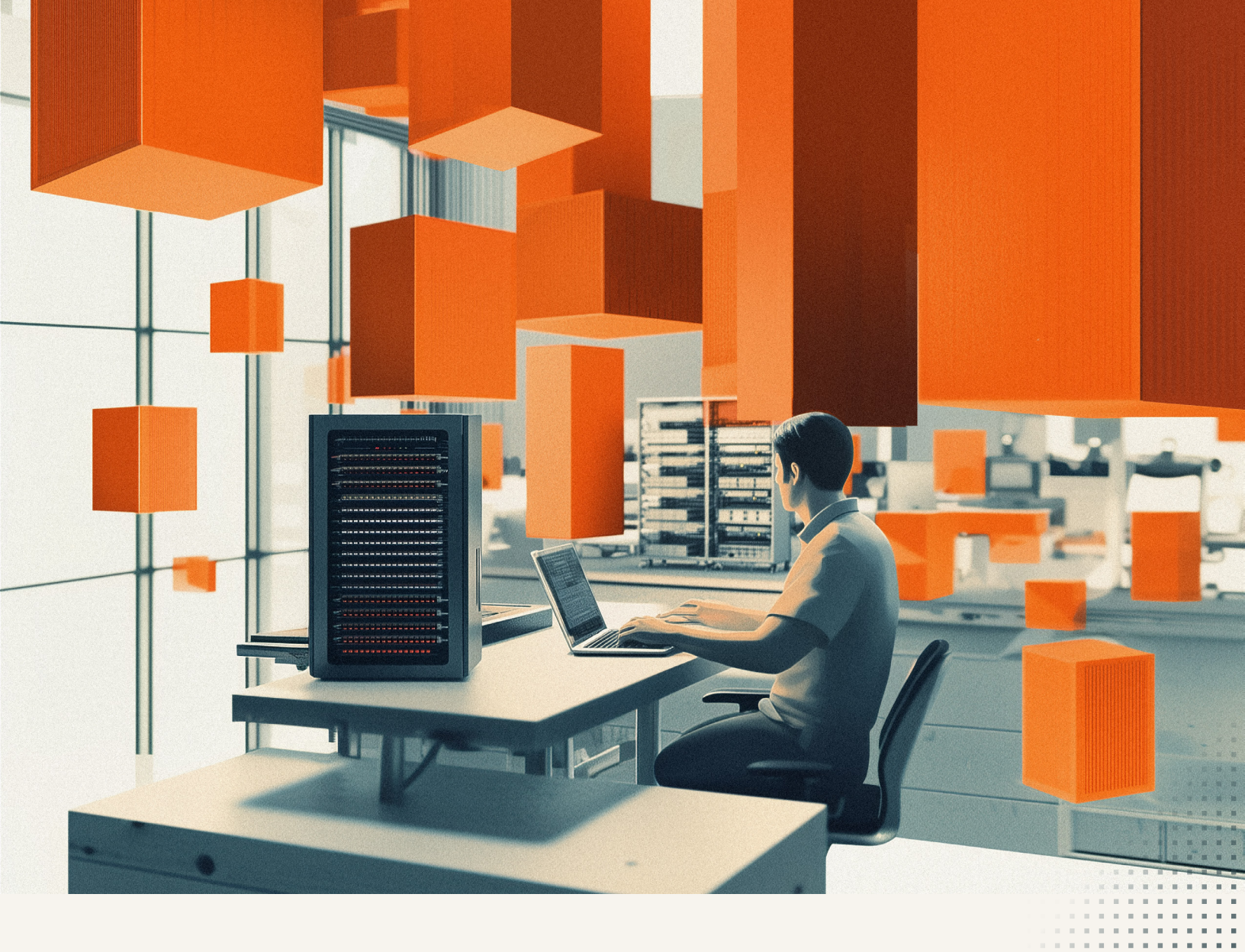
IT and cybersecurity leaders identified several key areas that would most improve their ability to detect, investigate, and respond to cloud-based cyber threats.



Base: all respondents n=1,150

PART 4

Conclusion



The data is clear: prevention alone is no longer enough.

Security teams are overwhelmed by noise. Too many tools, too few analysts, and not enough context are making it nearly impossible to focus on what matters most.

False positives consume hours of precious time each week. Missed alerts are leading to real-world consequences, from reputational damage to operational downtime. Lateral movement continues to fly under the radar, draining confidence and compounding risk.

That's why many security teams are looking beyond traditional detection tools. The data in this study shows they're tired of being buried in isolated alerts and are seeking observability that connects the dots across hybrid environments, delivers clearer signals, and highlights what truly matters.

Leaders want to turn raw alerts into context and action — to not just see more but understand more. They're looking for faster, more automated responses that cut through noise and help contain threats before they spread.

In short, the findings highlight clear priorities:

- Reduce false positives that waste time and resources
- Close context gaps that slow investigations
- Accelerate response to contain threats before they escalate

Now is the time to modernize detection and response and gain the observability and insight security teams need to prepare for whatever comes next.

APPENDIX

Methodology and participant profile

Methodology

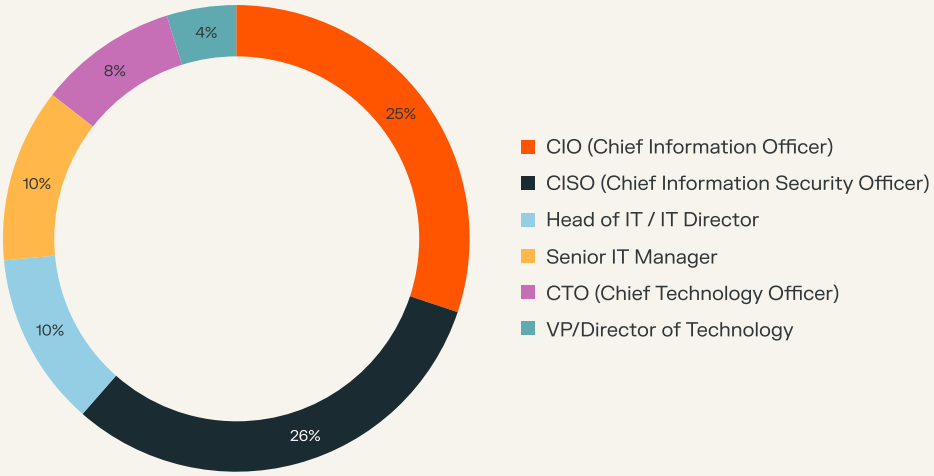
Vitreous World adopted an online methodology and recruited IT and cybersecurity decision-makers and key influencers. Interviews were conducted in the U.S., UK, France, Germany, Brazil, Japan and Australia.

All respondents were guaranteed to remain anonymous as part of the study. Fieldwork was carried out between August 1–13, 2025.

Participant profile

Total	U.S.	UK	FR	DE	BR	JP	OZ
N=1150	N=200	N=200	N=150	N=150	N=150	N=150	N=150
100%	**17%**	**17%**	**13%**	**13%**	**13%**	**13%**	**13%**

Job titles



1,150
respondents in total

15%
work for companies with between 51 and 250 employees

85%
work for companies with 251+ employees

76%
Senior management
(C-suite or C-level)

22%
Middle management
(vice president, director, department head, or senior manager)

3%
Senior non-managerial
(e.g., technical expert or subject matter expert)

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by the Illumio AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

illumio

Copyright © 2025 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.