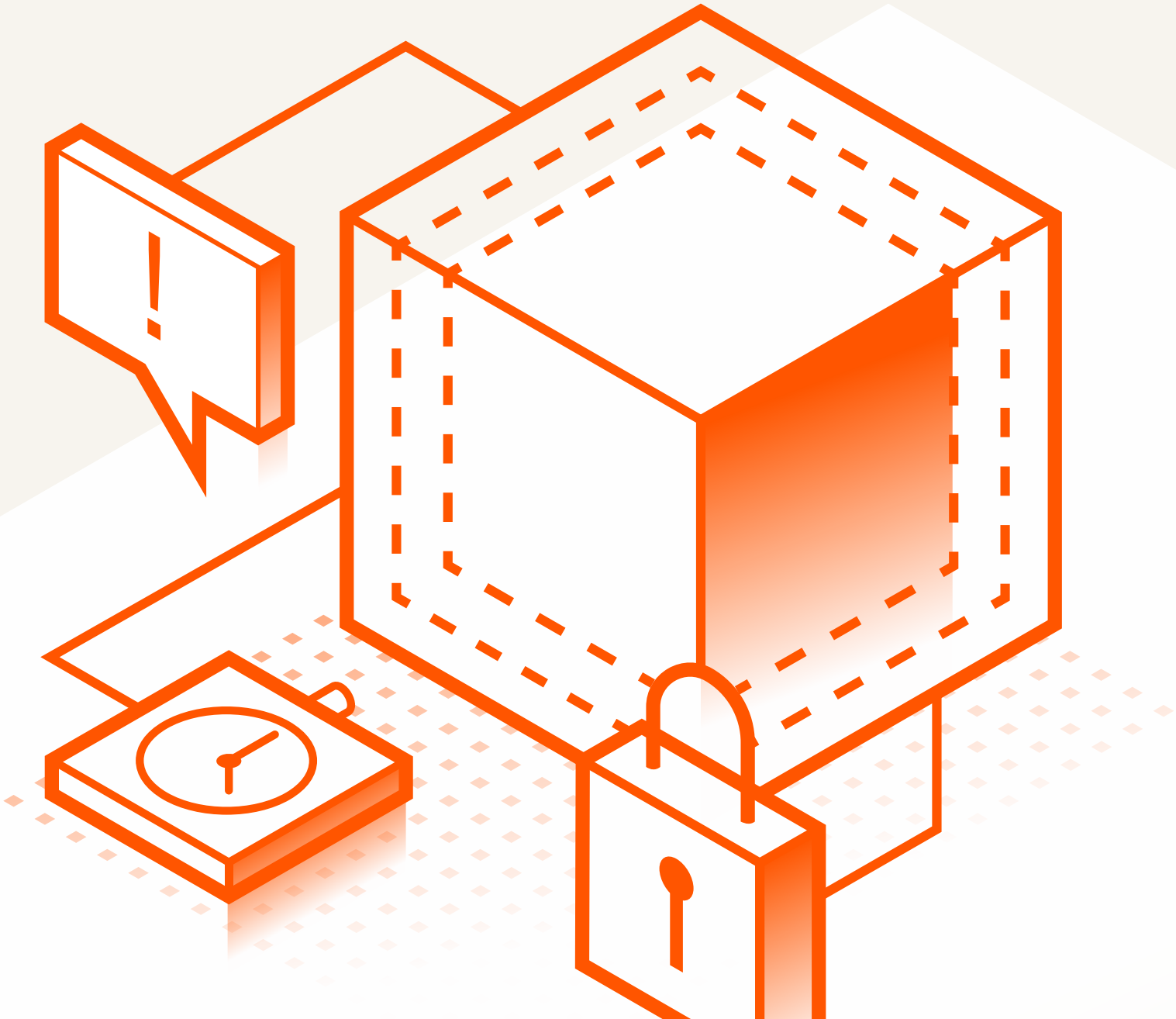
illumio | CYBEREDGE GROUP®

# The Containment Gap

## Exploring the Distance Between Detection and Resilience



# Contents

PART 1

# Introduction: confidence without containment

Something's rotten in the state of cybersecurity.

According to our latest research, 95% of IT and security professionals are confident they can detect unauthorized lateral movement. On paper, the modern security stack is working: visibility is high, tools are deployed, and teams feel prepared.

But the gap between feeling prepared and actually being protected is wide — and growing.

Despite this high confidence, nearly half (46%) of organizations admit they still struggle to stop attackers from moving once they are inside. While 87% believe they can contain an attack quickly, only 17% can actually isolate a compromised asset in near real-time.

The minutes or hours between "we see them" and "we've stopped them" are where the most significant damage occurs. The industry has spent decades perfecting the "deadbolt and burglar alarm" approach to security, investing billions into faster detection and thicker perimeters.

But the data in this report suggests an uncomfortable truth: the traditional cybersecurity model is broken.

To better understand this challenge, Illumio asked independent research firm CyberEdge to survey 700 cybersecurity and IT leaders across seven countries and 17 industries.

This report explores what we call the "containment gap" — the distance between seeing a threat and actually stopping it. To fix what is broken, we must move beyond the illusion of the perimeter and start building for resilience.

PART 2

# Summary of key findings

Breaches *will* happen. The real question is how well organizations respond once they do.

The data shows confidence is high. Many teams believe they can see threats and identify attacks quickly.

But performance is less consistent when it comes to containment. Complexity, fast-moving threats, and lateral movement still challenge even mature security programs.

This section reviews the key findings from the research. It explains what is working, where gaps remain, and why breach containment now plays a central role in modern cyber resilience.

# Cyber risk is broad and growing

Concern about cyber threats is nearly universal. Almost all respondents (98%) worry about at least one type of threat. This shows that cyber risk is now part of daily business operations.

## One provider, thousands impacted: analyzing the Kaseya incident

During the July Fourth U.S. holiday weekend in 2021, the REvil ransomware gang executed one of the most sophisticated supply-chain attacks in history. It exploited zero-day vulnerabilities in remote monitoring software from IT services firm Kaseya.

By breaching one company, attackers turned a trusted management tool into a weapon for mass distribution.

### Anatomy of the attack

- **The breach vector:** Attackers used an authentication bypass (CVE-2021-30116) to gain privileged access to on-premises VSA servers.
- **The amplification:** Because the VSA software was designed to manage and update thousands of endpoints with high-level administrative rights, the attackers were able to push a malicious hotfix disguised as a legitimate update directly to downstream customers.
- **The fallout:** Only about 60 direct Kaseya customers were initially breached. But the poisoned well effect caused follow-on attacks at 1,500 downstream businesses across 17 countries.
- **Real-world consequences:** In Sweden, the supermarket chain Coop was forced to close nearly all of its 800 stores for almost a week because its point-of-sale systems were encrypted. In New Zealand, 11 schools and over 100 nurseries saw their operations grind to a halt.

### Lessons for 2026

The Kaseya attack proved that even if an organization's own perimeter is secure, a single compromised upstream partner with broad access rights can bypass every local detection tool.

Without microsegmentation to limit the reach of administrative tools and service providers, a single breach in the supply chain becomes an instant, uncontainable crisis for everyone connected to it.

The range of threats is also notable. Traditional risks such as data or intellectual property theft (57%) and ransomware or extortion (53%) remain top concerns. At the same time, worry about AI-based threats, including deepfake impersonation (55%), is just as high. This shift highlights how quickly the threat landscape is changing.

Concern about cyber threats also varies by region. Ransomware worries are highest in Japan (73%) but much lower in Brazil (28%). Concern about data and intellectual property theft is higher in the United States (66%) and Brazil (68%) than in other regions. These trends suggest that local experience shapes how organizations view risk.

Overall, the data shows that organizations face multiple risks at the same time. Modern breaches rarely involve a single threat. Once attackers gain access, the damage can spread quickly if it's not contained.

# Most breaches begin with known weaknesses and complexity

When asked what creates the most cybersecurity exposure, respondents point to weaknesses in basic security practices and growing operational complexity.

The top risk is IT vulnerabilities (66%). Close behind is employee error, carelessness, or misconduct (50%). This reinforces the fact that many breaches begin with known gaps that could have been addressed.

Complex environments, including operational technology that supports critical infrastructure, add to the risk. Half of respondents (50%) say a lack of integration between IT and OT systems increases exposure. Securing a mix of legacy systems, operational technology, and modern cloud infrastructure is difficult and often inconsistent.

Credential theft and privilege escalation are also major concerns (45%). These tactics allow attackers to take advantage of internal trust when they gain access. Once inside, they can impersonate legitimate users, elevate privileges, and move deeper into systems.

Overall, exposure rarely stems from one single failure. It grows from a combination of technical weaknesses, human mistakes, and disconnected systems.

These systemic gaps make it easier for attackers to move laterally after they enter the organization.

# Visibility exists, but context around it is inconsistent

Many organizations report strong visibility across their environments.

On average, confidence in seeing traffic paths rates about 4 out of 5, with 5 being highest. Visibility is highest in data center environments (4.12) and in communication between endpoints and the cloud or data center (4.09).

This high confidence at the management level (this survey's sample population) may not fully reflect the operational reality on the ground. While leadership sees strong coverage in reporting tools, the data reveals a recurring context gap when environments overlap.

Scores are lower for cloud-to-cloud traffic (3.94) and cloud-to-data center communication (3.97). A likely reason: these areas change more often and are harder to manage. Dependencies shift, and controls aren't always applied in a consistent way.

This pattern is the same across regions and industries. Many organizations can see activity within a single environment, but fewer have clear visibility across all environments.

During a security incident, this gap becomes critical. Teams may detect unusual behavior, yet they struggle to understand how systems are linked and where an attacker might move next.

# Detection confidence is high, yet containment remains uneven

Confidence in detection is very high. Nearly all respondents (95%) say they believe they can detect unauthorized lateral movement before it reaches critical assets. Almost half (47%) say they're very confident.

However, confidence is lower in some areas. In manufacturing, 8% say they aren't confident that they can detect lateral movement. In retail, that number rises to 9%. In Japan, a significant 23% report a lack of confidence.

## When detection confidence fails to stop persistence

In late 2024 and throughout 2025, a China-linked threat actor known as Salt Typhoon executed a sprawling espionage campaign that shook the telecommunications industry to its core.

While many organizations say they're confident they can detect threats, Salt Typhoon proved that detection doesn't equal containment.

### Anatomy of the attack

- **The targets:** the group compromised at least nine major U.S. carriers, including Verizon, AT&T, T-Mobile, and Lumen. Beyond the U.S., it infiltrated over 200 organizations across 80 countries.
- **The breach of trust:** Most alarming, the attackers gained access to lawful intercept systems (CALEA), the backdoors law enforcement uses for court-authorized wiretapping. They essentially turned the U.S. government's own surveillance tools against its citizens.
- **High-profile surveillance:** The hackers monitored the call logs and unencrypted texts of more than one million users, specifically targeting the phones of presidential candidates and senior Washington officials to map out political networks and movements.
- **The persistence paradox:** Despite company assurances of containment by late 2024, DHS and FBI reports in 2025 indicated that the attackers likely remained active in these complex networks for over a year. They used living-off-the-land (LotL) techniques — abusing legitimate administrative tools and unpatched edge routers — to blend in with normal traffic.

### Lessons for 2026

Salt Typhoon didn't use exotic zero-day exploits; it used lateral movement and credential theft. By the time it was detected, the group had already moved from the perimeter into the core network backbone.

This case proves that detection is a lag indicator. Without microsegmentation to block lateral paths by default, an attacker can live inside what you think is a secure environment for months before the first alarm ever sounds.

While most teams trust their ability to detect threats, confidence drops when it comes to containing breaches. Nearly half of respondents (46%) say their organization struggles to stop unauthorized lateral movement.

Response speed highlights this gap. Only 49% of organizations report isolating compromised assets in near real time or within minutes; a full 51% require hours, days, or more.

Overall, the data shows that many organizations can detect attacks, but they still face challenges stopping them fast enough to prevent further spread and the resulting damage.

# Microsegmentation is mainstream, but not all approaches are equal

Microsegmentation is now widely adopted; 93% of respondents use at least one microsegmentation approach. But our data reveals a significant definition gap. While the intent to segment is nearly universal, not all methods achieve the same level of resilience.

For example, 68% of respondents still use network-based firewalls for microsegmentation. These hardware-based controls often struggle to scale in multi-cloud environments where IP addresses change constantly. And they often create disconnected islands of security rather than the consistent, granular containment needed to stop lateral movement.

To close the containment gap, 62% of organizations are moving toward modern software solutions. Modern microsegmentation is workload-based, granular, and decoupled from the underlying network. That means security policies can follow the workload wherever it goes — on-premises, in the cloud, or at the edge.

Organizations see clear value in these efforts. Many report faster detection and response (50%), stronger breach containment (47%), and better visibility into traffic and system dependencies (45%).

The main challenges are practical. Cost is the top concern (41%). Limited visibility into application dependencies (40%) and integration issues (39%) also rank high. Some teams worry about unclear ownership of the project (37%) and operational disruption (36%).

Buying priorities reflect these concerns. Respondents say they want consistent policy enforcement across hybrid environments (51%), real-time visibility (50%), and solutions that are fast and simple to deploy (49%).

PART 3

# Question-by-question analysis

Now that we've examined the key themes from the research, this section takes a closer look at the data.

Here, we break down each survey question and response from 700 cybersecurity and IT leaders across seven countries and more than 17 industries, including relevant regional and industry comparisons.

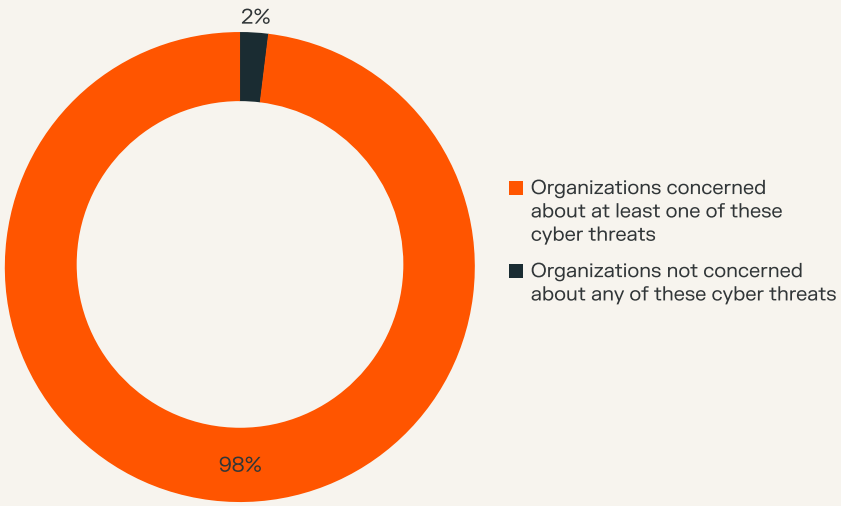
## Which cyber threats are most concerning to your organization? (Select up to three.)

Concern about cyber threats is nearly universal. A total of 98% of organizations report concern about at least one type of threat.

When asked to list their top three concerns, respondents most often cited data loss (57%) and operational disruption (56%).

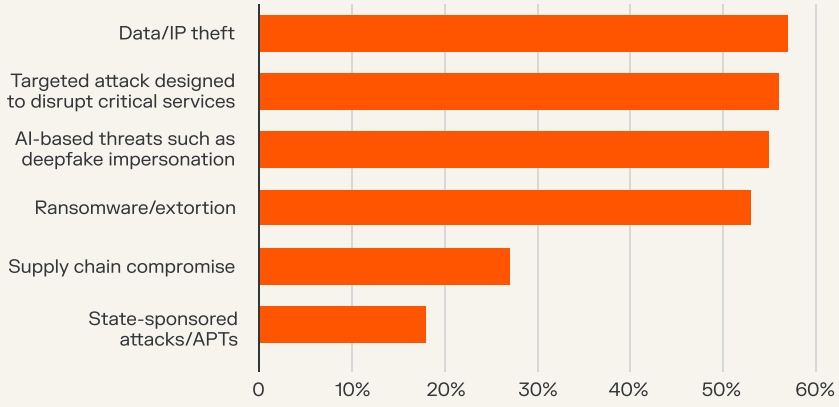
The similar ranking of ransomware (53%) and AI-based threats (55%) shows that organizations no longer separate traditional and new risks. They expect attacks to blend both methods.

Regional differences highlight how the global threat landscape varies. For example, concern about ransomware is much higher




98%

of organizations report concern about at least one type of threat



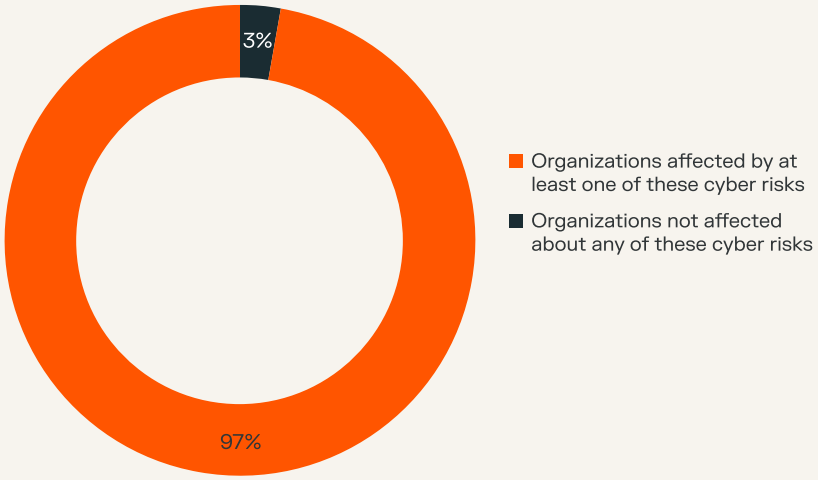
## Which cyber risks are most concerning for your organization? (Select up to five.)

Respondents point to weaknesses they already recognize inside their organizations:

- IT vulnerabilities: 66%
- Employee error or misconduct: 50%
- Lack of IT/OT integration: 50%
- Credential theft and privilege escalation: 45%

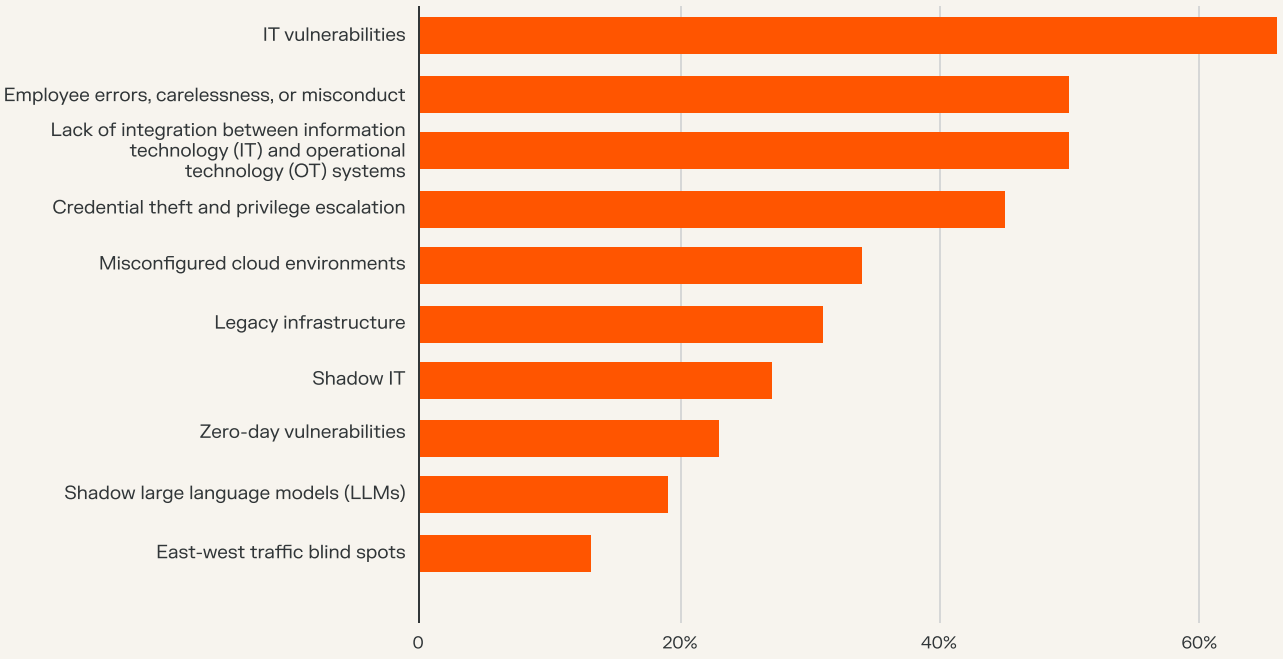
More advanced risks rank lower. Zero-day vulnerabilities are cited by 23% of respondents, and shadow AI tools by 19%. This pattern suggests that unresolved fundamentals still drive most exposure.

Overall, 97% of organizations surveyed say they were affected by at least one cyber risk in the past year.




**97%**

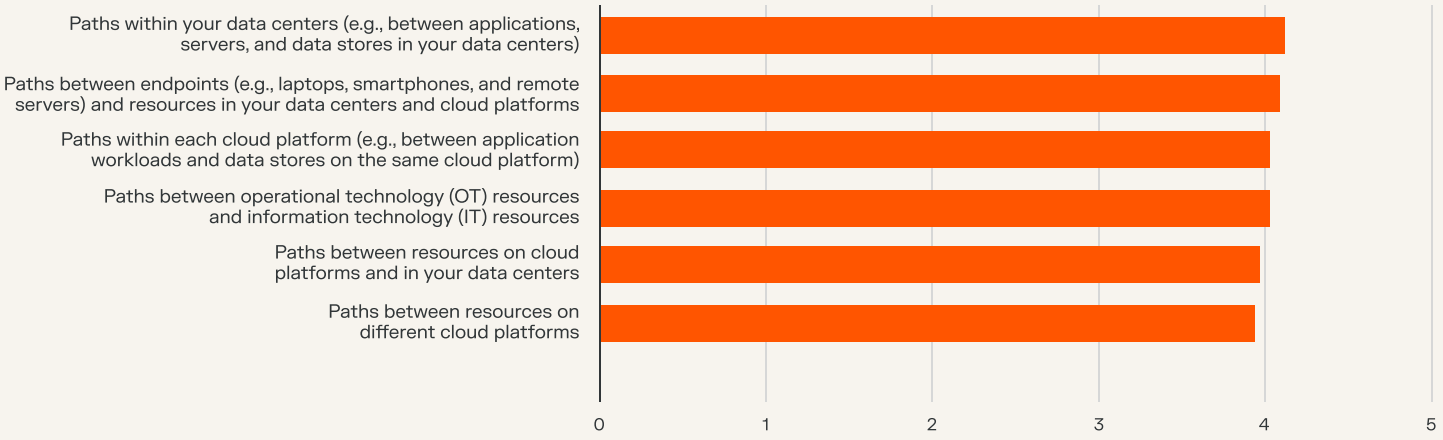
of organizations say they were affected by at least one cyber risk in the past year



## How would you rate your organization's visibility into communication paths that threat actors might be able to use for lateral movement?

Overall visibility receives strong ratings, with an average score of 4.03 out of 5. Confidence is highest in data center environments (4.12) and in communication between endpoints and other systems (4.09).

Visibility is weaker across cloud boundaries, where the average score drops to 3.94. These gaps are important because attackers often move laterally between environments instead of remaining within a single platform.



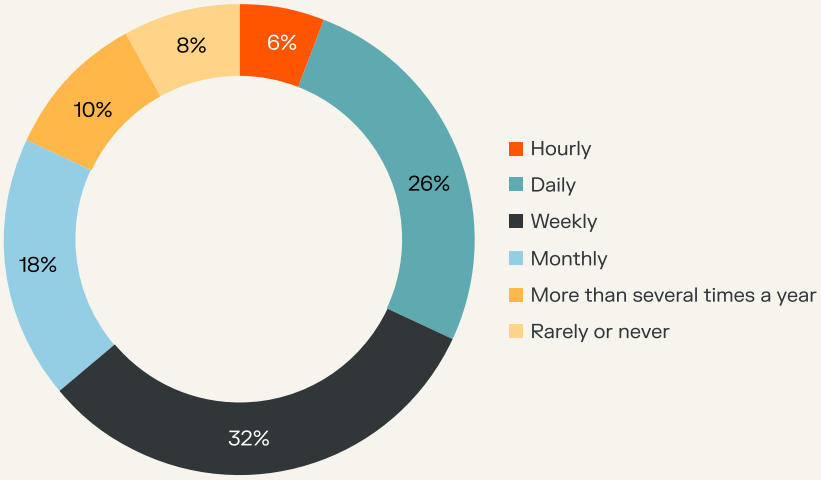
## How often do you discover previously unknown communication paths through scans, security assessments, or other means?

While many organizations report high confidence in their visibility, a deeper look at discovery speeds reveals a wide gap in real-time readiness. For a security model built on resilience, real-time discovery is the only standard that matters; most organizations fall short of this goal.

A total of 63% find new paths weekly or more often, and 32% identify them daily or even hourly. Worse, 37% detect these paths only once a month or less. This creates long periods when access may go unmanaged.

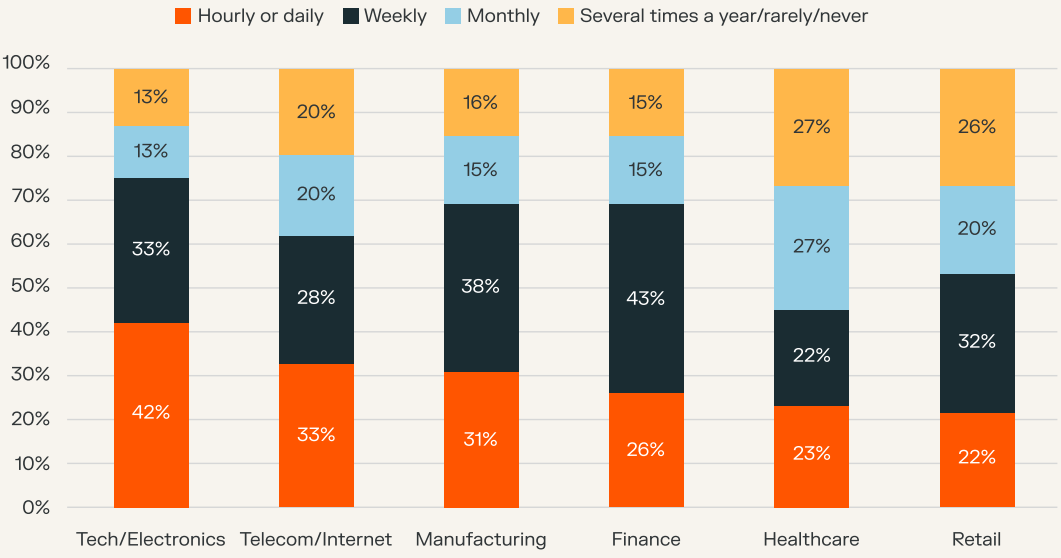
Differences across industries are clear. Among technology companies, 76% detect new paths weekly or faster. In manufacturing, the figure is 69%. In retail, it drops to 54%, and in healthcare, to 45%.

These gaps show how operating models affect security visibility. Technology and manufacturing environments tend to be more automated, which supports faster detection. Retail and healthcare environments are often more distributed and rely on legacy systems, which can slow the discovery of new connections.




**68%**

take a week or more to find unauthorized communications paths



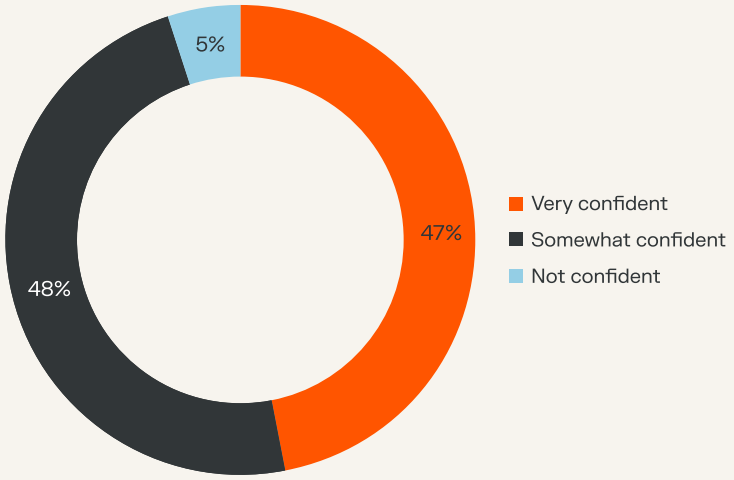
## How confident are you that your team can detect unauthorized lateral movement before it reaches critical information assets?

Confidence in detecting unauthorized lateral movement is extremely high, with 95% feeling very confident or somewhat confident.

Only 5% report low confidence, reinforcing the idea that detection tooling is widely trusted.

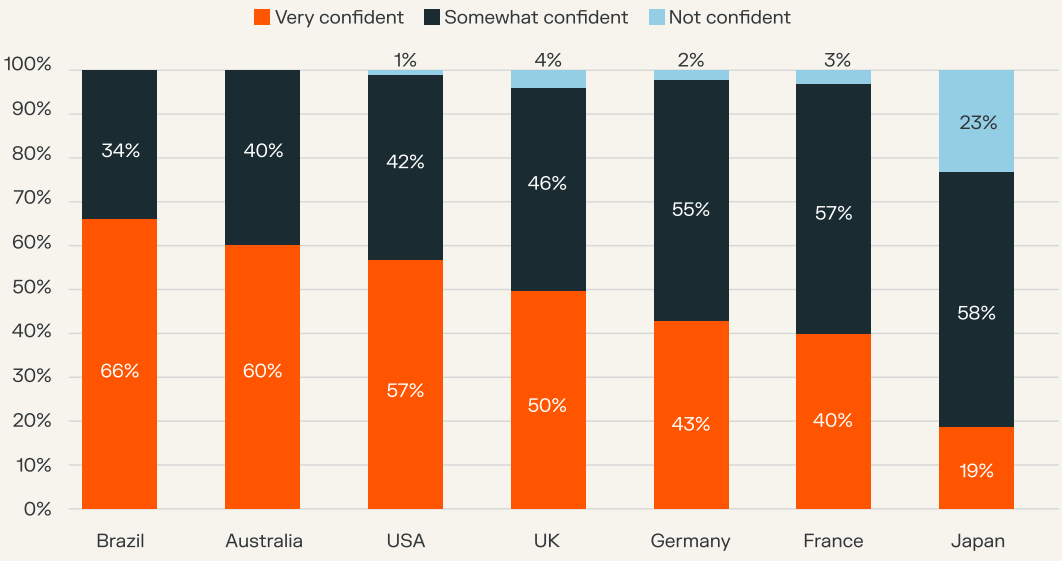
However, this confidence is not uniform. Lower confidence appears in specific pockets, including manufacturing (8%), retail (9%), and most notably Japan (23%).

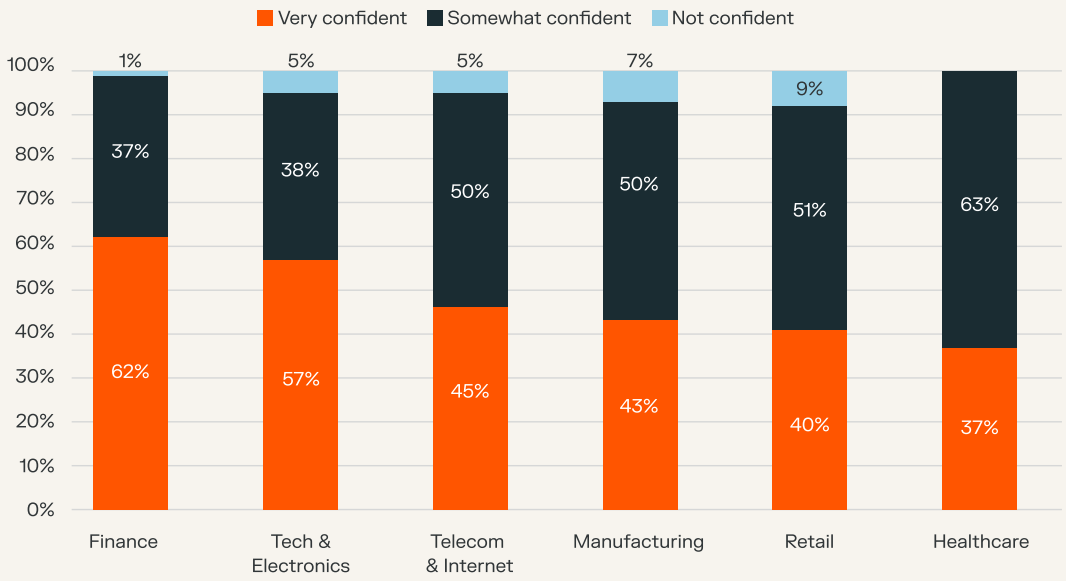
These gaps suggest that detection confidence is influenced by industry complexity and regional operating conditions, even as overall trust in detection remains strong.




# 95%

feel very confident or somewhat confident in detecting unauthorized lateral movement





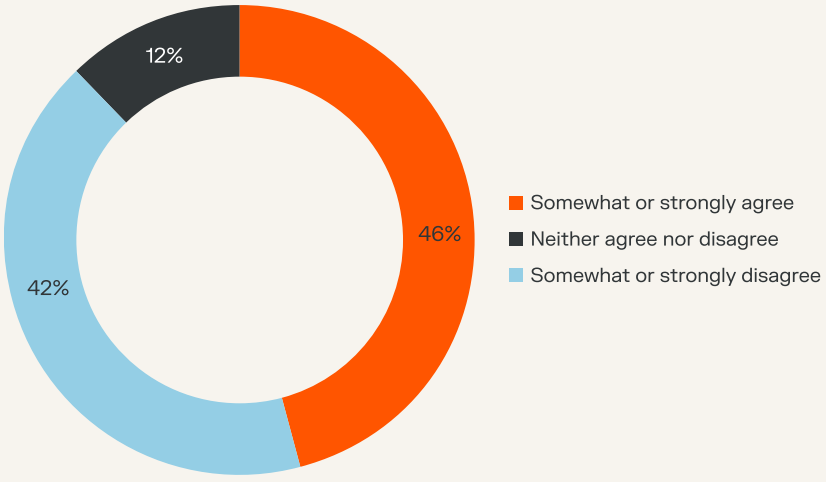

## Describe your agreement with the following statement: "My organization struggles with stopping unauthorized lateral movement."

Responses are sharply divided. Overall, 46% agree that their organization struggles to stop unauthorized lateral movement, while 42% disagree.

Another 12% neither agree nor disagree, suggesting lingering uncertainty or limited visibility into how attacks spread internally.

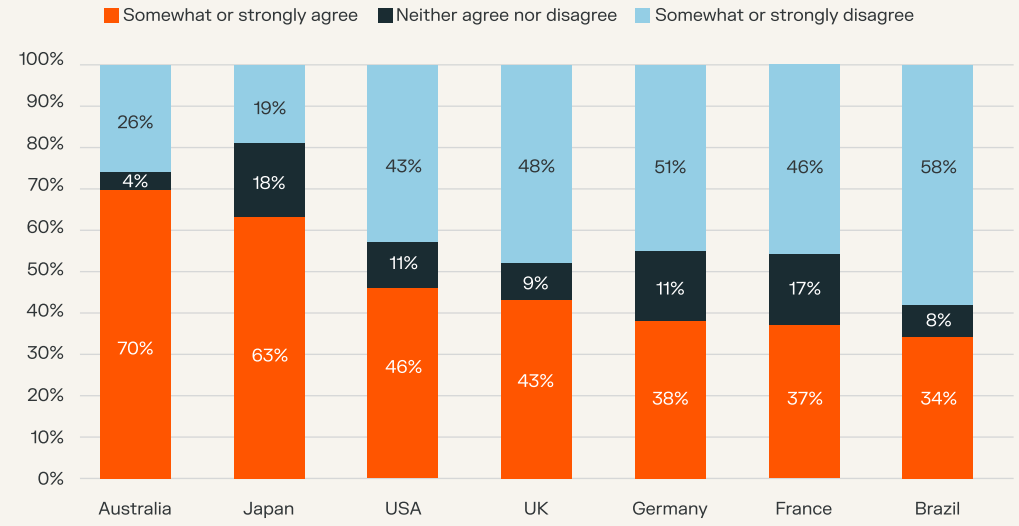
Regional differences are significant. Agreement is highest in Australia (70%) and Japan (63%), well above the global average. Fewer respondents report struggling in France (37%) and Brazil (34%).

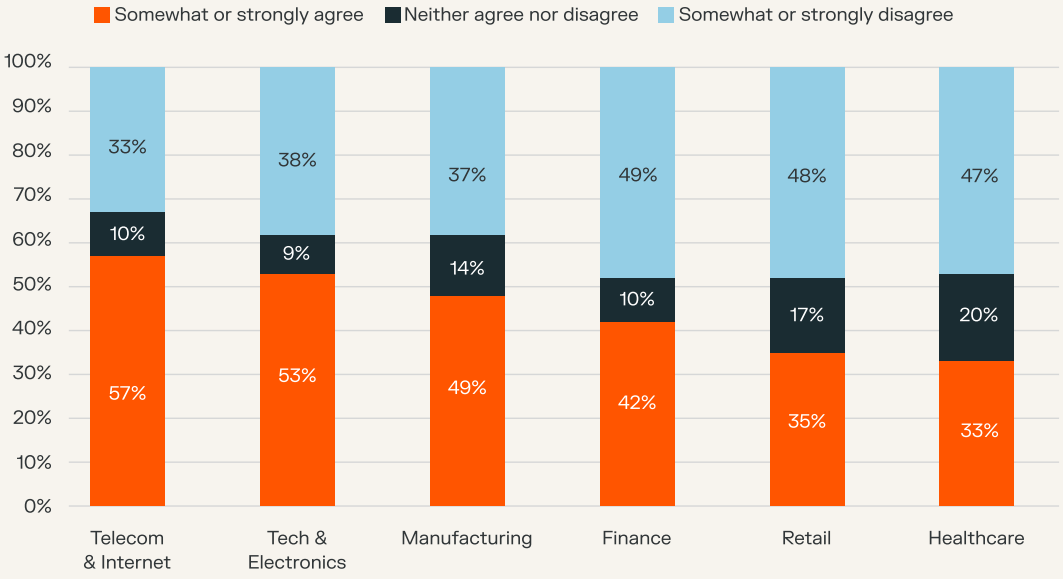
Industry gaps are also pronounced. Telecom (57%) and technology (53%) report the greatest difficulty stopping lateral movement, while retail (35%), and healthcare (33%) report lower levels of struggle.




**46%**

agree that their organization struggles to stop unauthorized lateral movement


Somewhat or strongly agree
Neither agree nor disagree
Somewhat or strongly disagree
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
26%
4%
70%
19%
18%
63%
43%
11%
46%
48%
9%
43%
51%
11%
38%
46%
17%
37%
58%
8%
34%
Australia
Japan
USA
UK
Germany
France
Brazil


Somewhat or strongly agree
Neither agree nor disagree
Somewhat or strongly disagree
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
33%
10%
57%
38%
9%
53%
37%
14%
49%
49%
10%
42%
48%
17%
35%
47%
20%
33%
Telecom & Internet
Tech & Electronics
Manufacturing
Finance
Retail
Healthcare

## Typically, how quickly do you isolate compromised workloads and applications when an intrusion is detected?

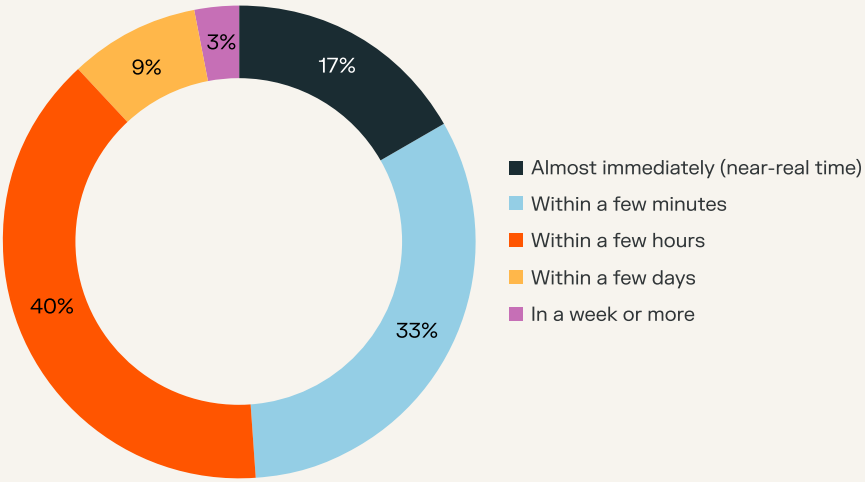
Isolation speed varies widely, which shows uneven containment readiness across organizations.

About half of respondents can act quickly. In total, 17% isolate threats in near real time and 33% do so within minutes, for a combined 50%.

However, 40% still take hours to isolate affected systems, and 11% need days or longer. That delay gives attackers more time to move laterally and increase damage.

These long response windows create significant risk during an active breach.

Overall, the findings show that some teams have strong automation and fast response, but rapid breach containment is not yet consistent across the market.




40%

take hours to isolate affected systems

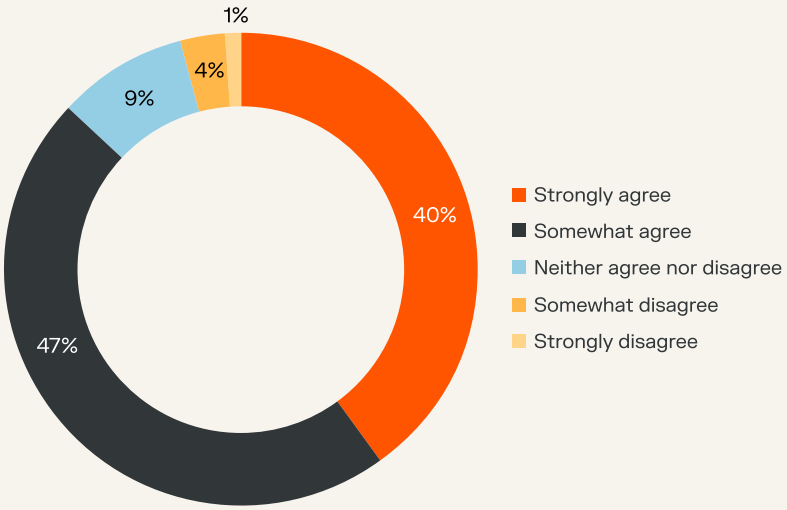
## Describe your agreement with the following statement: “My organization is confident we can quickly contain attacks after a threat actor has established a foothold in our environment.”

Confidence in containment is high overall. In total, 87% somewhat or strongly agree that they can quickly contain attacks after a threat gains a foothold.

Only 4% somewhat or strongly disagree, suggesting that few organizations openly doubt their ability.

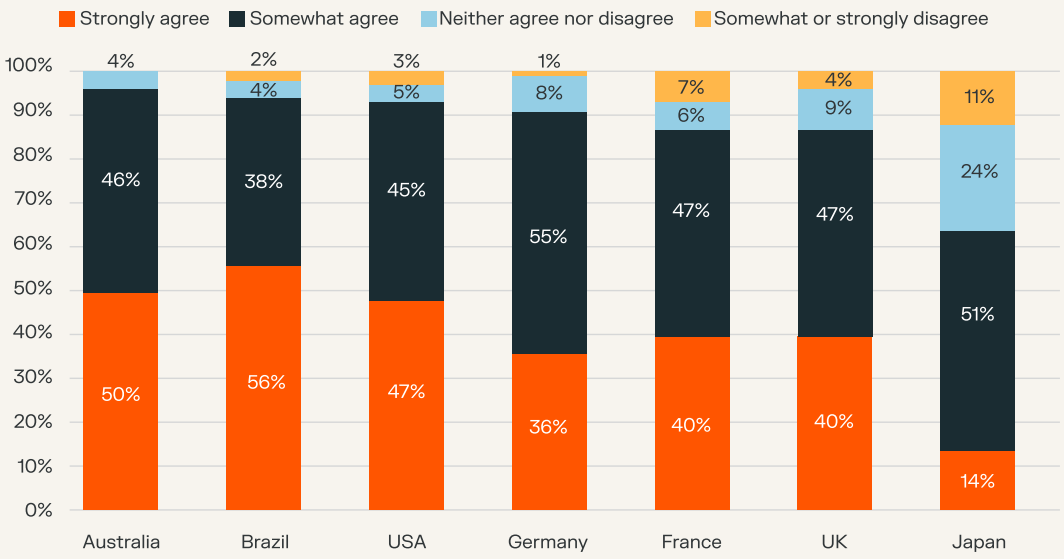
Regional differences, however, are striking. Brazil reports the highest confidence, with 94% somewhat or strongly agreeing. In contrast, Japan stands out as a clear outlier, with only 65% expressing confidence.

These gaps highlight how perceptions of containment readiness vary widely by region, even when overall global confidence appears strong.




**87%**

somewhat or strongly agree that they can quickly contain attacks after a threat



## What approaches to microsegmentation is your organization using now?

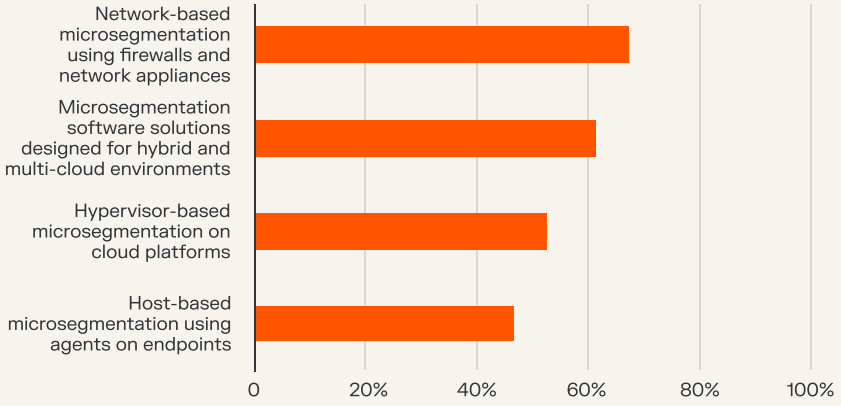
Microsegmentation has officially moved from a niche security project to a mainstream mandate. In total, 93% of organizations report using at least one approach to segment their environments.

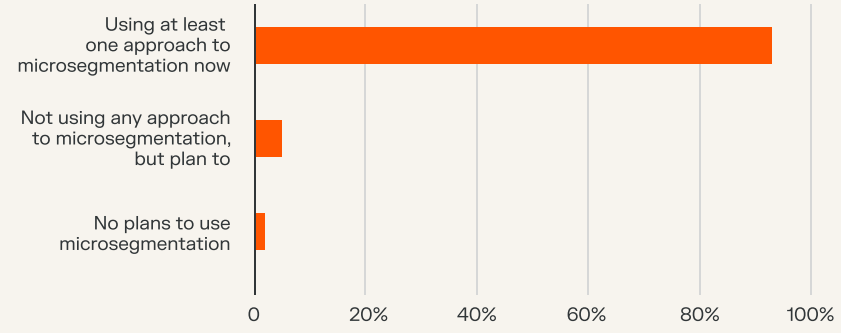
Still, the survey data also reveals a significant definition gap. While the term is widely used, not all approaches achieve the same level of resilience.

The data shows that many organizations are still relying on legacy methods:

- **The firewall:** 68% of respondents still use network-based firewalls for microsegmentation. While familiar, these appliance-based controls often struggle to scale in dynamic, multi-cloud environments where IP addresses change constantly.
- **Modern microsegmentation:** 62% of organizations have moved toward software solutions designed for hybrid and multi-cloud environments. This shift reflects a growing realization that microsegmentation requires a platform that can follow the workload wherever it goes, whether that's on-premises, in the cloud, or at the edge.

Ultimately, these results show that while the intent to segment is nearly universal, the method matters. Organizations relying on hardware-centric tools may find they have created islands of security rather than the consistent, granular containment needed to stop modern lateral movement.




## What is modern microsegmentation?

Modern microsegmentation is the process of isolating individual workloads, applications, or processes from one another — not just dividing the network into large zones.

Unlike traditional segmentation, which relies on hardware perimeters, modern microsegmentation is software-defined, granular, and decoupled from the underlying network.

It provides a way to enforce security policies based on the identity of the workload rather than its IP address.

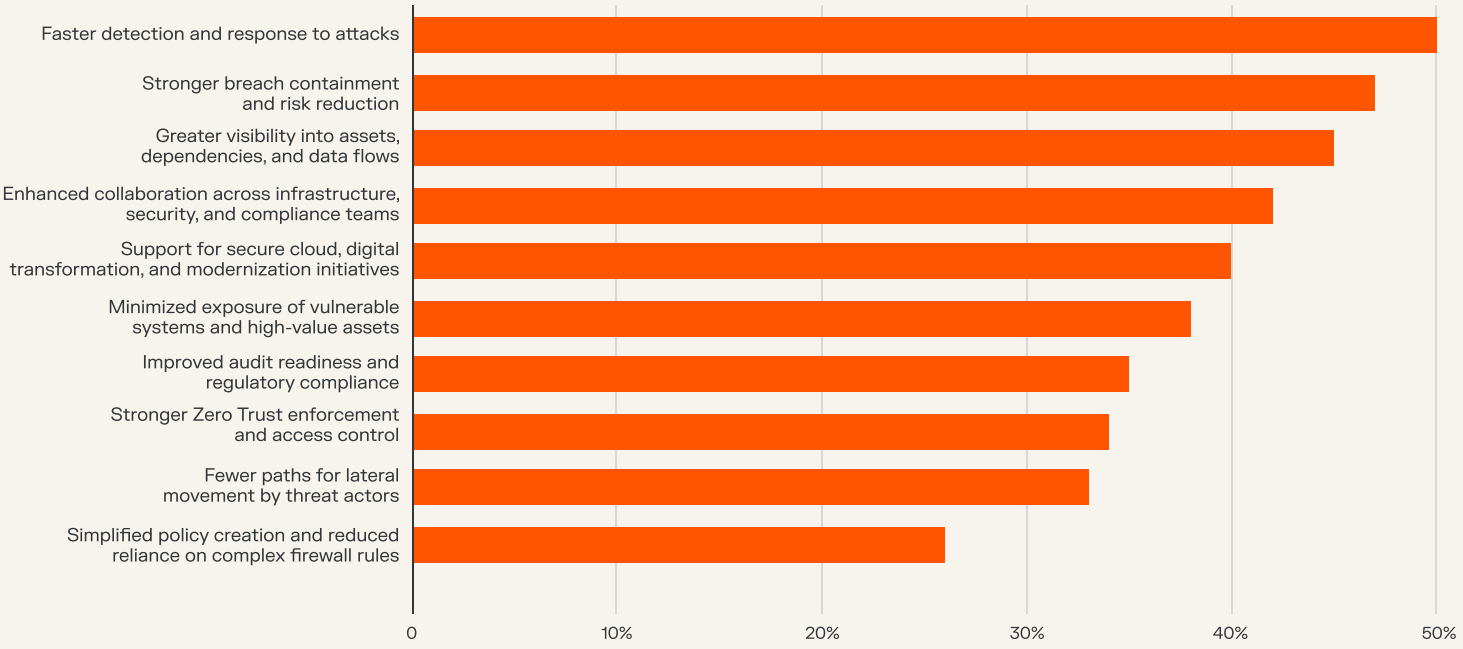
## What are the most important benefits of microsegmentation and extensive visibility into application and workflow traffic between endpoints, applications, data stores, and other information assets? (Select up to five.)

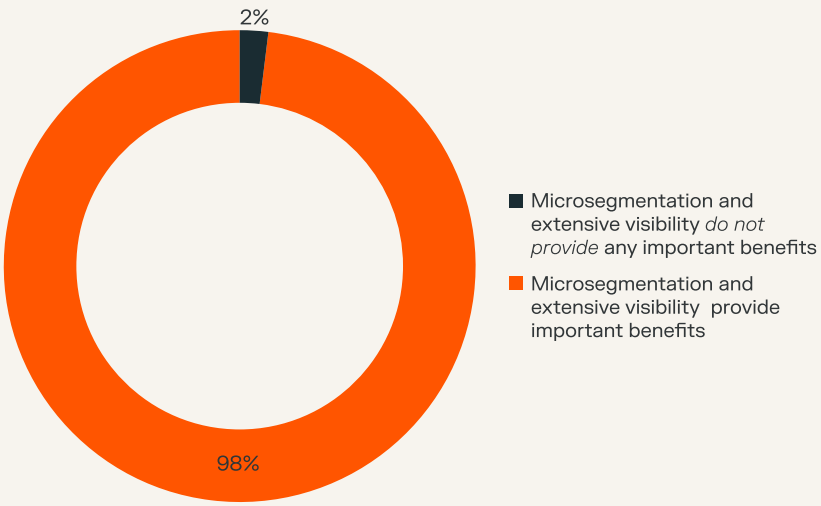
Microsegmentation provides clear value for most organizations. In total, 98% of respondents say it delivers meaningful benefits.

The most important benefits relate to direct security outcomes. Half of the respondents report faster detection and response to attacks as one of the top five benefits they have experienced. And almost as many (47%) include stronger breach containment in their top five list.

In addition, 45% point to improved visibility into assets and data flows, which helps teams see how threats move through the environment.

All of the 10 benefits listed in this question were selected by at least a quarter of the respondents. This shows that microsegmentation delivers broad value across many security and operational needs.




98%

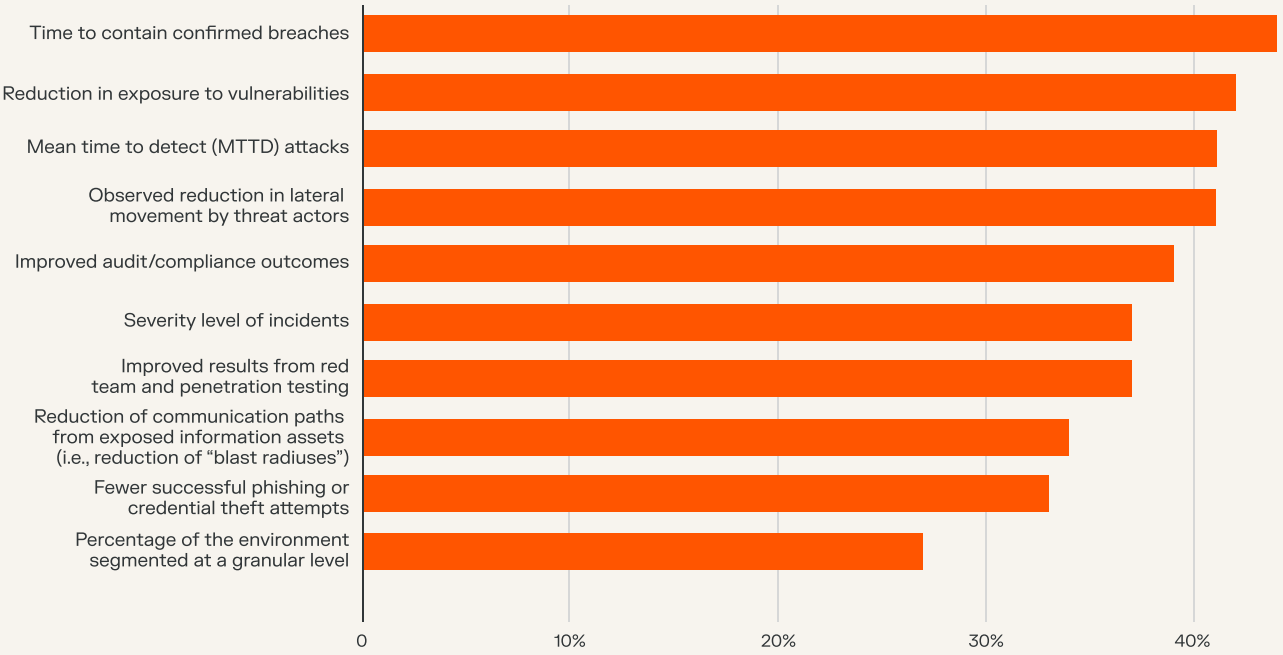
of respondents say microsegmentation delivers meaningful benefits

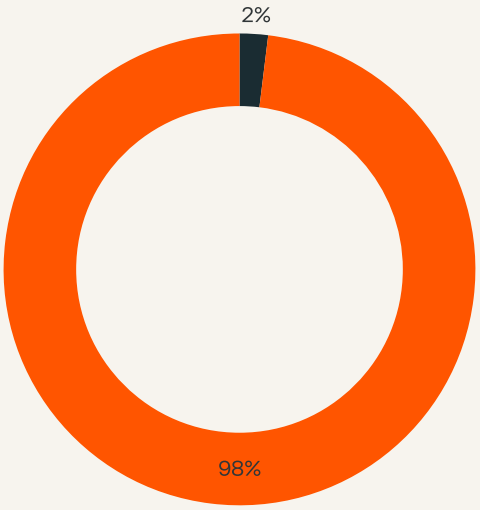
## What metrics does your organization use to track the performance of microsegmentation efforts and activities to reduce lateral movement by threat actors?

Nearly all (98%) of organizations track at least one metric tied to microsegmentation and efforts to reduce lateral movement. The most common metrics focus on real outcomes. Globally, 44% measure time to contain confirmed breaches, 42% track reduced exposure to vulnerabilities, and 41% measure both mean time to detect and observed reductions in lateral movement.

This consistency holds across industries. Retail reports the highest measurement rate at 99%. Technology reports the lowest, but it's still at 96%.

Together, these patterns show that organizations are not only measuring technical performance but also trying to align microsegmentation metrics with industry-specific risk and business priorities.




*Don't* measure the performance of microsegmentation and reduction in lateral movement

*Do* measure the performance of microsegmentation and reduction in lateral movement

98%

track at least one metric tied to microsegmentation and efforts to reduce lateral movement

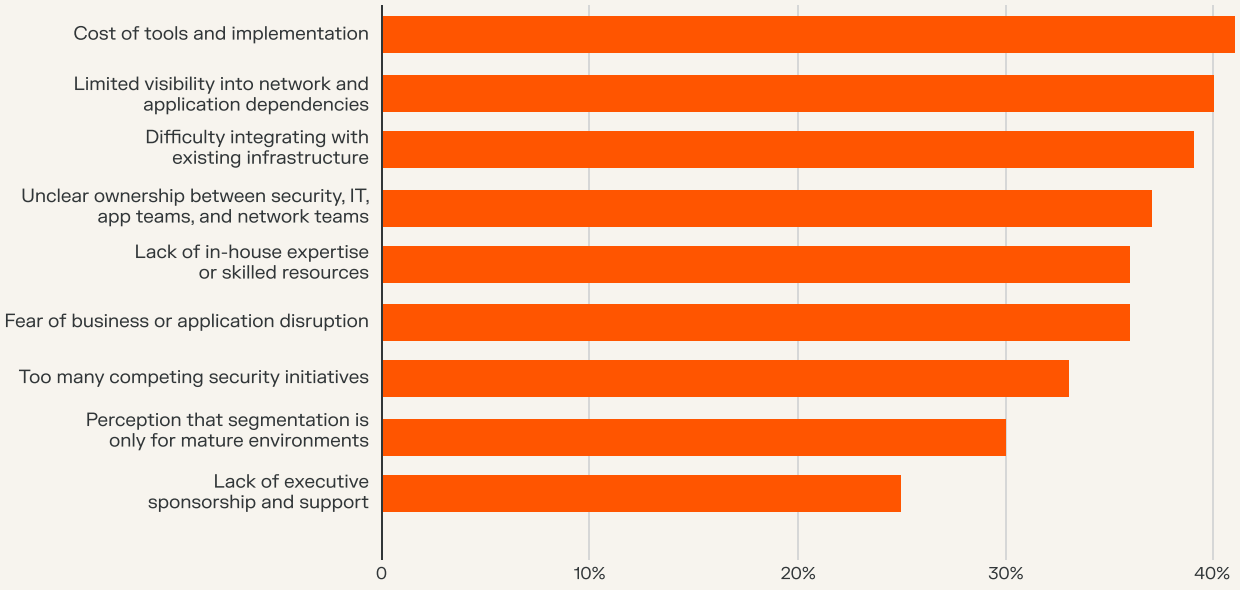
## What are the biggest barriers to improving or implementing microsegmentation in your environment? (Select up to five.)

The barriers to microsegmentation are largely practical rather than strategic.

The most common challenges are cost (41%), limited visibility into network and application dependencies (40%), and difficulty integrating with existing infrastructure (39%). These issues likely reflect operational complexity more than resistance to the strategy itself.

Organizational factors also play a role. About 37% cite unclear ownership across teams, while 36% point to a lack of in-house expertise. Another 36% express concern about potential business disruption during deployment. These challenges show that coordination and skills gaps can slow progress.

In contrast, lack of executive sponsorship ranks lowest at 25%. This indicates that most CISOs and IT leaders already support microsegmentation. The primary obstacles are execution and implementation, not leadership buy-in.



PART 4

# Conclusion: closing the containment gap

The data is clear: hidden beneath today's cybersecurity confidence lies a critical, systemic gap.

For years, the industry's broken status quo has relied on a two-pillar strategy of prevention and detection. We've been told that if we just build a thick enough perimeter and buy enough visibility, we're secure.

The research shows the failure of this model. Prevention is no longer a guarantee. Nearly every organization (97%) was concerned about at least one cyber risk last year. And while detection tools are widespread, they're often toothless without the immediate power to act.

Organizations now report high visibility, yet only 17% can isolate a threat in near-real time. This is why we say cyber is broken. Detection and visibility are no longer enough to prevent disaster.

If an attacker can be detected but remains uncontainable for hours or days, the system has failed. The current model relies on a chain of internal trust that attackers now exploit as a high-speed highway.

To fix the system, the focus must shift:

- **From detection to containment:** Detection only alerts you to the fire; containment is what puts it out. Success must be measured by how quickly a threat is neutralized, not just how fast it was spotted.
- **From implicit to explicit trust:** The trust tissue of the internal network is a liability. We must replace wide-open pathways with granular, workload-level controls that assume breach by default.
- **From network silos to unified policy:** Modern microsegmentation must be the standard, providing a consistent kill switch for lateral movement across every environment, whether it's on-premises, cloud, or OT.

The era of find-and-fix is over. The future of security depends on closing the breach containment gap: the ability to withstand an attack by ensuring it has nowhere to go.

The research shows that organizations understand they need to make this shift. What remains is the execution to close the containment gap for good.

APPENDIX

# Methodology and participant profile

# Methodology

CyberEdge adopted an online methodology and recruited IT and cybersecurity decision-makers and key influencers.

Interviews were conducted in the United States, United Kingdom, France, Germany, Brazil, Japan, and Australia.

All respondents were guaranteed to remain anonymous as part of the study. Fieldwork was carried out between September 15–25, 2025.

**700** respondents in total

**65%** work for companies with more than 5,000 employees

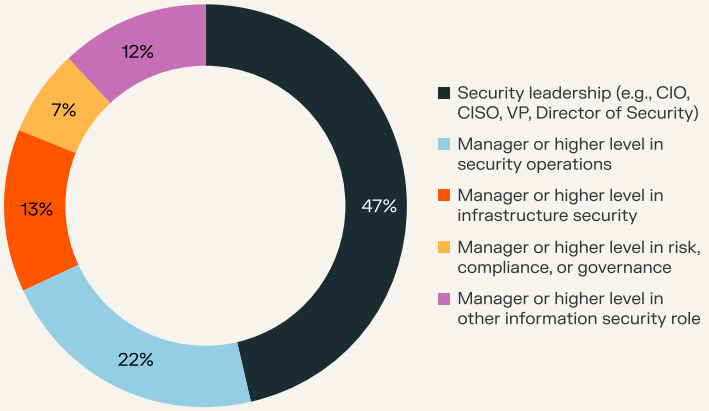
**47%** are in security leadership roles (CIO, CISO, VP, Director of Security)

**25%** work in the technology industry

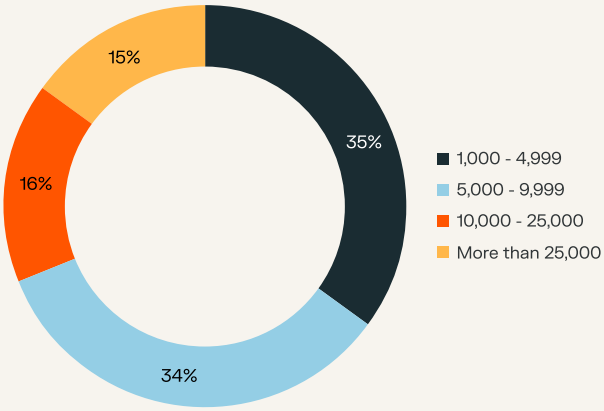
# Participant profile

| Total | U.S. | UK | DE | FR | JP | OZ | BR |
|---|---|---|---|---|---|---|---|
| N=700 | N=200 | N=100 | N=100 | N=100 | N=100 | N=50 | N=50 |
| **100%** | **29%** | **14%** | **14%** | **14%** | **14%** | **7%** | **7%** |

## Job titles




## Organization size




## Top industries

| Industry | Quantity | Percentage |
|---|---|---|
| Technology & Electronics | 110 | 16% |
| **Manufacturing** | 105 | 15% |
| **Finance & Financial Services** | 92 | 13% |
| **Retail & Consumer Durables** | 71 | 10% |
| **Telecom and Internet** | 61 | 9% |
| **Healthcare & Pharmaceuticals** | 51 | 7% |
| **Other** | 210 | 30% |

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an 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.

The Illumio Platform comprises:

**Insights**. Hybrid AI detection and response. Identify risks, detect attacks, and contain threats with one click.

**Segmentation**. Cloud and network breach containment. Proactively enforce security policies to prevent lateral movement.

Learn how Illumio can close the containment gap with first and only platform built to stop breaches where they start.

Visit: www.illumio.com/company/about-illumio


Founded in 2012, CyberEdge Group is the premier research, marketing, and publishing firm dedicated exclusively to serving the cybersecurity vendor community. As the producer of the distinguished Cyberthreat Defense Report (CDR) and numerous other award-winning research studies, CyberEdge has earned recognition from top-tier business and technology outlets, including The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Media, Dark Reading, CISO Magazine, and Security Buzz.

Renowned for its depth of cybersecurity expertise and commitment to excellence, CyberEdge delivers world-class market research, survey analyses, analyst reports, white papers, and custom books and eBooks tailored to the cybersecurity industry. Its unmatched combination of subject-matter knowledge and comprehensive service offerings continues to set the gold standard for quality and insight.

To learn more, visit www.cyberedgegroup.com.