Bitdefender

CYBERSECURITY ASSESSMENT REPORT

Global Insights from 1,200 Cybersecurity Professionals

June 2025

Bitdefender

Summary

The 2025 threat landscape is defined by speed, stealth, and scale. Cyberattacks are more adaptive and harder to detect, fueled by stolen credentials, fileless techniques, and generative AI tools that empower low-skilled adversaries. At the same time, internal cybersecurity teams are battling growing complexity, a disconnect between the C-suite and the frontline, and pressure to keep reportable breaches quiet.

Our annual Bitdefender Cybersecurity Assessment Report is based on two things: an industry survey of 1,200 IT and security professionals across six countries; and internal analysis conducted by our threat research team. The data reveals that some of today's most dangerous risks are also the quietest. Attackers are weaponizing common and trusted tools to evade detection as they move through networks of organizations around the world.

The 2025 findings reveal that proactive security is no longer optional. Organizations are overwhelmingly looking to reduce their attack surface in addition to relying on detection and response. The survey data also confirms ongoing concerns around AI: worry about usage by attackers, yes, but also the risk created by organizations themselves as they increasingly utilize the immense number of AI tools flooding the market.

In the final analysis of the research results, it's likely the next generation of security leaders will be defined not only by how fast they react but also by how smartly they prepare.

84%

of modern attacks leverage Living Off the Land (LOTL) techniques, bypassing traditional detection systems.

68%

of security leaders agree they need to reduce their attack surface by disabling unnecessary tools or applications.

58%

of respondents say they were told to keep a breach confidential, often in conflict with compliance and ethical standards.

Only **19%**

of mid-level managers report strong confidence in their organization's cyber readiness, despite 45% of C-level executives saying they feel "*very confident.*"

SECTION 1

Proactive Defense — Shrinking the Attack Surface

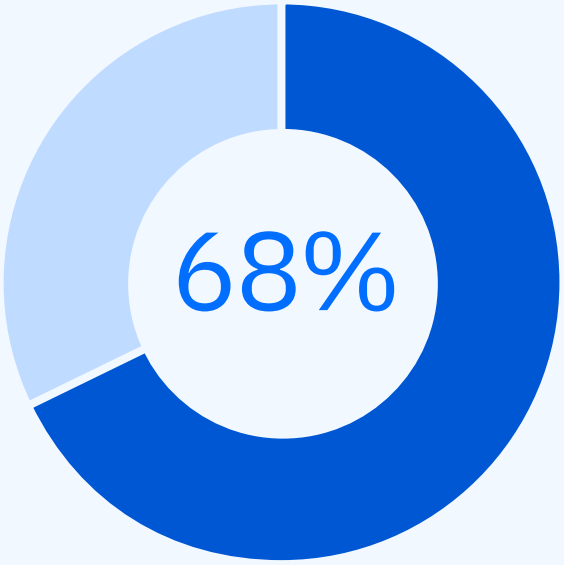
Detection alone is no longer enough, as modern threats are increasingly stealthy. Today, attackers are more likely to "log in, instead of breaking in" using stolen credentials, legitimate tools, and native access to quietly blend into their target's environment. This makes traditional security strategies insufficient. The path forward begins not with more alerts but with shrinking the attack surface itself.

The urgency is clear: 68% of security leaders agree that reducing the cyberattack surface by disabling unnecessary tools and applications is critical. This shift alone would give threat actors fewer ways into an environment and fewer places to hide once they are inside. This pivot toward proactive defense reflects the growing understanding that every unused admin account, dormant application, or excessive permission is an open invitation to a threat actor.

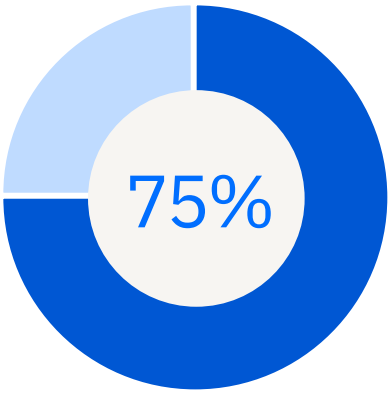
Survey Results

We need to reduce our attack surface by disabling unnecessary tools or applications.

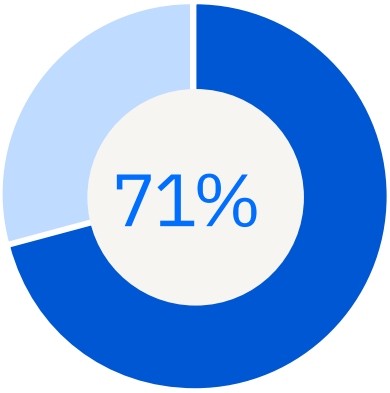
Overall



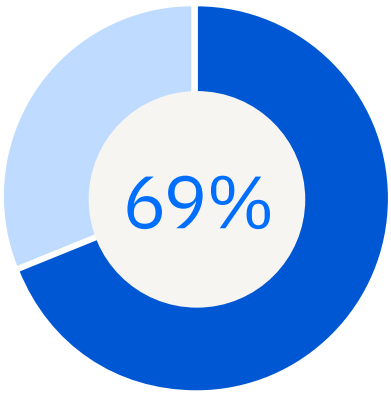
USA



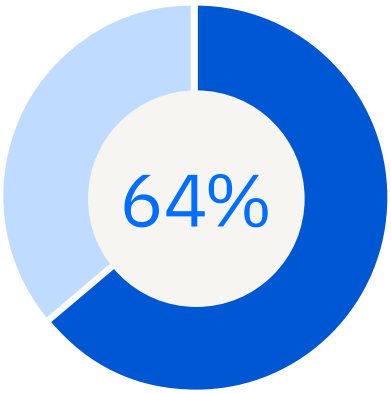
Singapore



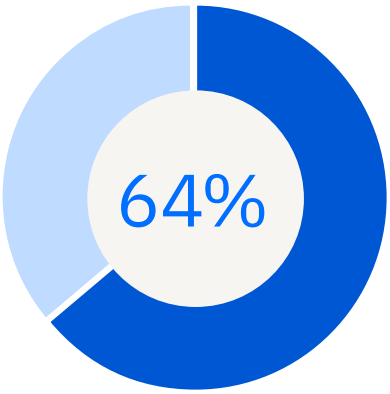
Italy



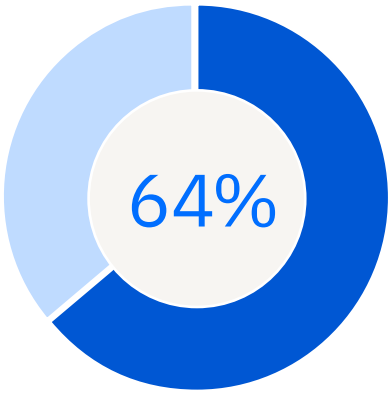
Germany



UK



France



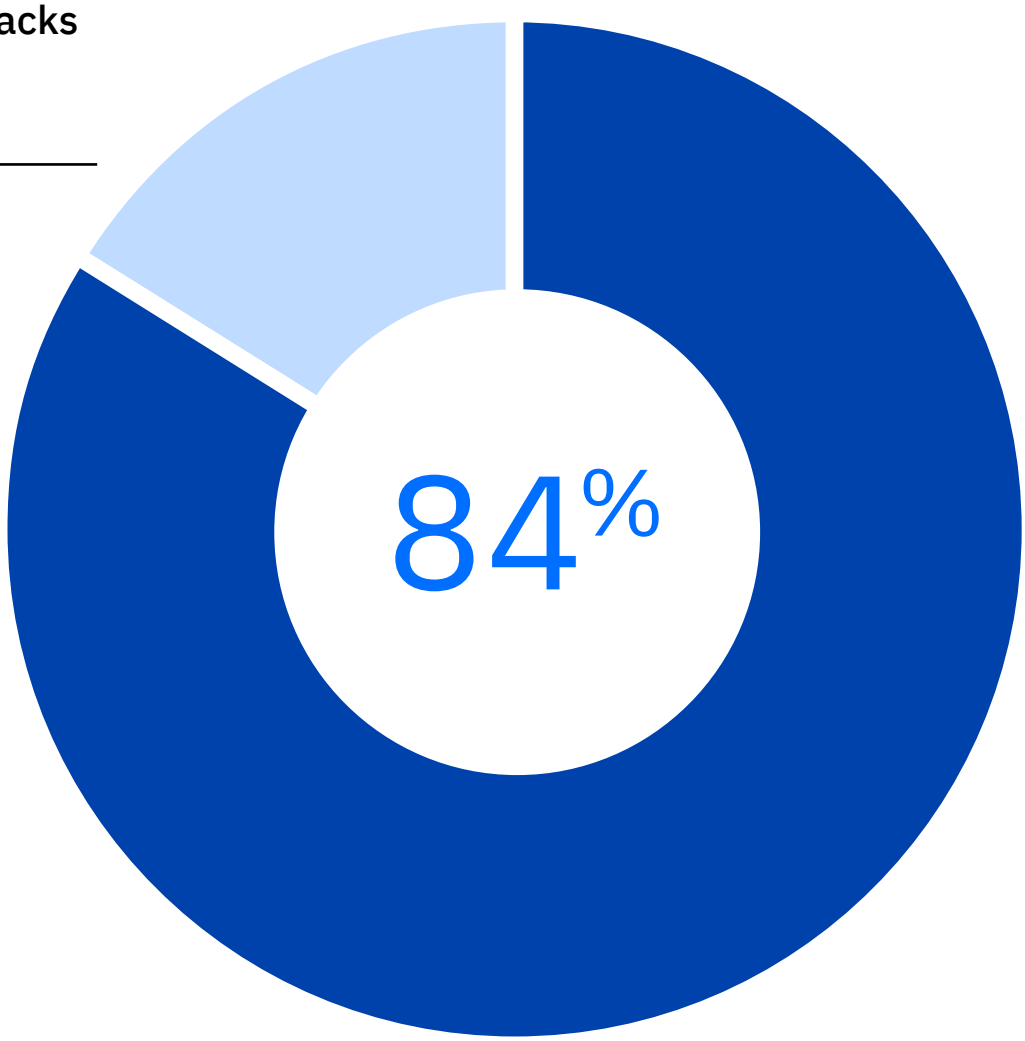
A New Risk Environment: Built from Within

Why are security leaders increasingly focused on shrinking the attack surface? It's because the modern attack surface isn't defined by external perimeters. It often exists within. Every excess credential, every overlooked software tool, and every over-provisioned user represents a possible path to compromise. Attackers have taken notice.

New data reveals that techniques like Living Off the Land (LOTL), which rely on tools already present in the environment (e.g., PowerShell, WMI), now dominate the threat landscape. Bitdefender recently analyzed more than 700,000 cyber incidents and discovered that 84% of major attacks leverage LOTL techniques. This is a major threat actor pivot to bypass traditional defenses.

84% of major cyberattacks use LOTL techniques

Bitdefender analyzed 700,000 cyber incidents



Understanding LOTL Techniques

Rather than introducing foreign binaries or malicious software that might trip alarms, threat actors use legitimate utilities already in the operating system, network, or cloud infrastructure.

Because these tools are widely used by IT teams and administrators, their presence doesn't inherently trigger alerts. That's the danger. There's no malware to scan for, often there's no suspicious downloads to trace, just familiar utilities that are quietly manipulated to escalate privileges, disable defenses, and exfiltrate data. Addressing this type of attack surface risk is challenging, as this year's Cybersecurity Assessment survey reveals.

Common LOTL tools include:

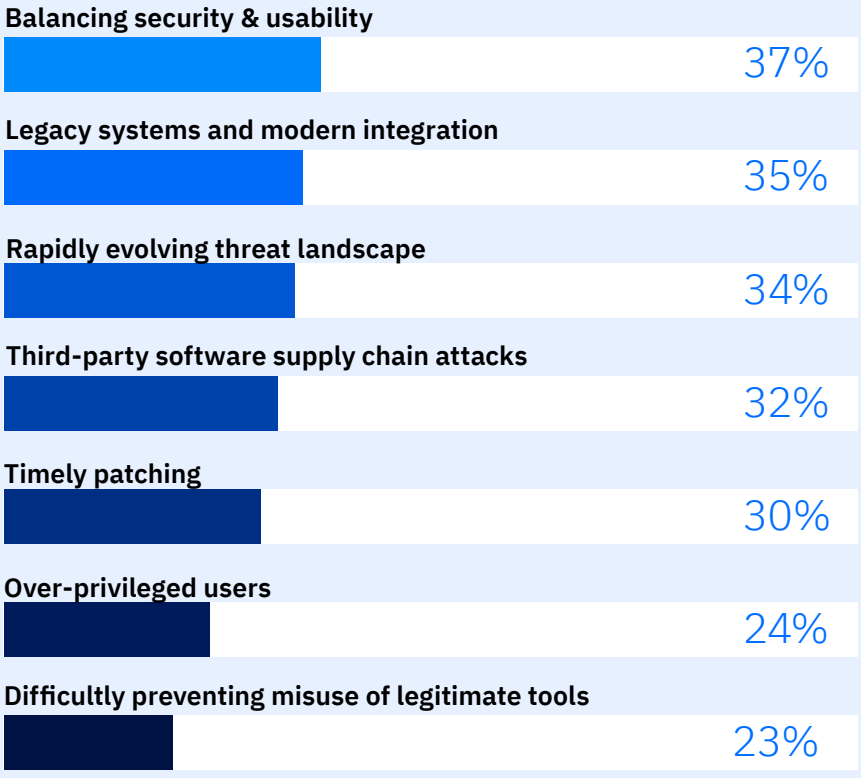
- **PowerShell:** Used for scripting, automation, and system management.
- **Windows Management Instrumentation (WMI):** Used for device management and querying system information.
- **Remote Desktop Protocol (RDP):** Enables remote access to desktops and servers.
- **PsExec:** A Microsoft utility used to execute processes on remote systems.

Survey Results

What, if any, are the top challenges your organization faces in attack surface hardening and reduction?

Respondents selected up to three of their top choices.

Overall



USA

Germany

UK

France

Italy

Singapore

The Struggle of Traditional Tools

Traditional “one-size-fits-all” security controls, like group-based application restrictions or universal tool blocking, often fail in practice. Organizations can’t simply disable every risky tool as users have legitimate needs. For example, in a healthcare setting, clinicians may rely on specific diagnostic software, IT staff need scripting access, and third parties may require temporary privileges. Over-restricting leads to friction while under-restricting opens the door to compromise.

What’s needed is granular, adaptive control, not blanket restrictions.

Proactive Security, Personalized at Scale

Modern proactive defense takes a different approach. Rather than trying to block everything by default, it focuses on understanding what’s normal then flagging deviations. This means building individualized baselines for every user and endpoint pair, with an understanding of the tools they use, when, and how often. And this should be paired with a knowledge of how threat actors typically abuse these same tools.

Proactively reducing the attack surface makes it harder for attackers to move, escalate, or exfiltrate. It eliminates easy footholds and forces adversaries to behave abnormally, raising their chances of detection.

This approach frees up detection and response tools (EDR/XDR) to focus on genuinely novel threats, not noise. When proactive hardening is done right, it doesn’t replace detection. It elevates it.

SECTION 2

The Complexity Problem Lurks Around Every Corner

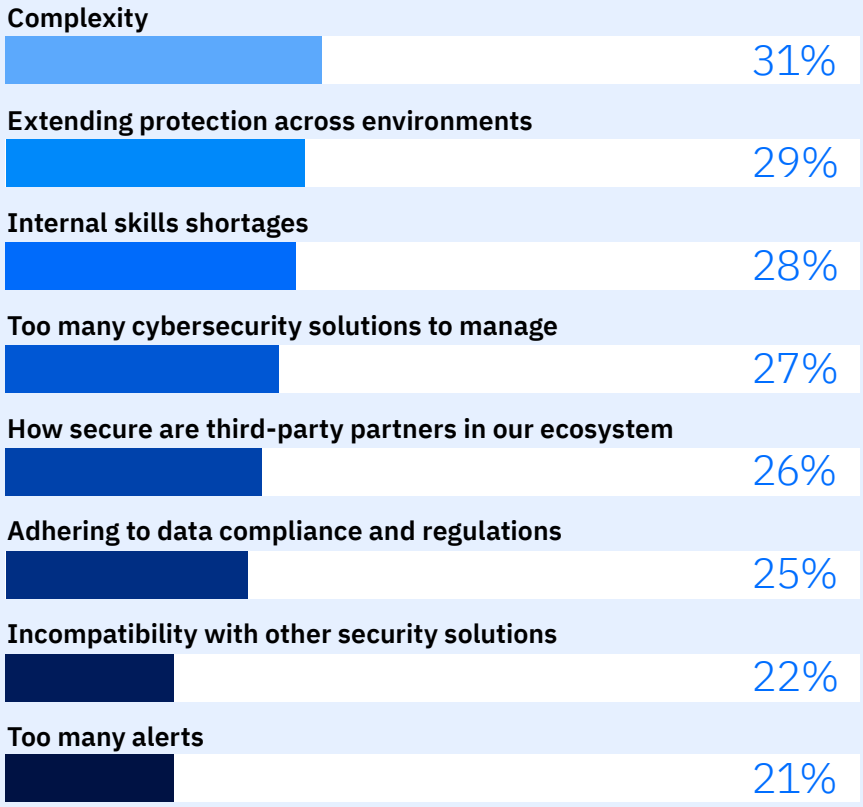
While the threat landscape grows more complex, so does the security environment at many organizations. A large number of disparate tools continues to create overlap, gaps, and alert fatigue. Nearly one-in-three (31%) IT & security professionals listed “complexity” as the biggest challenge relating to their current security solutions. And speaking of complexity, the growing number of regulations led 25% of respondents to say that adhering to data compliance and regulations is one of their top 3 challenges about their current security environment.

Question

What are your top security solutions challenges?

Respondents selected up to three of their top choices.

Overall



The Number One Security Solutions Challenge by Country

USA

34% Extending capabilities across multiple environments

Germany

42% Complexity

UK

34% Complexity

France

32% Lack of internal security skill set to drive full value of solutions

Italy

30% Lack of internal security skill set to drive full value of solutions

Singapore

39% Lack of internal security skill set to drive full value of solutions

Lack of Visibility and Automation

Visibility is a top priority and also an ongoing struggle for organizations. 77% of research respondents say they lack enough insight into their environment. And security operations teams are already overwhelmed: 50% say a lack of automation hinders their work and 49% report burnout from the constant need to monitor and respond.

Machine learning driven automation can help by creating high-fidelity alerts, filtering out the noise and surfacing only the alerts that need human attention. Services like MDR take even more of the load off internal teams, so they can focus on bigger-picture security priorities.

77% of research respondents say they lack enough insight into their environment.

50% say a lack of automation hinders their work.

49% report burnout from the constant need to monitor and respond.

SECTION 3

The AI Arms Race – Friend and Foe

Artificial intelligence is reshaping the cybersecurity battlefield. For defenders, AI supports automation which can speed up detection and response measures. For attackers, AI lowers the barrier to entering the ransomware ecosystem and can improve their overall efficiency. Some ransomware groups utilize AI tools to refine the code they've developed; others rely on AI to create it.

The Bitdefender threat research team recently profiled a ransomware group that started out with limited knowledge, leading many to perceive them as script kiddies. The group, FunkSec, wrote numerous posts asking for advice on how to hack systems and where to start. Then, the group turned to Generative AI to create basic ransomware code. This was code that the group did not have the skills to develop on their own. Fast forward to today and the group's victim count is climbing as it successfully targets organizations in countries around the globe. The threat actor continues to use AI to fill knowledge gaps and improve operations.

As AI becomes more accessible and powerful, both sides are adopting it, fueling a high-stakes arms race and redefining how cyber battles are fought. This has many IT & cybersecurity experts concerned: 51% of survey respondents say AI-generated threats are their number one concern. These include things like sophisticated deepfake-based social engineering, and automated vulnerability exploitation.

On the defensive side, AI helps security teams detect threats faster, prioritize risks more accurately, and accelerate investigations. Machine learning can flag unusual behavior, correlate signals across systems, and automate responses, often before a human analyst intervenes.

But attackers are adapting quickly. Generative AI tools like LLMs enable threat actors to craft polished phishing emails, build fake login pages, refine malicious code, and scale attacks with minimal skill. Common red flags, like typos or clumsy language, are disappearing. Even low-skill attackers can now launch various cyberattack campaigns that previously required specialized expertise.

AI Concerns: Perceptions vs. Reality

With generative AI's availability came fears of an AI-infused super-malware. Despite the media hype, our investigations at Bitdefender, along with broad industry research, reveal a different picture. There's little evidence that attackers are using AI to create unusually sophisticated malware. Instead, what's happening is a widening of the playing field. LLMs are being used for basic tasks like debugging or refining existing code, effectively upskilling less experienced threat actors.

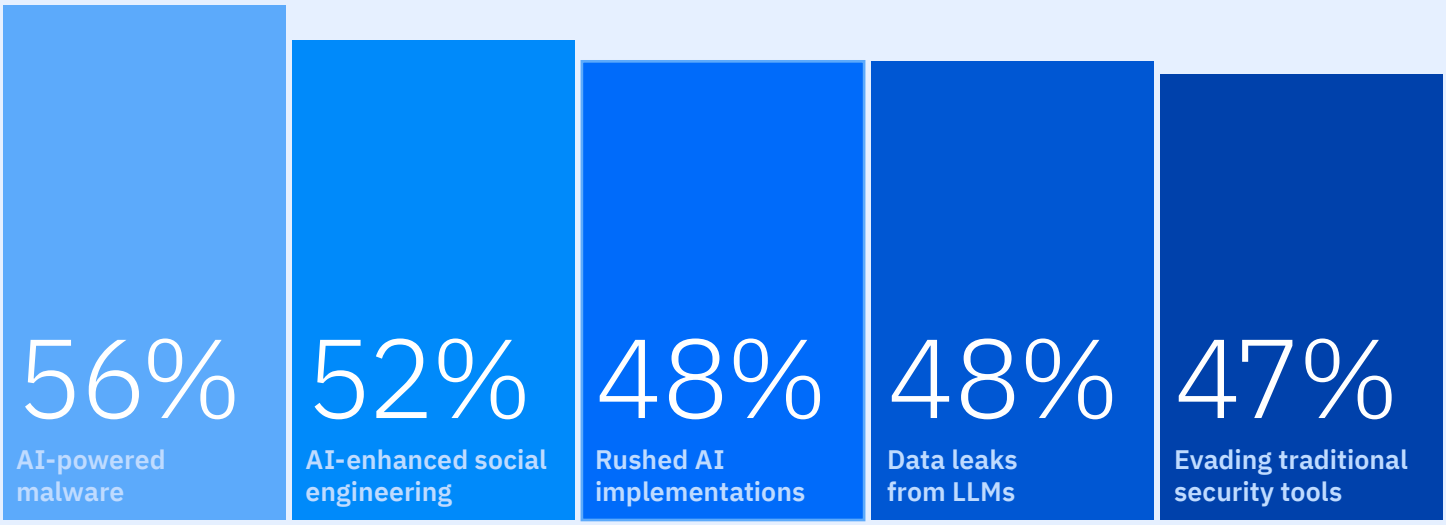
For now it appears AI isn't necessarily making elite attackers more powerful—it's making average ones more dangerous. However, the 2025 Cybersecurity Assessment Report reveals a significant amount of perceived risk from threat actors leveraging AI, and some concerns, about self-inflicted risks as organizations increasingly adopt AI powered tools.

Question

How much of a risk to your company (as a threat to cybersecurity) are the following aspects of AI?

Respondents selected up to three of their top choices.

A significant risk:



AI-Driven Security Impacts

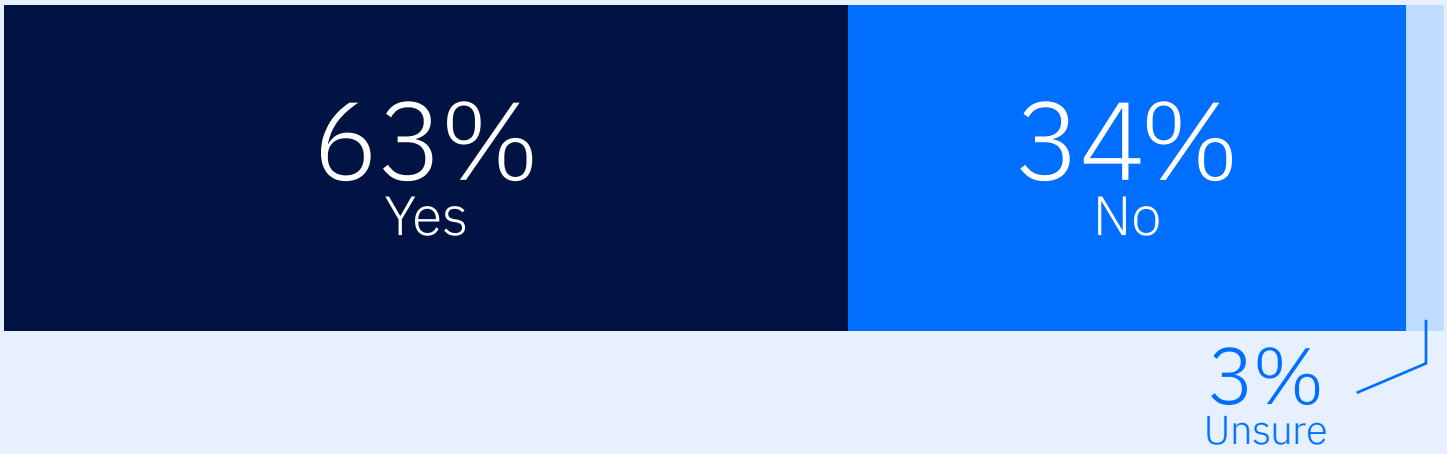
While the most advanced AI-driven attacks may still be rare, many believe their presence is growing. 67% of organizations report seeing an increase in AI-powered cyberattacks, and 63% say they've already experienced an AI-related incident in the past year. Additionally, 65% say identifying malicious communications in an era of nearly flawless text generation is difficult.

Based on the new research, two things remain clear. First of all, the AI-enabled cyber battlefield is evolving and remains unsettled. And secondly, true cyber resilience requires more than just deploying an AI-powered platform. It depends on foundational security hygiene, behavioral baselining, and human oversight. Organizations that pair intelligent automation with experienced analysts and layer it over a hardened, well-managed infrastructure are far more likely to succeed than those chasing "set-it-and-forget-it" solutions.

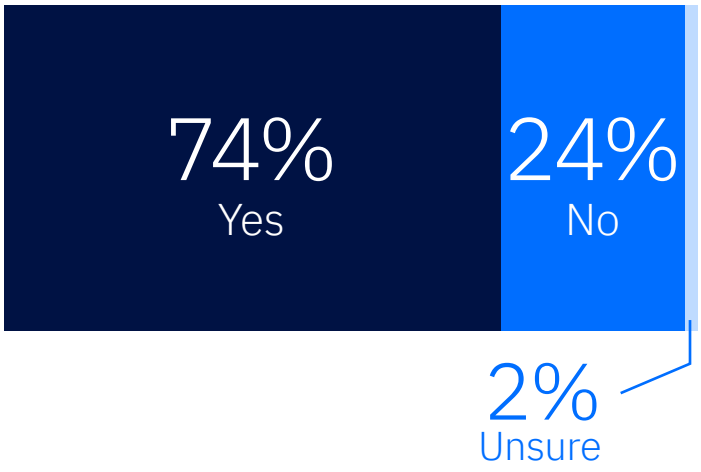
Question

In the last 12 months, has your organization experienced an attack that you believe involved AI?

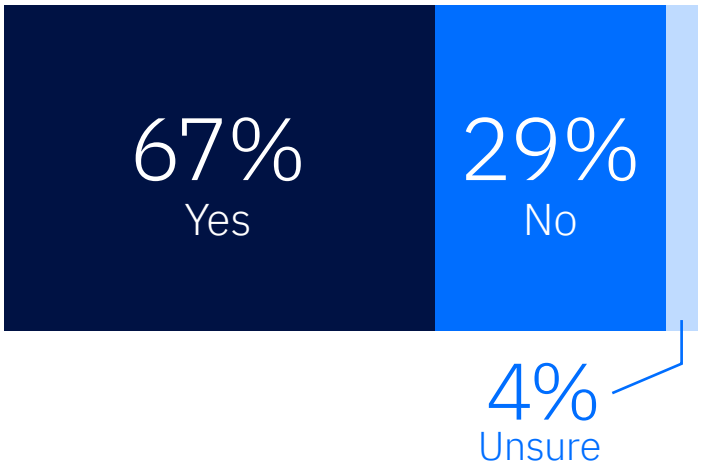
Overall



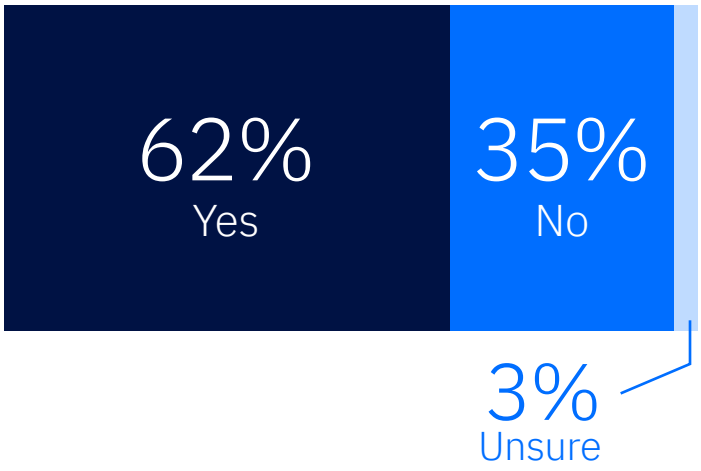
USA



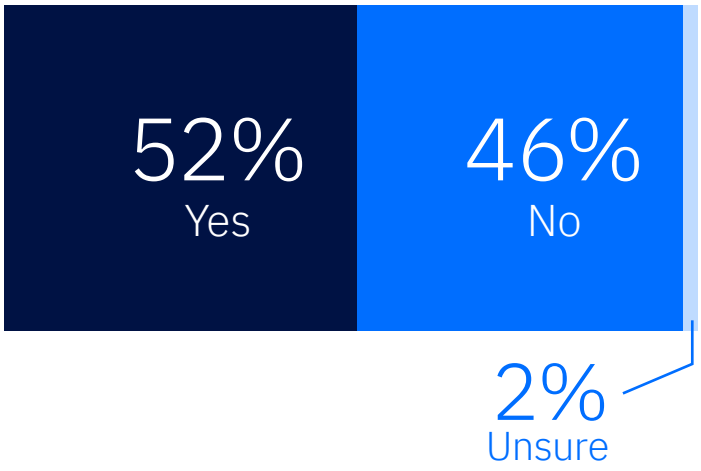
Germany



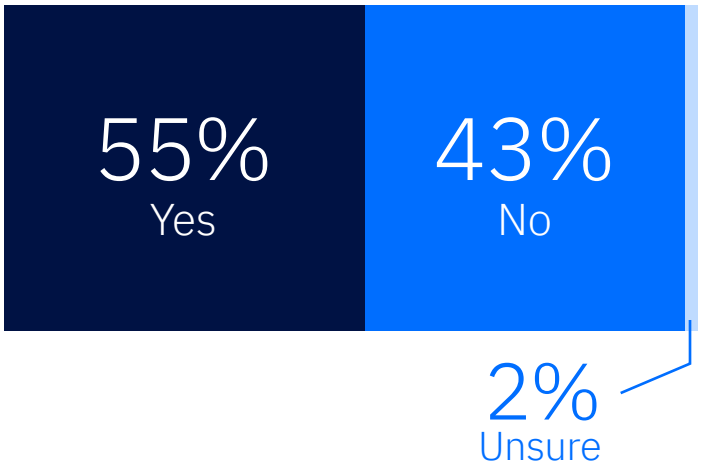
UK



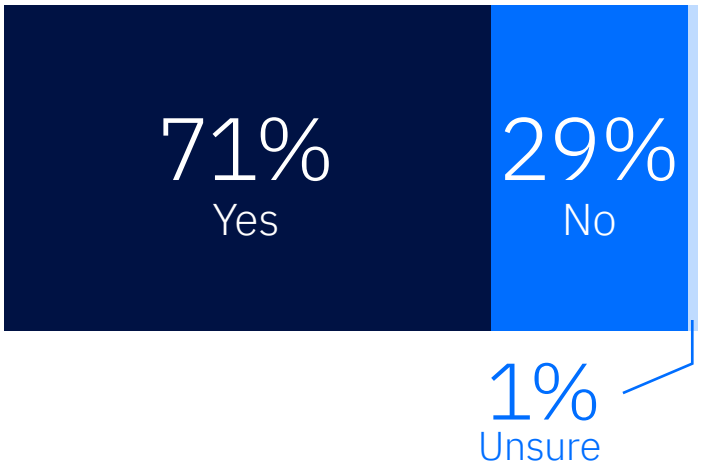
France



Italy



Singapore



SECTION 4

Perception Gaps – Executives vs. the Frontline

Cybersecurity is only as strong as the decisions behind it, and those decisions depend on clear, shared visibility into risk. When executive leaders and frontline practitioners operate from different assumptions about what's secure and what's vulnerable, the organization is often left exposed. Small disconnects today quickly become major gaps tomorrow.

Our research reveals a growing perception gap, and it's happening across industries. At first glance, it seems like all is well because confidence in cyber readiness runs high: 93% of surveyed professionals say they're either "somewhat confident" or "very confident" in their ability to manage risk as the attack surface continues to grow. However, a closer look at the data tells a more complicated story.

Confidence at the Top, Caution on the Ground

C-level executives are often the most confident. Nearly half of CISOs and CIOs in the 2025 survey say they are “very confident” in their organization’s ability to manage expanding risk. That’s more than twice as confident as mid-level managers. The disconnect may stem from differing vantage points. Leaders see strategy, budgets, and roadmaps, while practitioners see unpatched systems, alert overload, and emerging attacks in real time.

Question

How confident are you in your organization’s ability to manage risks as the attack surface continues to grow?

Very Confident:

Unfortunately, when leadership overestimates readiness, it can result in underinvestment in people, process improvement, and technology.

And this example is far from the only data that points to a disconnect between the top and mid-levels of IT and security.

Misaligned Priorities, Misguided Investments

Different levels of the organization are also prioritizing different things this year. The C-suite respondents say their top priority is adopting AI tools for advanced threat detection (41%), while less than a third of mid-level managers agree. Instead, managers listed their number one priority (35%) as strengthening cloud security and identity management.

This split reflects a broader challenge: executives may chase innovation and high-visibility technologies while frontline teams wrestle with day-to-day operational risk. The end result includes a lack of focus and slower progress as teams row toward different priorities.

Has the Skills Gap Changed? Depends on Who You Ask

The shortage of qualified cybersecurity talent continues according to ISC2 research , which says the cyber workforce has leveled off at 5.5 million workers. So, is the skills gap getting worse or are we at least holding steady? This is another area where senior management and front-line managers differ.

Question

The cybersecurity skills gap in my organization has worsened in the last 12 months.

Strongly Agree

57%
C-level

40%
Mid-level management

A perceived skills gap (or lack of one) can drive organizations to consider certain security approaches or solutions above others. And so can independent evaluations, especially for executives. In the survey, 72% of C-level leaders say they rely heavily on third-party validations like MITRE or Gartner in purchasing decisions, compared to just 53% of mid-level managers.

Where Views Align

Not all perceptions diverge. When it comes to identifying the biggest threats, alignment exists across roles. C-level and mid-level respondents rank data breaches that lead to customer or intellectual property loss and BEC/phishing attacks as their top concerns. This shared awareness offers a valuable foundation for bridging other gaps.

Question

What cybercrime-related challenges, if any, pose the greatest threat to your business in 2025?

Business Email Compromise (BEC) and targeted phishing campaigns

There's a good reason for this alignment:

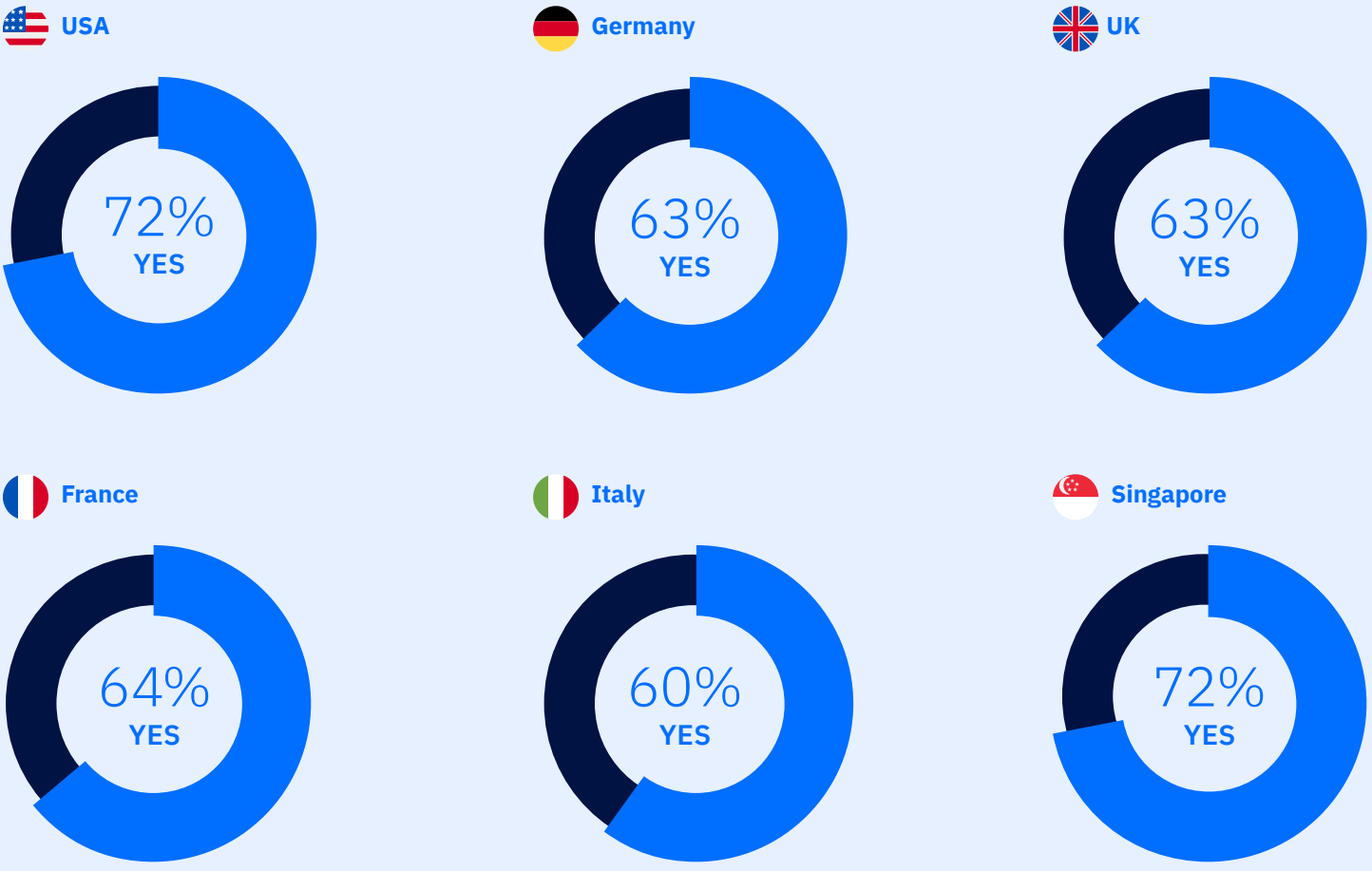
The number of BEC attacks are growing.

Agreed: BEC Attacks on the Increase

While threat actors manipulate trusted tools in LOTL attacks, they are also increasingly abusing trusted people and information through Business Email Compromise (BEC) attacks. In this year's survey, 66% of respondents say they have witnessed an increase in BEC attacks.

These attacks rely on pre-texting: where the attacker creates a believable scenario that needs urgent and often confidential action, while impersonating someone an employee may know and trust; a vendor they do business with or an executive they answer to within their organization. This approach is both effective and expensive: according to the FBI, organizations around the world lost more than $55 billion through BEC attacks during a single decade.

I have seen an increase in Business Email Compromise Attacks



SECTION 5

Increased Regulation, Growing Pressure to Keep Breaches Quiet

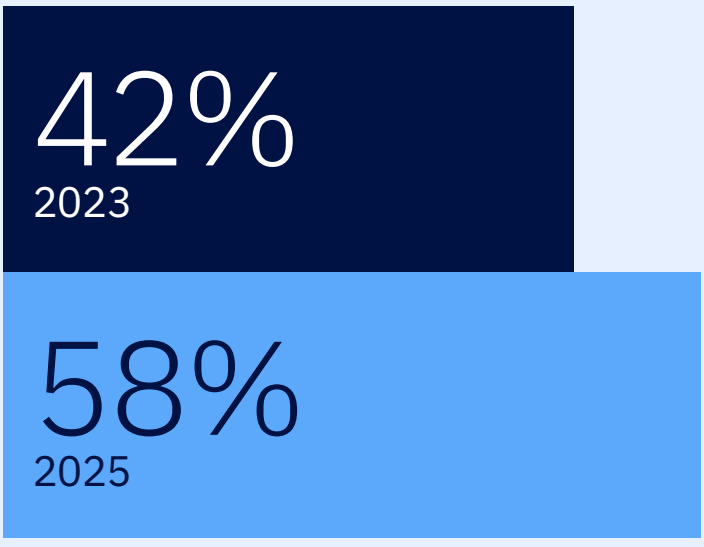
In cybersecurity, timing is critical. When a breach occurs, the speed and transparency of the response can significantly affect how much damage is done. Early disclosure allows faster remediation, limits regulatory exposure, and may help to preserve long-term customer trust. But in many organizations, transparency is not the goal, keeping a breach quiet is. Shockingly, nearly 6-in-10 survey respondents say they were told to keep quiet about a cybersecurity incident at their organization. This is a 38% increase since we asked about this in the Bitdefender 2023 Cybersecurity Assessment report.

Question

You said you experienced a security incident or breach in the last 12 months. Were you told to keep the incident confidential when you knew it should be reported to authorities?

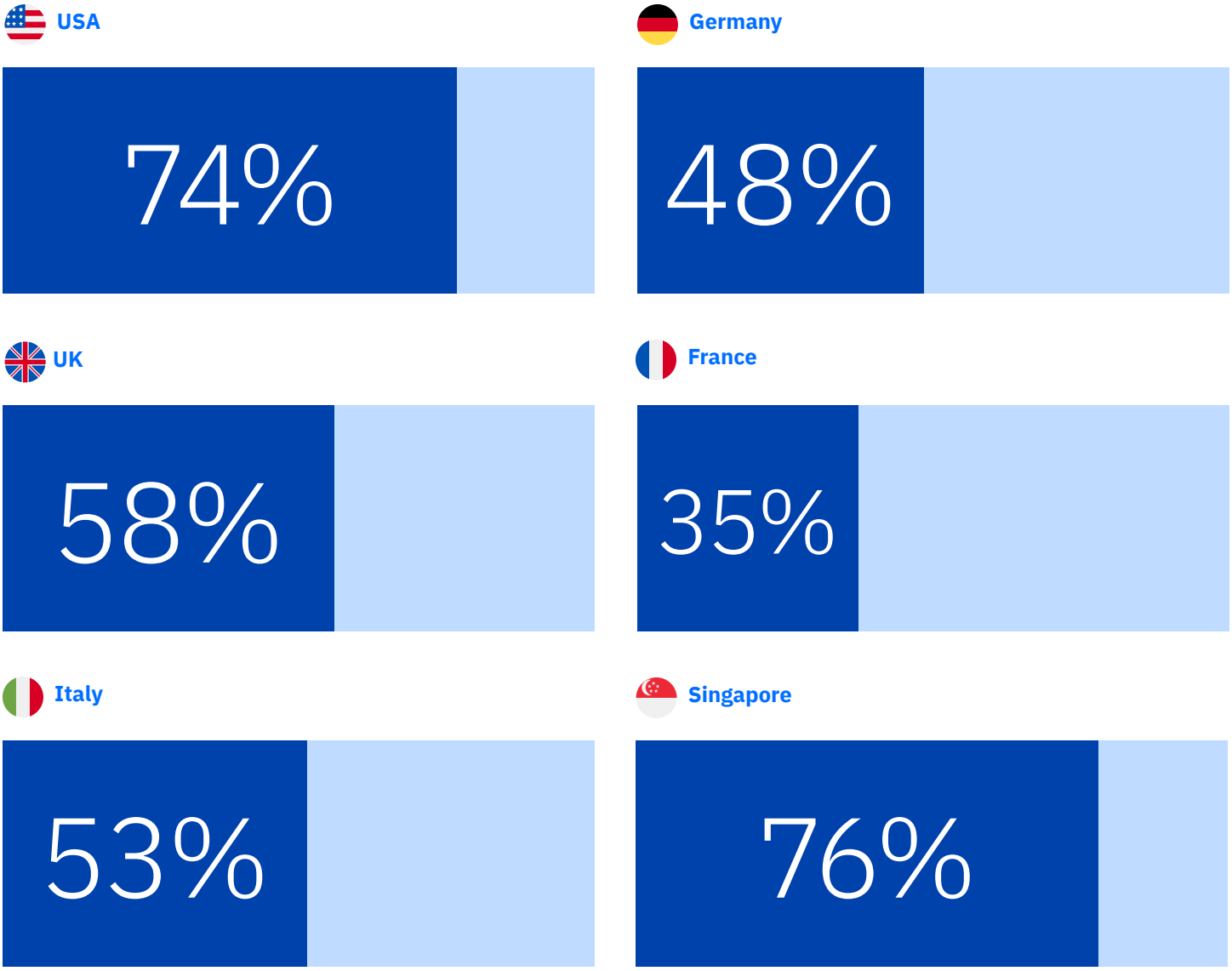
% of respondents saying "Yes"

By Year



38% percentage increase (2023 vs. 2025)

% of respondents saying they were told to keep quiet, by country:



CISOs and CIOs feel the most pressure in this area, as 69% of C-level executives report being told to stay silent, while 46% of mid-level managers were told the same. The overall numbers indicate that breach concealment isn't an isolated issue but instead it is systemic. What emerges is a picture of cultural norms and internal decision-making frameworks that increasingly value discretion even in cases where that may not be allowed.

One possible driver of this trend is the pressure organizations face to achieve and maintain compliance with the growing number of regulatory mandates. If a breach notification reveals non-compliance, then the financial, regulatory, and reputational impacts could be severe. This is one of the reasons a growing number of organizations utilize compliance manager tools that simplify compliance and help achieve meaningful risk reduction at the same time. It's time to treat compliance as more than a checkbox, but instead as a strategic enabler, to mitigate cyber risk, strengthen defenses, and build long-term resilience.

The High Cost of Staying Quiet

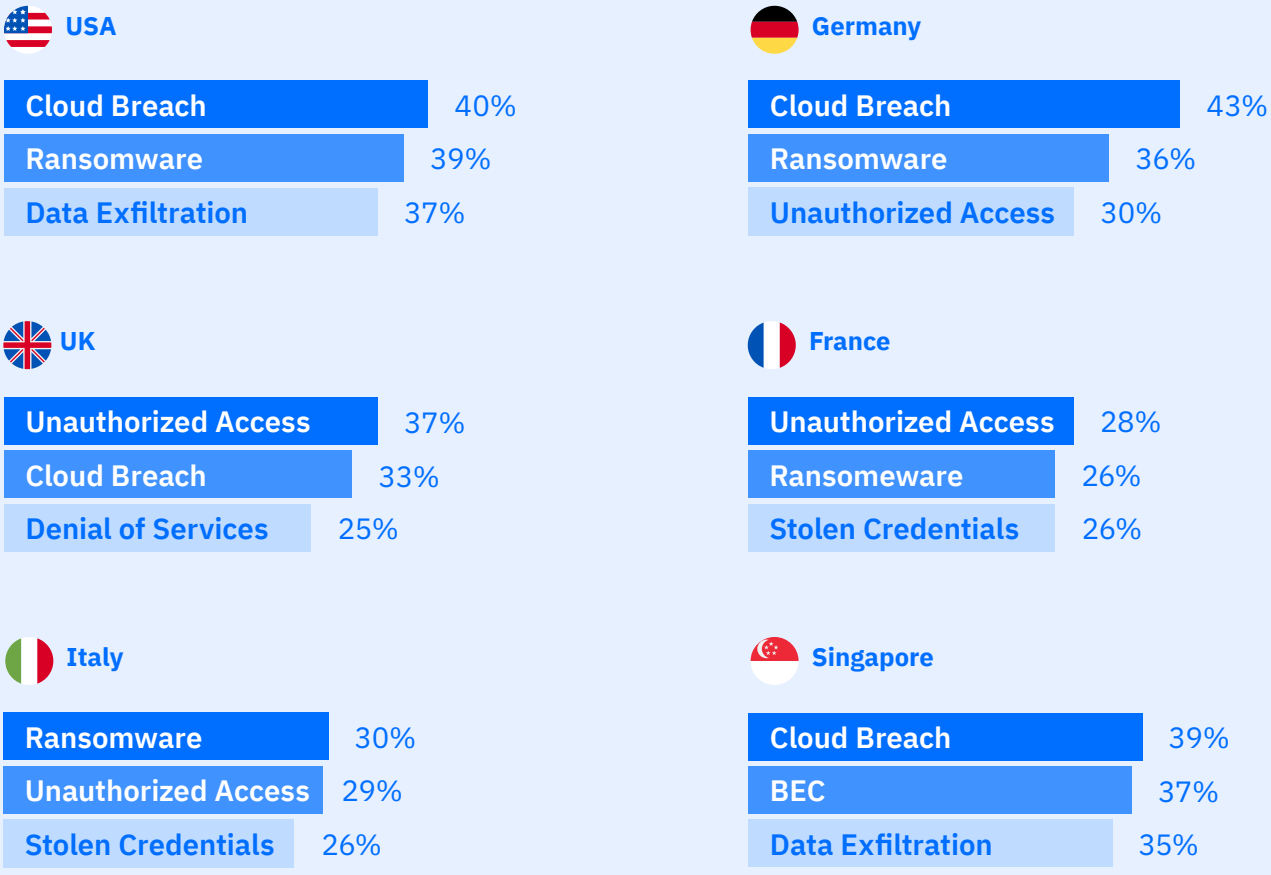
For organizations that do keep notifiable breaches quiet, the long-term costs of concealment, if discovered, are steep:

- Regulatory fines under GDPR, CCPA, and other laws can escalate rapidly when breach notification timelines are missed.
- Reputational damage multiplies when customers discover they were kept in the dark.
- Internal morale suffers when teams are told to suppress issues instead of addressing them.

Question

In the last 12 months, what type(s) of security breach(s) and/or incident(s) have you experienced, if any?

Top 3 breaches/cyber incidents by country



SECTION 6

Talent Gaps, Burnout, and the Increased Need for MDR

Cybersecurity isn't just a technological challenge. It requires people, even in this age of AI, to be successful. And right now, those people are under enormous strain. Security teams are being asked to do more than ever: protect an expanding attack surface, respond to faster, more sophisticated attacks, and maintain control over complex multi-cloud environments. In this high-pressure environment, critical tasks start slipping through the cracks, and vulnerabilities multiply.

A Widening Talent Gap and Escalating Burnout

Despite ongoing investments in training and recruitment, the overall perception is that the cybersecurity talent shortage is worsening. Half of the IT & security professionals surveyed report that the skills gap has widened in the last year. And it's not just about general staffing shortages but deep expertise in areas like threat hunting, AI-driven detection, and LOTL techniques. These specialized skills are harder to find, yet they are increasingly vital.

At the same time, the emotional toll on existing teams is increasing. In this year's survey, 49% of cybersecurity professionals report feeling burned out, primarily due to the constant pressure to monitor, triage, and respond to threats in real time. Burnout leads to higher error rates, lower vigilance, and, ultimately, higher turnover. In fact, nearly 4-in-10 professionals say they plan to look for a new role during the next year.

Increased turnover often means organizations fall behind on proactive initiatives like asset management, patching, and security posture hardening. Organizations shift into a reactive mode, perpetually fighting fires instead of building long-term resilience.

49%

of cybersecurity professionals report feeling burned out, primarily due to the constant pressure to monitor, triage, and respond to threats in real-time.

MDR: Not a Trend—A Long-Term Strategy

MDR isn't new, but its importance is accelerating. With attacks growing in speed and scale and internal teams unable to scale accordingly, MDR has become a foundational component of modern cybersecurity strategies.

The market is reflecting this urgency. According to Gartner®, the MDR market totaled $7.1B in 2024 and will reach $13.8B by 2029.[1] MDR provides depth, not duplication. These services give organizations access to 24x7 monitoring, forensic investigation, incident response, and expert threat hunting without the hiring costs and retention challenges of building an in-house SOC. By offloading these time- and skill-intensive tasks to external partners, internal teams are free to focus on strategic initiatives, from architecture improvements to compliance enforcement to proactive risk reduction.

As threats evolve and teams stretch to their limits, combining internal expertise with external MDR support is no longer a luxury. It's a requirement for sustaining long-term, high-performing security operations.

MDR isn't a temporary fix. It's a structural shift in how modern security operates.

> It expands the reach of internal teams without expanding headcount.

> It creates space for in-house security professionals to focus on what matters most.

> And it ensures that critical coverage doesn't stop when people get sick, vacation or take holidays off.

SECTION 7

The Layered Approach – Building True Cyber Resilience

Cybersecurity isn't a one-tool problem; it doesn't have a one-tool solution. In an environment where threats move faster, hide more effectively, and strike from more directions than ever, relying on a single tactic or technology is a recipe for failure. True protection demands a layered approach, where prevention, detection, and response work together seamlessly to stop threats before, during, and after they strike.

That's the essence of cyber resilience, which is not just about avoiding attacks but also about absorbing impact, adapting quickly, and recovering fully with minimal disruption to operations, finances, or reputation.

What Cyber Resilience Really Means

At its core, cyber resilience is about balance. It requires two tightly integrated layers:

Proactive Prevention and Hardening

This layer is the first line of defense. It includes strategies like shrinking the attack surface by removing unnecessary access for each user and restricting unused applications, and atypical but high-risk actions. The goal is to stop the attacker before an attack begins. New solutions like GravityZone PHASR (Proactive Hardening and Attack Surface Reduction) help organizations rapidly achieve these outcomes.

Reactive Detection and Response

This layer ensures that if something slips through, the organization can detect it in real-time, investigate it rapidly, and respond precisely. It also includes structured recovery: data restoration, continuity plans, and breach disclosure protocols. The goal: minimize impact and bounce back fast.

Together, these layers create overlapping coverage that adapts to modern threats, not just blocking what's known but detecting what's new and evolving.

The Data Behind the Strategy

The need for a layered approach is backed by real-world insight:

77%

of security teams say they need better threat visibility, a requirement that spans both proactive and reactive layers.

72%

express confidence in their ability to respond to threats, but only when prevention and detection are strong and aligned.

68%

agree that reducing unnecessary tools is essential, reinforcing attack surface management as a foundational element of resilience.

These survey results paint a clear signal that visibility, automation, and integration are essential across every stage of the security lifecycle.

CONCLUSION

Preparing for the Next Wave

The findings from the 2025 Bitdefender Cybersecurity Assessment leave little room for debate: cyber threats are becoming faster, stealthier, and more adaptive. Attackers are no longer breaking in; they're logging in and using trusted credentials and everyday tools to blend into legitimate environments. At the same time, complexity is mounting, talent is stretched thin, and burnout is compromising security vigilance across the board.

In this climate, proactive defense is no longer optional. Organizations that rely solely on detection and response are already behind. The path to cyber resilience begins earlier, with efforts to shrink the attack surface by reducing unnecessary access and risky actions within legitimate tools. These preventative strategies don't just improve security posture. They give defenders the time, visibility, and control they need to act with confidence.

Many organizations focused on best practices, take a layered, integrated approach:

They harden their environments proactively.

They detect and contain threats quickly.

They recover efficiently, minimizing operational and reputational damage.

To support this shift, Bitdefender offers a unified security platform, GravityZone, with capabilities like PHASR and Compliance Manager, combining automation, visibility, and out-of-the-box protection across identity, cloud, endpoint, and network layers. With a growing reliance on Managed Detection and Response (MDR), organizations pair internal teams with expert-driven, scalable defenses that adapt quickly. Looking forward, as AI reshapes the battlefield, the future belongs to those who blend intelligent automation, human expertise, and foundational security disciplines and tools. We believe 2025 is the year to enhance the power of reactive security by becoming increasingly proactive at the same time.

[1]Gartner, Forecast: Information Security, Worldwide, 2023-2029, 1Q25 Update, Shailendra Upadhyay et al., March 26, 2025.