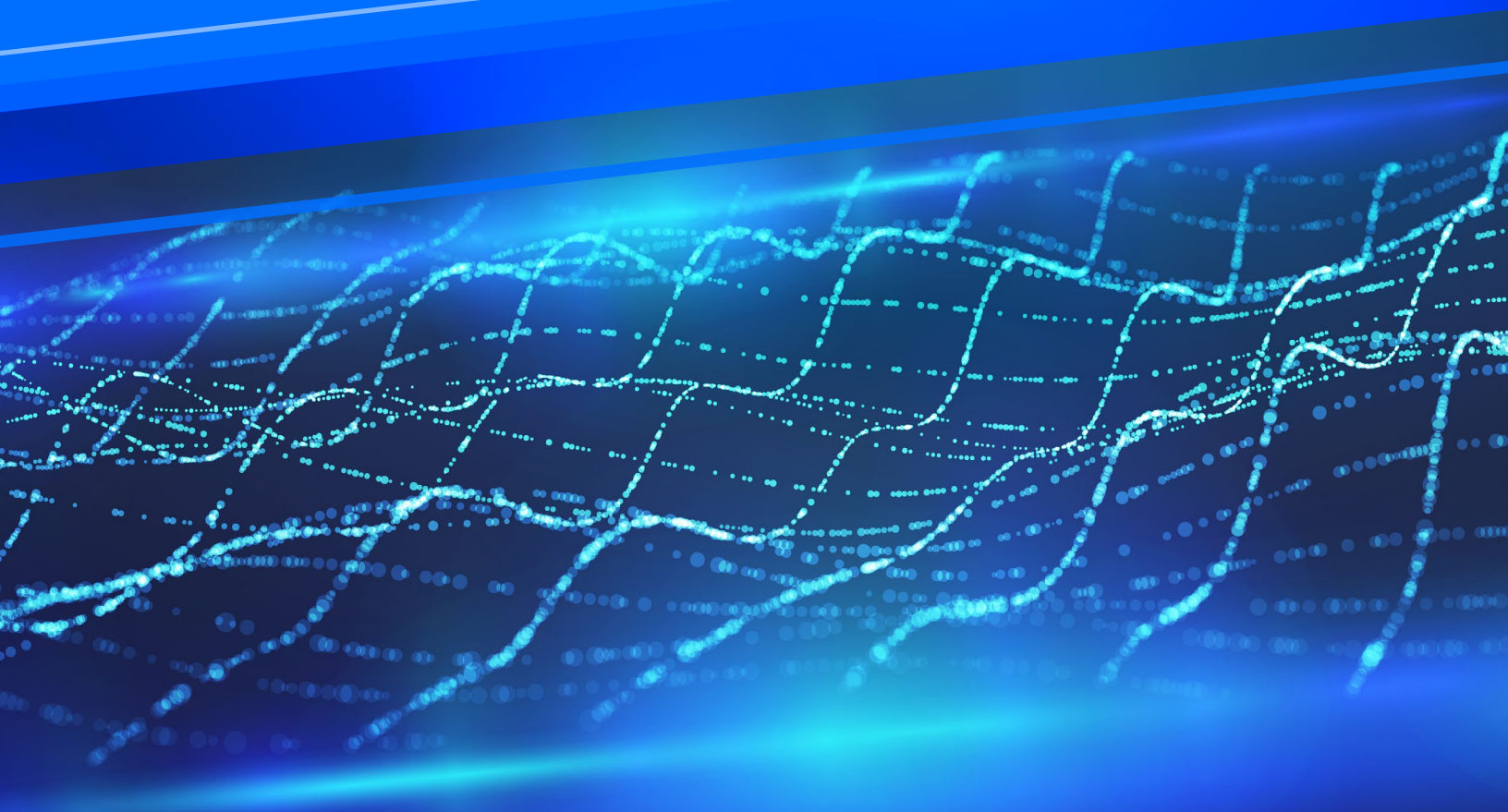
Bitdefender

Bitdefender Cybersecurity Assessment 2026

Global Insights from 1,200 IT & Cybersecurity Professionals



Key Findings at a Glance

Cybersecurity is a journey, not a destination. Along the way, there are checkpoints that reveal progress, challenges and opportunities.

These data points represent key findings from IT and cybersecurity professionals about today's journey: what keeps them up at night, what's holding them back, and where they see things heading.

BREACH DISCLOSURE

55.2%
were told to keep a breach quiet

THREATS & TOOLS

70.1%
are seeing more sophisticated phishing attacks

59%
have complaints about their EDR/XDR

AI

47.4%
lack visibility into employees' Shadow AI use

52.6%
believe AI is helping attackers more than defenders

OPERATIONS & COVERAGE

47.6%
cannot staff 24x7 coverage

61.5%
say the talent gap is driven by something other than a lack of candidates

48.7%
admit they struggle to balance security restrictions with productivity

COMPLIANCE & SOVEREIGNTY

76.1%
report data sovereignty is becoming a buying criterion

61.6%
say compliance requirements are overwhelming

Executive Summary

Three contradictions define cybersecurity in 2026. Organizations are more confident, yet breaches remain stubbornly common. AI threats are confirmed, but most teams can't see their own AI exposure. Common attack vectors are well understood but often neglected. Together, these gaps don't just represent blind spots. They show what happens when novelty over fundamentals drives the agenda: a fact that attackers are counting on.

This is Bitdefender's fourth annual Cybersecurity Assessment Report, based on independent research among 1,200 IT and cybersecurity professionals at multiple levels: management, from mid-level managers up to executive leadership, and security practitioners on the front line of cyber defense. Research participants are located across multiple continents and six countries: France, Germany, Italy, Singapore, the United Kingdom, and the United States.

The research reveals a startling gap between how leaders of organizations feel about their security posture, and what the people doing the work think about it. The gap between the two perspectives is one of the report's key findings. It turns out that executive leadership and managers are consistently more optimistic than the practitioners who implement their strategies.

Another key finding this year: demand for data sovereignty is driving buying decisions.

We also tracked several metrics year over year, and the trends are revealing. Breach cover-up rates have plateaued at stubbornly high levels despite new disclosure mandates. AI threats have completed the journey from hypothetical to confirmed. And when it comes to managing compliance, the struggle is real and relentless. So are frustrations around overly complicated security environments, along with concern about an expanding attack surface.

After analyzing the 2026 data, the strongest security postures may not belong to the organizations with the most tools or the loudest AI strategy, but to those that can reduce complexity, regain visibility, and focus on what actually prevents attacks.

SECTION 1

The Disclosure Gap

If you ask security leaders whether they've ever been told to keep a breach quiet (we did), more than half will say yes. That number hasn't meaningfully changed despite a wave of new mandatory disclosure regulations.

The persistence of this finding suggests something deeper than a policy gap. It points to a cultural norm, one that new regulations are testing but have not yet shifted.

55.2%

of respondents report being told to keep a breach confidential

The Number That Won't Move

In 2023, we first asked security professionals whether they'd been told to keep a breach confidential when they knew it should be reported. 42% said yes. In 2025, the number jumped to 57.6%. This year, across all 1,200 respondents, it's 55.2%. That plateau is arguably just as troubling as the initial spike.

The U.S. Securities and Exchange Commission (SEC) cybersecurity disclosure rules took effect in 2023. NIS2 began applying across Europe in 2024. DORA went live in early 2025. Yet the cover-up rate barely budged.

There are a few ways to interpret this. The charitable reading: disclosure mandates stopped the number from climbing higher. The less charitable reading: regulations are fighting an institutional reflex that's been decades in the making.

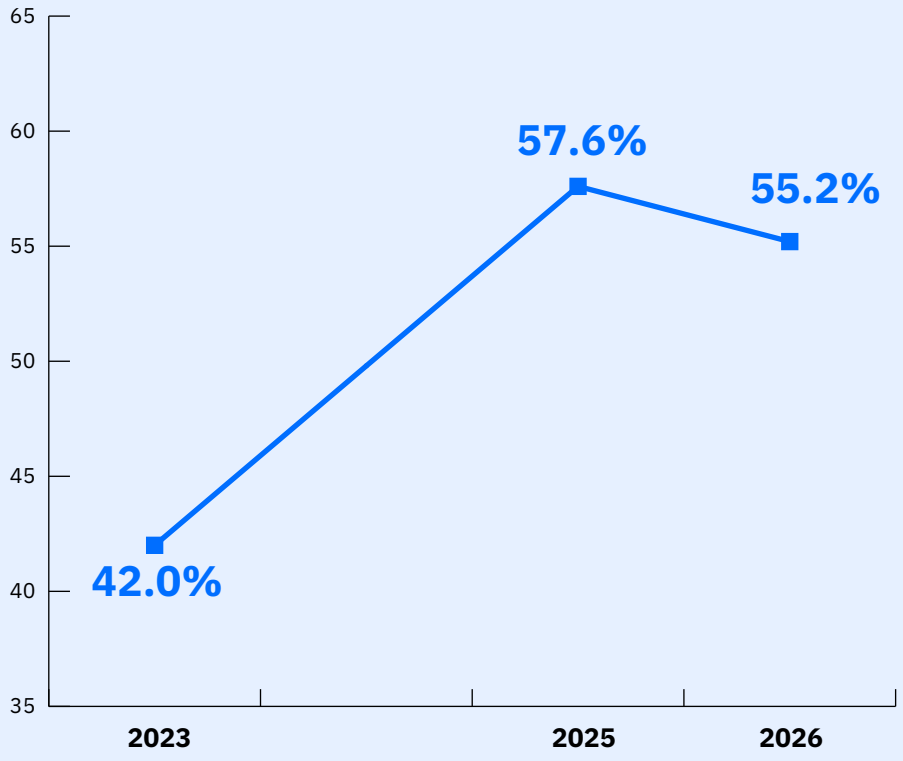
We lean toward a more nuanced reading:

The regulations have succeeded in establishing a baseline expectation of disclosure, and the plateau suggests organizations are internalizing these requirements. But the stubbornly high rate also reveals that cultural change lags behind policy change. Regulations set the floor, but changing behavior may require making disclosure feel less punishing. Or perhaps the opposite: making secrecy impossible to justify.

Survey Results

Security Professionals Told to Keep Breaches Confidential

Source: Bitdefender 2026 Cybersecurity Assessment

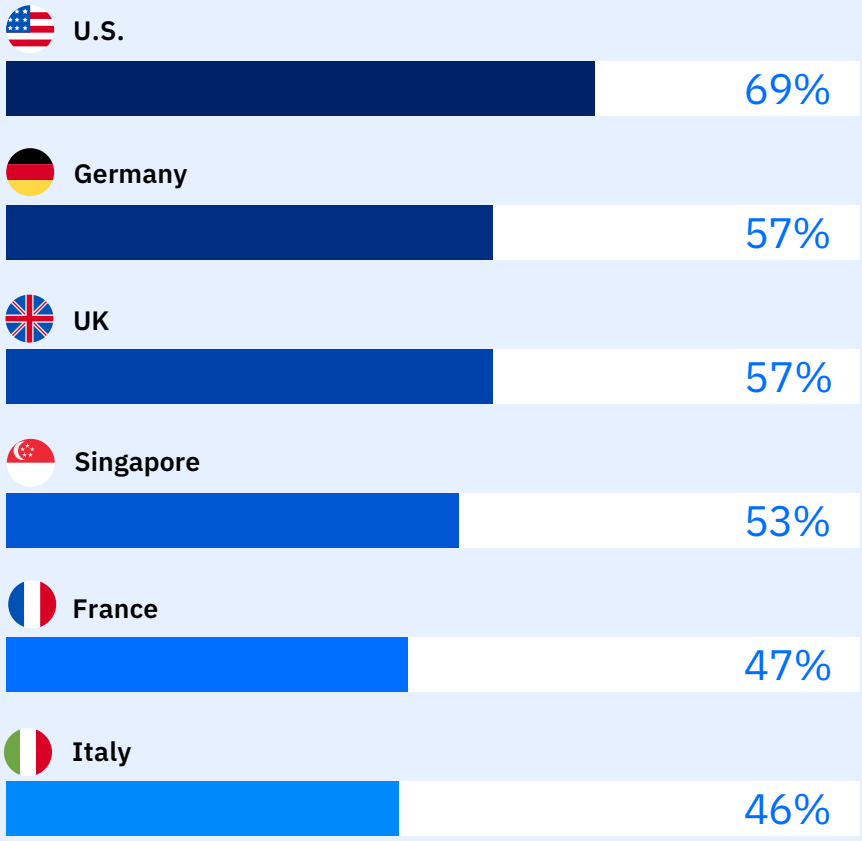


Survey Results

The Geography of Silence

% who say they were told to keep a breach confidential in the last 12 months

Source: Bitdefender 2026 Cybersecurity Assessment



The Breach Scorecard

What happened in the last 12 months? More than 50% of organizations say they experienced a "security breach or incident" in the last year. Here's what they mean:

41.8%
Unauthorized access to cloud infrastructure or applications

25.6%
Data encryption for ransom

22.2%
Data exfiltration for ransom

35.9%
BEC (business email compromise) resulting in financial or data loss

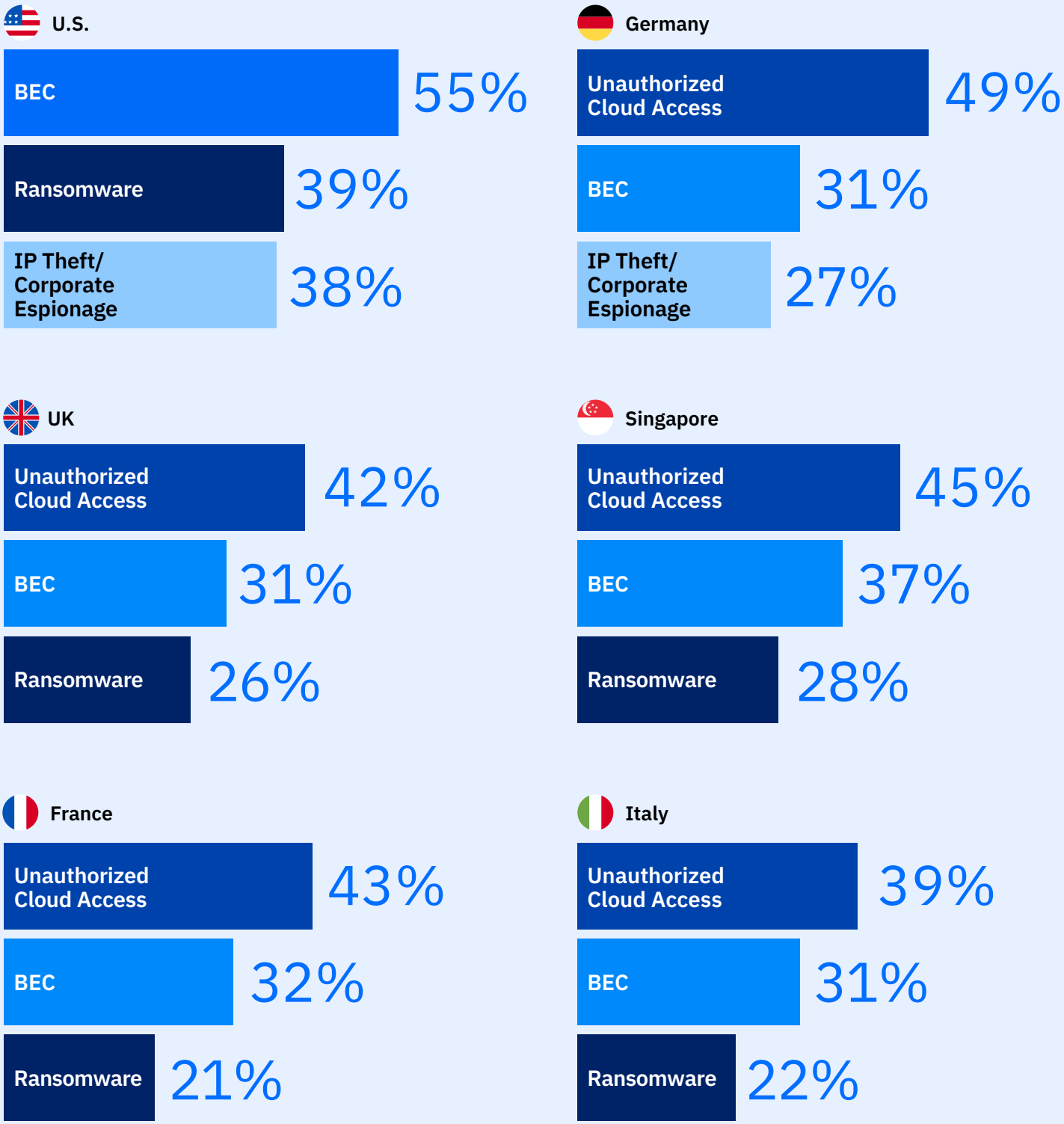
24.5%
Intellectual property theft or corporate espionage

20.3%
No incidents experienced

Survey Results

In the last 12 months, what are the top three security breaches or incidents you have experienced?

Source: Bitdefender 2026 Cybersecurity Assessment



SECTION 2

The AI Threat Comes Into Focus

The AI Era Has Arrived — And It's Armed.
AI-powered threats and cyber risk are arguably cybersecurity's hottest talking point in 2026. Three years ago, AI-powered cyberattacks were a conference talking point. Two years ago, they were a growing concern. Last year, organizations started reporting them. This year, our research reveals that AI-enabled cyberthreats are both confirmed and common. Amid all the AI hand-wringing, 53% of research respondents say AI is helping attackers more than defenders.

Plus, at least part of the AI risk is coming from inside the house. Many IT and cybersecurity professionals say the threat is already inside their environments as AI tools spread across the workplace. Yet, they are struggling to see it and secure it.

52.6%

say AI is helping attackers more than defenders

> *I don't think many organizations are really asking the right questions about AI yet. They have a lot of tools in the organization that have AI capabilities within them without really understanding the impact of those capabilities."*
>
> — Nicholas Jackson, Bitdefender Director of Cybersecurity Services

AI and Cybersecurity: Tracking the Trends

Bitdefender started using AI in its cybersecurity solutions in 2008 and holds dozens of AI-related patents, giving us deep experience in AI-enabled defense. But here's a trendline to consider: in the 2023 Cybersecurity Assessment Report, we didn't even ask about *AI-driven threats*. There wasn't enough signal to justify the question.

By 2024, we asked, and 96% of respondents told us they were concerned about AI threats.

In 2025, 63% said their organization had already experienced an attack they believed involved AI.

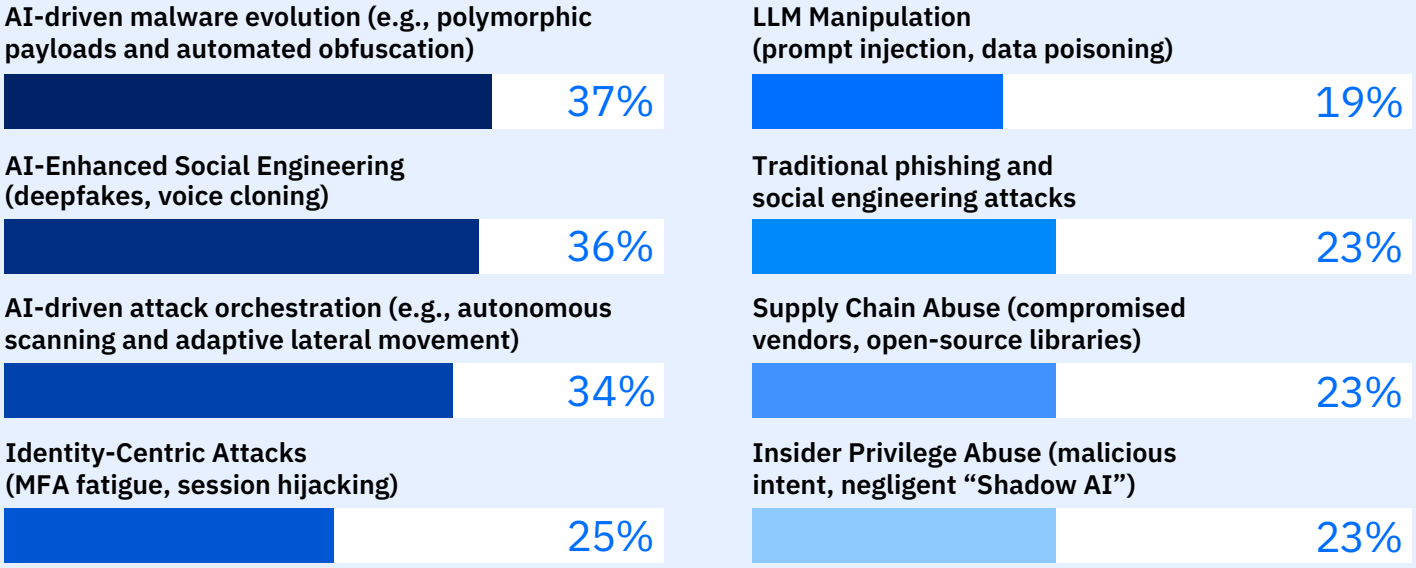
Now, in the 2026 Bitdefender Cybersecurity Assessment, IT and cybersecurity professionals told us the **top 3 attack methodologies** that threaten their organization ***all involve AI.***

To be sure, threat actors are increasingly leveraging AI. Bitdefender Labs recently documented how APT 36 is using an AI-driven development model; and our threat researchers also uncovered how AI elevated another threat actor from script kiddie to ransomware operator. However, to date, the AI attack apocalypse many feared has not materialized.

Survey Results

Top Attack Methodologies Threatening My Organization

Source: Bitdefender 2026 Cybersecurity Assessment

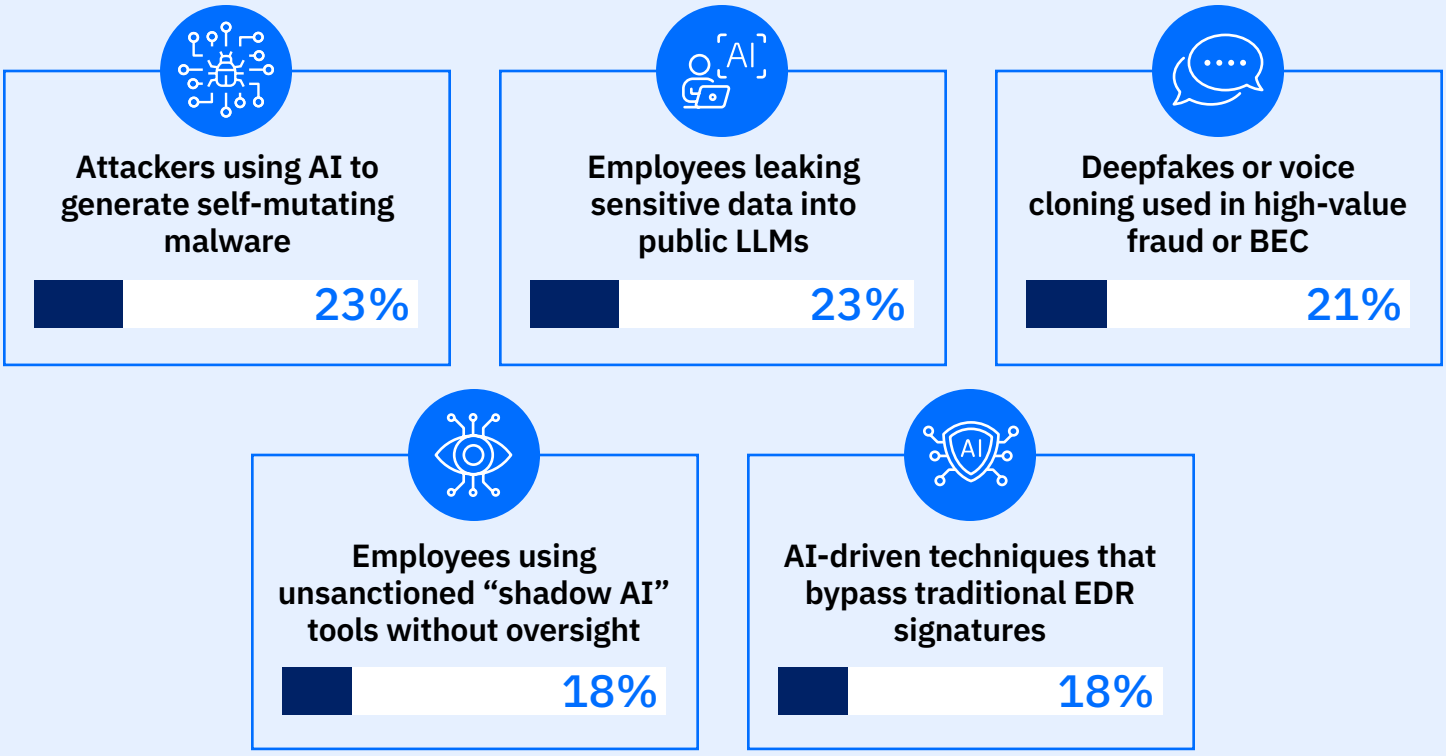


> *The top concern in this survey, AI-driven malware evolution, is the threat I'm most confident is overblown. We documented APT36 shipping AI-generated malware at a daily cadence. None of it was innovative. The threat is real, but it isn't a breakthrough in malware sophistication; it's an optimization of the mediocre. AI raised the attacker floor, not the ceiling."*
>
> — Bitdefender Technical Solutions Director Martin Zugec

Survey Results

AI Scenarios Viewed as "Extreme Risk"

Source: Bitdefender 2026 Cybersecurity Assessment



The Shadow AI Problem

While organizations are bracing for future AI-powered attacks from external threat actors, many may already be underestimating the AI-related risks emerging inside their own environments. In this year's research, only 51.8% of organizations claim full visibility into which AI tools their organization and its employees are using. The rest are flying partially blind (44.8%) or completely blind (2.5%).

This isn't a technology problem alone; it's also a governance vacuum.

Shadow AI may appear to be the new Shadow IT, but it's harder to detect, and the potential for data leakage is orders of magnitude greater.

Survey Results

Our Visibility Into LLMs and AI Tools Employees Currently Use

Source: Bitdefender 2026 Cybersecurity Assessment

Full visibility: We monitor and log all sanctioned and unsanctioned AI usage, including browser extensions and API calls.

Partial visibility: We track official enterprise LLMs, but lack visibility into individual "Shadow AI" subscriptions or personal accounts used for work.

No visibility: We do not currently track which AI tools or LLMs are being used by our workforce.

	Full Visibility	Partial Visibility	No Visibility
France	42%	56%	2%
Germany	52%	43%	4%
Italy	50%	45%	6%
Singapore	48%	50%	2%
UK	58%	40%	2%
U.S.	63%	37%	--

Where Does AI Go From Here?

We know AI is changing everything. For organizations, for defenders, for threat actors. Nearly six in ten IT and security professionals (59.2%) say their organization has experienced social engineering attacks they believe involve AI; more than five in ten (55.7%) say their organization has experienced malware-based attacks that involve AI. Seven in ten (70.1%) organizations say they are seeing more sophisticated phishing attacks powered by AI.

Looking toward the future of AI-related threats, very few now believe that AI attacks are “mostly industry hype” (17.5%). The pool of skeptics is shrinking. However, the jury is still deliberating on how far things will go.

Today’s phishing emails use AI-generated content and correct regional grammar to evade basic filters, with engagement rates rivaling legitimate marketing campaigns. Effective protection requires post-delivery visibility and rapid response — legacy approaches simply can’t keep up.”

— Brian Byrne,
Bitdefender VP of Email Security

The pool of skeptics is shrinking.

17.5%

of security professionals now believe that AI attacks are “mostly industry hype”

Survey Results

The Technical Novelty of AI-Driven Threats

Source: Bitdefender 2026 Cybersecurity Assessment

AI is a force multiplier for the current, full attack chain.
AI accelerates every stage.

AI is a force multiplier for social engineering, but the backend malware and exploit methods remain traditional.

AI is a revolutionary technical threat.
AI creates new, AI-native malware and autonomous attack chains.

SECTION 3

The Cybersecurity Optimism Gap

Cybersecurity is not exactly known for its optimism. Yet this edition of the Bitdefender Cybersecurity Assessment Report reveals a consistent trend across geographies: leaders tend to see the state of cybersecurity more positively than the frontline practitioners responsible for implementing and managing security controls day to day.

On average, IT and security leaders rated their organization's cybersecurity posture and ability to handle security challenges 8% higher than frontline employees did.

8%

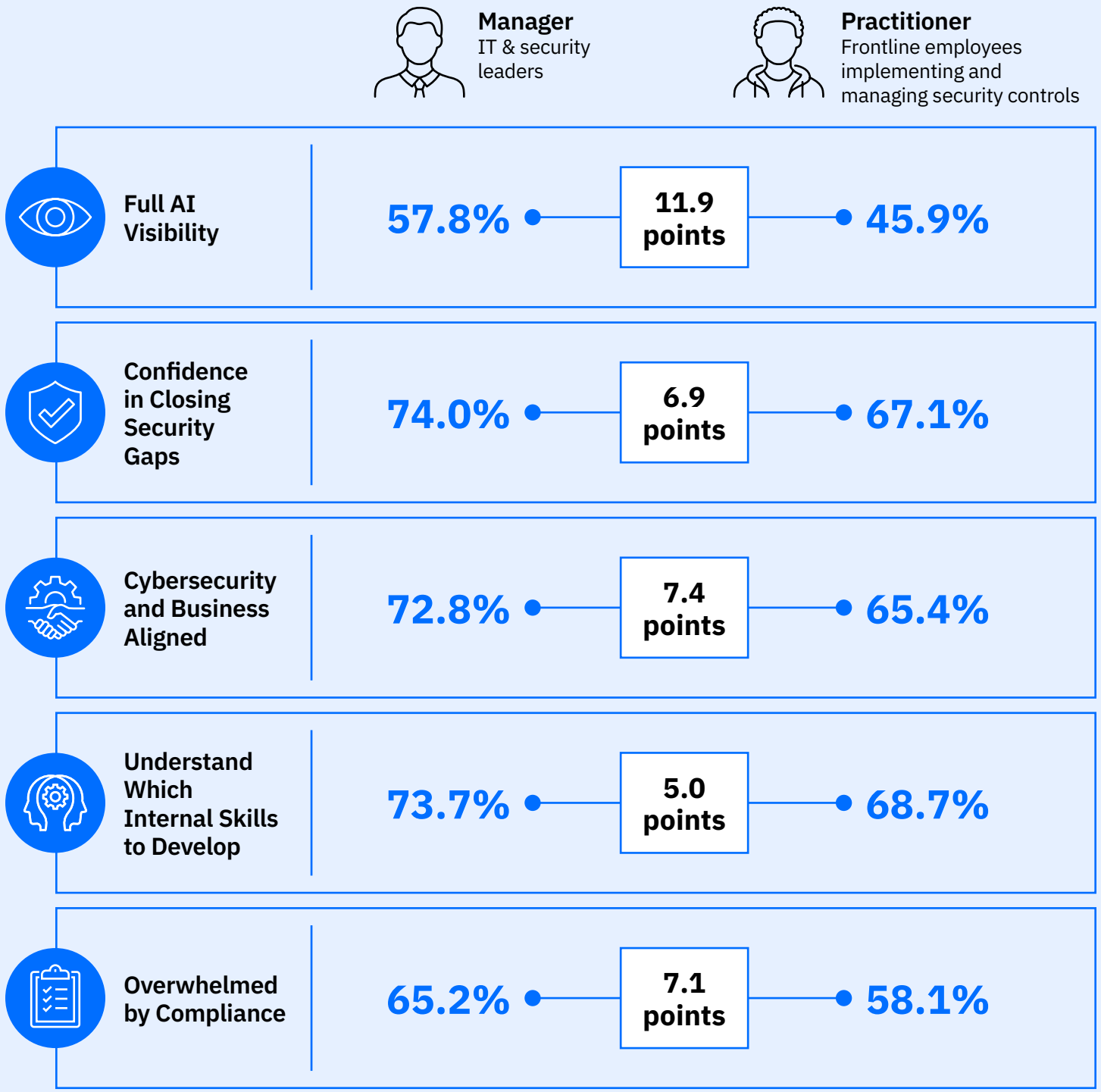
on average, how much higher IT & security leaders rate their security posture vs. front line employees

This perception gap appears across multiple areas, from visibility into AI usage and confidence in closing security gaps to business alignment, workforce readiness, and compliance management. While leaders may see progress and strategic momentum, practitioners are often closer to the operational realities: understaffed teams, alert fatigue, expanding attack surfaces, and the growing complexity introduced by AI-enabled threats.

The 2026 findings suggest that cybersecurity leaders and practitioners are not necessarily disagreeing about the threats themselves — they are experiencing them from different vantage points. Bridging that gap may become just as important as closing technical security gaps in the years ahead.

Manager vs. Practitioner Perception Gap

Source: Bitdefender 2026 Cybersecurity Assessment



SECTION 4

The American Paradox

Overconfident, Under-Resourced

U.S. respondents are simultaneously the most strained and the most confident in our entire dataset. They report higher rates of breach concealment, more AI-driven attacks, and greater tool complexity. And yet they also report higher confidence in their security posture, stronger vendor relationships, and greater willingness to invest. The data doesn't resolve this contradiction. It just measures it.

18.7%

U.S. control bypass rate above the global average

The U.S. strain metrics are consistently the highest in the survey. 69.7% of U.S. respondents say AI gives attackers the advantage (vs 52.6% overall). 61.7% struggle to manage alert volumes (vs 44.7% globally). 66.7% report that security controls are regularly bypassed (vs 48.0%). And 63.2% say they lack 24×7 coverage (vs 47.6%), a key driver for increasing MDR (managed detection and response) adoption.

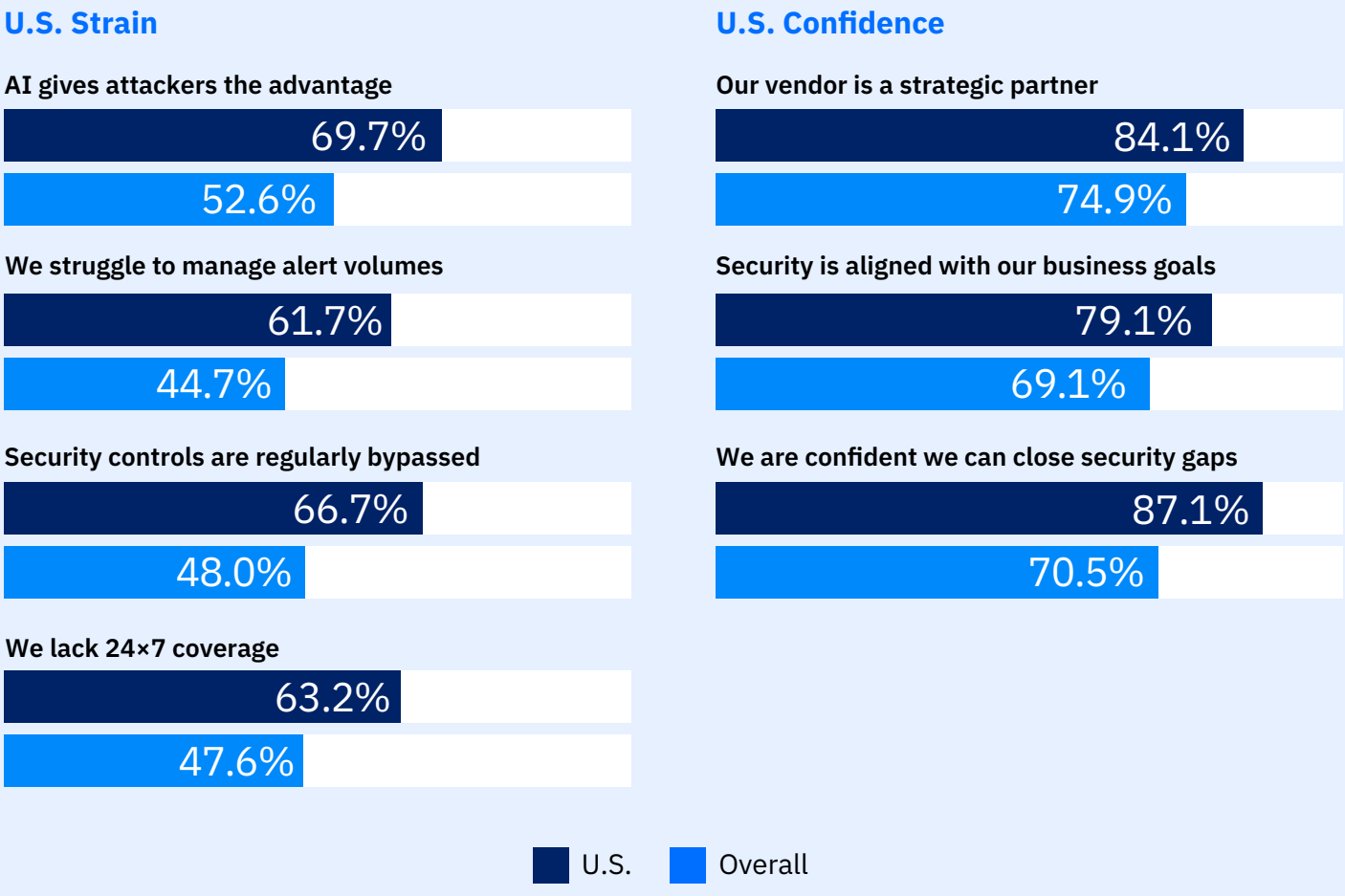
Every one of those figures is 15 to 20 percentage points above the global average. That's not noise. It's a signal.

But flip to the confidence side and the picture inverts. 84.1% of US respondents view their vendor as a strategic partner (vs 74.9% overall). 78.1% say security is aligned with business goals (vs 69.1%). 87.1% express confidence they can close security gaps (vs 70.5%). U.S. organizations are heavily invested and overstretched. The same cultural factors that drive higher spending also drive higher self-assessment. Both can be true simultaneously.

Survey Results

U.S. respondents are the most strained and the most confident in our entire dataset

Source: Bitdefender 2026 Cybersecurity Assessment



SECTION 5

The New Question Isn't Where—It's Who

For years, organizations focused on where their data was stored. Today, the greater concern is who can access it, process it, and claim jurisdiction over it. As sovereignty requirements become more prominent, security and IT leaders are factoring these considerations into purchasing decisions.

76%

say data sovereignty is increasingly important in purchasing decisions

From Checkbox to Deal Breaker

The sovereignty finding cuts across every region, though the intensity varies. U.S. respondents lead switching intent at 87.1%, followed by the UK at 85.0% and Germany at 77.0%. Even at the lower end, France (62.5%) and Italy (68.5%) show majority willingness to change vendors.

The drivers are layered. Regulatory requirements, geopolitical tensions, and concerns about reliance on foreign technology all play a part.

What's notable is the tiny gap between "sovereignty matters" (77%) and "we'd switch over it" (76.1%). Those numbers are almost identical, which suggests that for most respondents, sovereignty isn't just a nice-to-have. It's already a decision criterion.

A 2026 IDC Market Note detailed how this is working in practice.

"Questions have moved from 'Where is the platform hosted?' to 'Who governs it, and from where, and which foreign government can legally impose its will on providers of our critical technology?'"

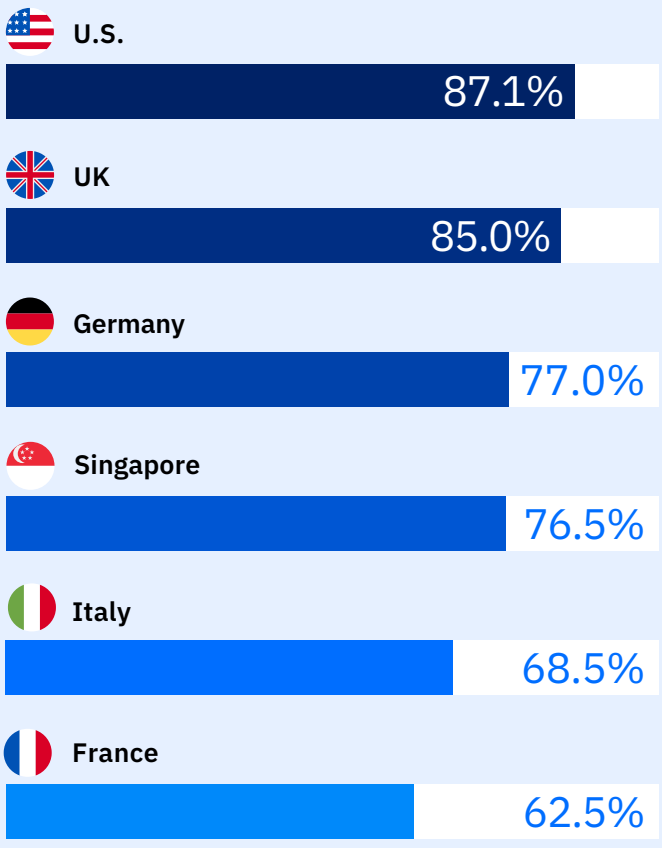
This type of organizational soul-searching is creating demand for solutions that deliver security, compliance, and sovereignty by design.

"Most recently, in October 2025, OVHcloud and Romania-based cybersecurity vendor Bitdefender announced the launch of a sovereign cybersecurity platform hosted on OVHcloud's SecNumCloud-certified service," IDC noted[1]

Survey Results

Likely to Switch Vendor Over Data Sovereignty

Source: Bitdefender 2026 Cybersecurity Assessment



Implication
Audit your vendor contracts for data residency, jurisdiction, and sub-processor clauses. If your vendor can't answer these questions clearly, look for a vendor that can.

[1] IDC Market Note: Bitdefender & OVHcloud Join Forces with European Sovereign Cybersecurity Platform Offering (Doc #EUR254251926, February 2026)

SECTION 6

Lost in AI's Glare

Bitdefender Labs analyzed more than 700,000 cyber incidents and found that 84% of major attacks leverage Living off the Land (LOTL) techniques. Yet only 20.5% of survey respondents rank LOTL as a top-three threat. That 63.5 percentage-point gap between real-world prevalence and perceived importance is the single largest disconnect in this report.

84%

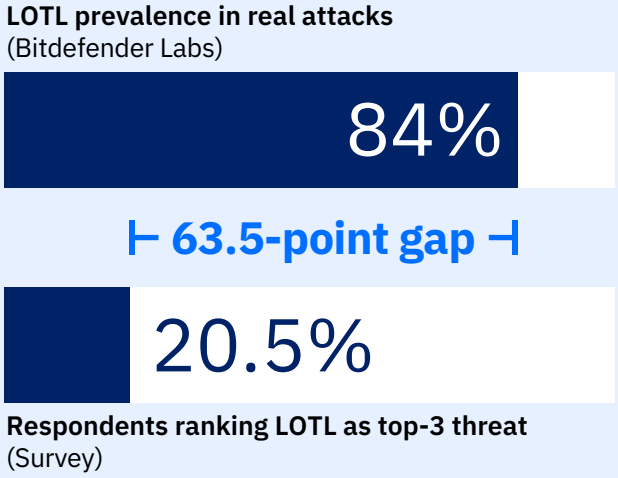
of major attacks leverage Living off the Land techniques

The 84% vs. 20% Problem

What attackers actually use vs. what defenders worry about

Source: Bitdefender 2026 Cybersecurity Assessment

Implication
Invest in prevention-first architecture that detects malicious behavioral patterns regardless of the tools being used. LOTL attacks evade signature-based defenses by design.



Living off the Land attacks use tools already present in the target environment, like PowerShell, WMI, RDP, and other legitimate admin utilities. They don't trigger malware signatures because they aren't malware. Attacker actions look like normal admin activity, because they use the same tools.

This points to a long-term security problem that more organizations are addressing through prevention, which helps stop attacks even when they look like normal activity.

In this year's research, AI-driven malware evolution (37.5%) and AI-enhanced social engineering (36.2%) were the dominant concerns. The industry isn't wrong to worry about AI threats, but the AI narrative is crowding out attention to the techniques attackers use most. It's the cybersecurity equivalent of worrying about sharks while swimming in a river full of hippos.

> *"For years now, the security conversation has revolved around detection and response. These continue to be critical capabilities. But our team asked, 'What if we stop giving attackers room to move around in the first place?' This is the simple and fundamental premise that led us to build something designed not just to react to threats, but to reduce the likelihood that the threat will exist."*
>
> — Daniel Daraban,
> Bitdefender Vice President of Products

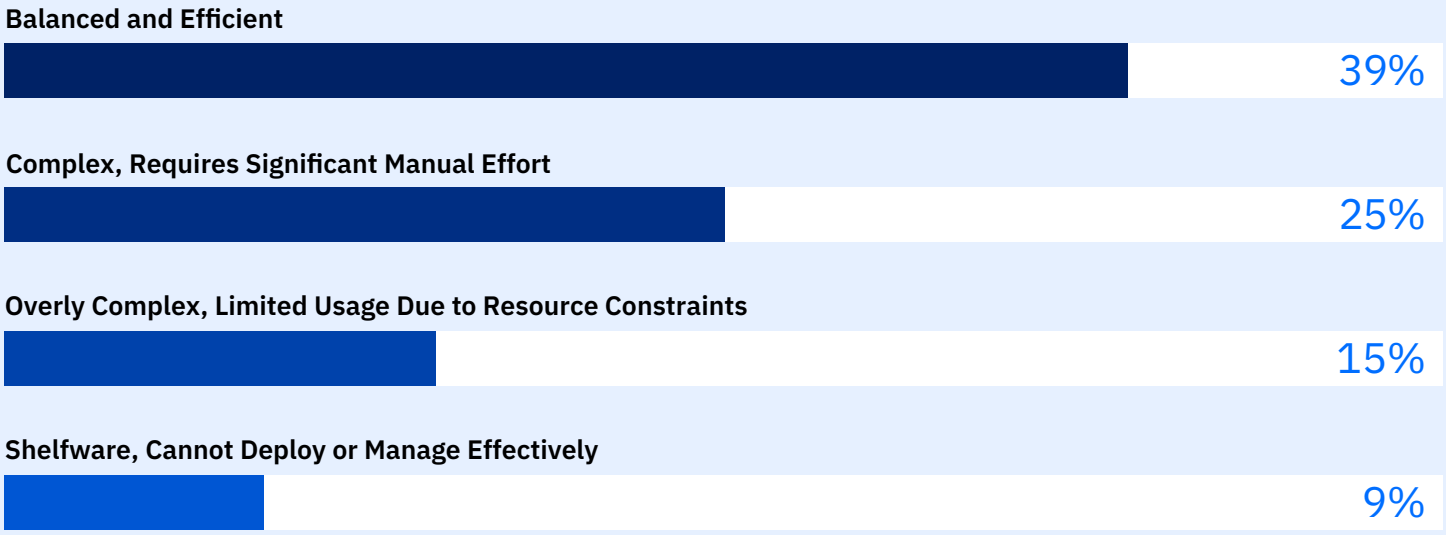
The Complexity Tax

The LOTL blind spot is partly a symptom of a broader problem: tool complexity. Only 39% of respondents describe their current EDR/XDR as ‘well balanced.’ In fact, a full 40% say their EDR/XDR is so complex “it takes significant manual effort” or that it “cannot be fully implemented.”

Survey Results

How We View Our Current EDR/XDR Platform

Source: Bitdefender 2026 Cybersecurity Assessment



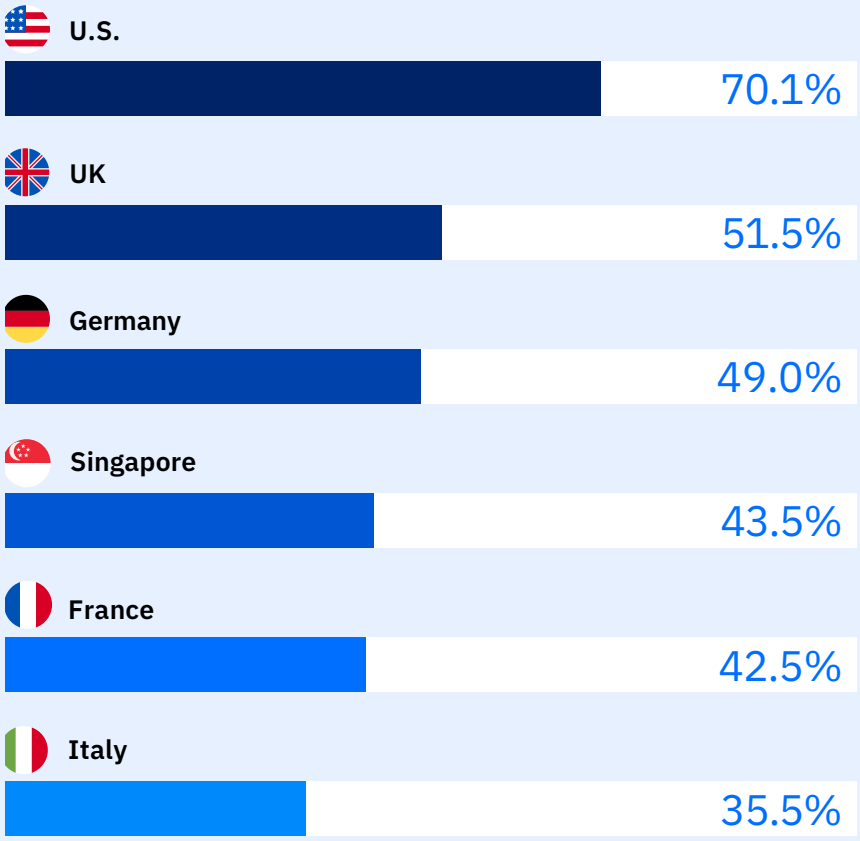
For lean security teams, the answer isn’t adding another point solution. It’s consolidating to fewer, better-integrated tools that cover the full OS spectrum from a single console, and using AI to proactively reduce the number of openings attackers can exploit.

The attack surface is both complex and expanding. A full 57.0% of respondents agree they need to reduce their attack surface and they want to do so by disabling unnecessary or risky tools, but also worry they could disrupt business operations if they do.

Survey Results

“We struggle to balance security restrictions with employee productivity.”

Source: Bitdefender 2026 Cybersecurity Assessment



Overall, 38.0% say the high overhead of maintaining hardening rules and exceptions is a barrier to shrinking the attack surface, with 34.6% citing resource constraints and nearly that many (33.8%) reporting that visibility gaps are a barrier.

The result is an environment where organizations know they have too many tools and should reduce them, yet feel unable to act successfully on either insight.

57.0%

of respondents agree they need to reduce their attack surface, but

38.0%

say the high overhead of maintaining hardening rules and exceptions is a barrier to shrinking the attack surface.

SECTION 7

When Compliance Becomes the Goal

When 56% of respondents describe their organization's compliance efforts as 'primarily a checkbox exercise,' it's worth asking what exactly all that compliance spending is buying. The real measure of security posture isn't whether you pass audits. It's whether you stop attacks. Independent evaluations, not compliance certifications, tell that story.

56%

describe compliance efforts as primarily a checkbox exercise

The Checkbox Paradox

Compliance data points from the 2026 Bitdefender Cybersecurity Assessment create a paradox that should unsettle anyone writing checks to auditors.

Most (62%) IT and cybersecurity professionals say keeping up with compliance is overwhelming, and 61% say it's more complicated than it needs to be because of manual research and documentation. And 56% characterize their efforts as primarily checkbox-driven. These numbers describe an industry that is spending enormous resources on compliance and getting questionable security value in return.

The correlation with control bypass rates is troubling. 48.0% of all respondents report that security controls are regularly bypassed, at least temporarily, for business purposes. In the US, 66.7% say security controls are bypassed.

When organizations focus on passing audits rather than preventing attacks, the controls they implement tend to be audit-shaped rather than threat-shaped. The way out isn't more compliance. It's building a security posture measured by independent third-party tests that measure actual prevention capability against real attack techniques, not whether a policy document exists. Small and mid-sized teams are also relying more heavily on compliance management tools to simplify the compliance process.

62%

of IT and cybersecurity professionals say compliance is overwhelming

56%

describe efforts as primarily a checkbox

48%

report controls are regularly bypassed

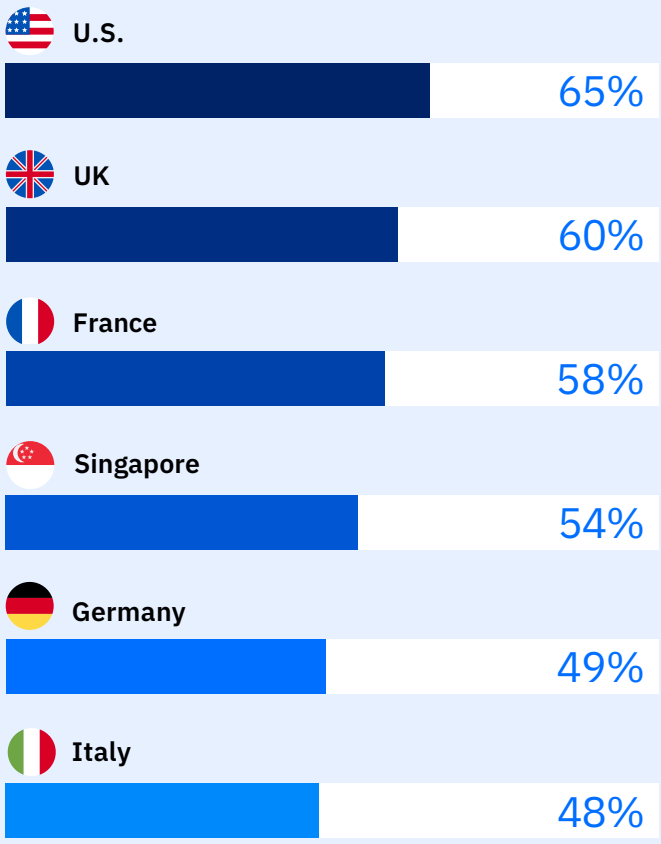
66.7%

of U.S. respondents report that security controls are regularly bypassed — 18.7% above the global average.

Survey Results

Security Strategy Driven by Checkbox Compliance Instead of Actual Threat Prevention

Source: Bitdefender 2026 Cybersecurity Assessment



Implication

Consider cybersecurity platforms with built-in compliance monitoring to simplify evidence collection, automate compliance tracking, and streamline workflows to ensure audit readiness.

SECTION 8

Skills Gap Impact and Diagnosis

The cybersecurity talent crisis isn't new. But in this year's research, IT and cybersecurity professionals pointed to a multi-headed mix of causes behind the shortage at their organization.

48%

say they lack 24×7 security coverage

Survey Results

The Primary Cause of the Skills Shortage at My Organization

Source: Bitdefender 2026 Cybersecurity Assessment

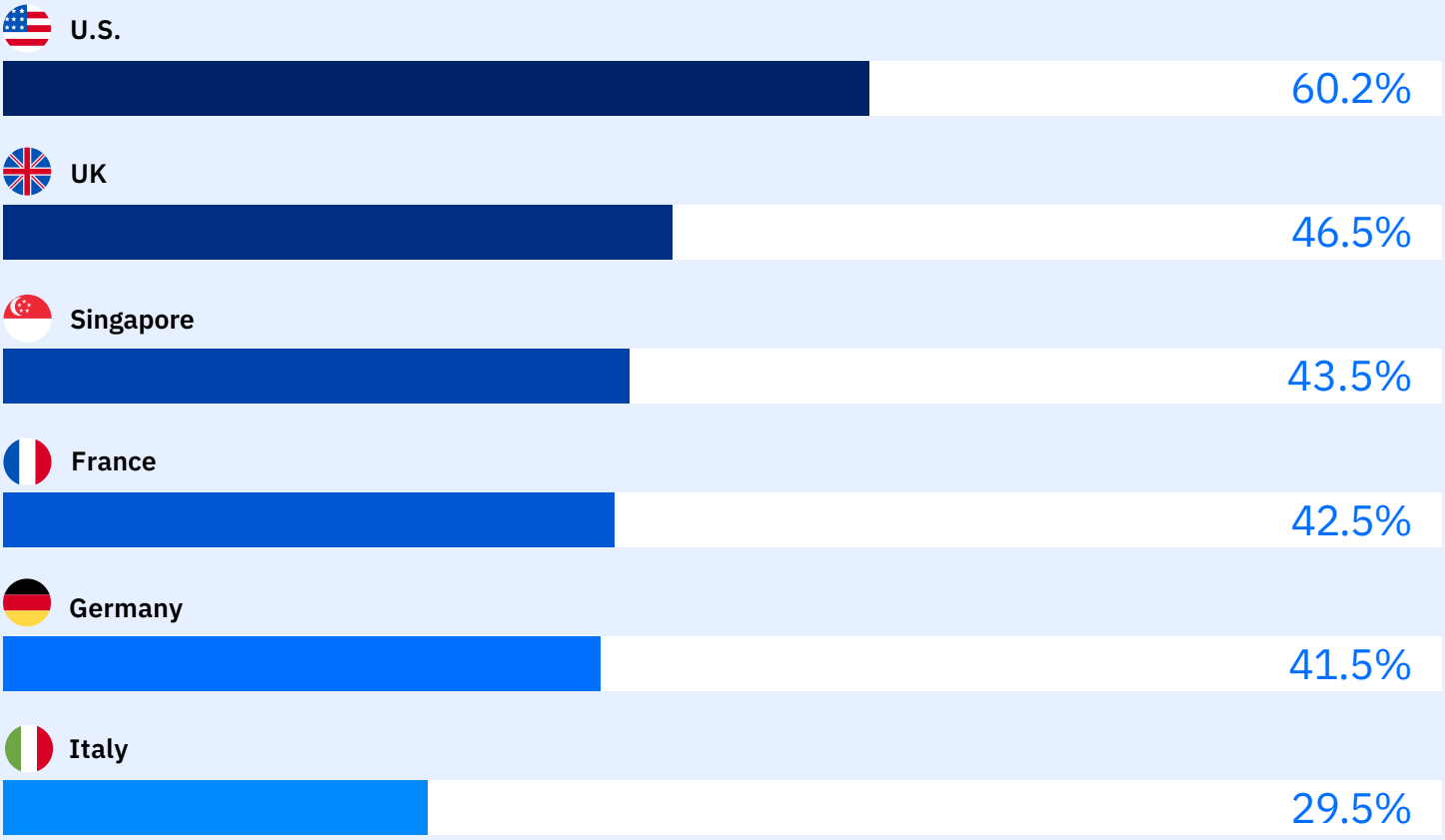
While IT and cybersecurity professionals cite multiple causes for the skills shortage, leadership is now pursuing help to fill gaps that hiring alone can't close.

This increasingly appears as a two-pronged approach: platform consolidation and managed detection and response (MDR), which helps protect the organization 24x7. Lean teams are pursuing fewer, better tools that cover every OS from a single console, not more products that each require dedicated headcount (and time) to operate. Too much technology remains untapped within IT environments. This is linked to a lack of time and expertise.

Survey Results

We lack the time or expertise to fully utilize our current security tools

Source: Bitdefender 2026 Cybersecurity Assessment



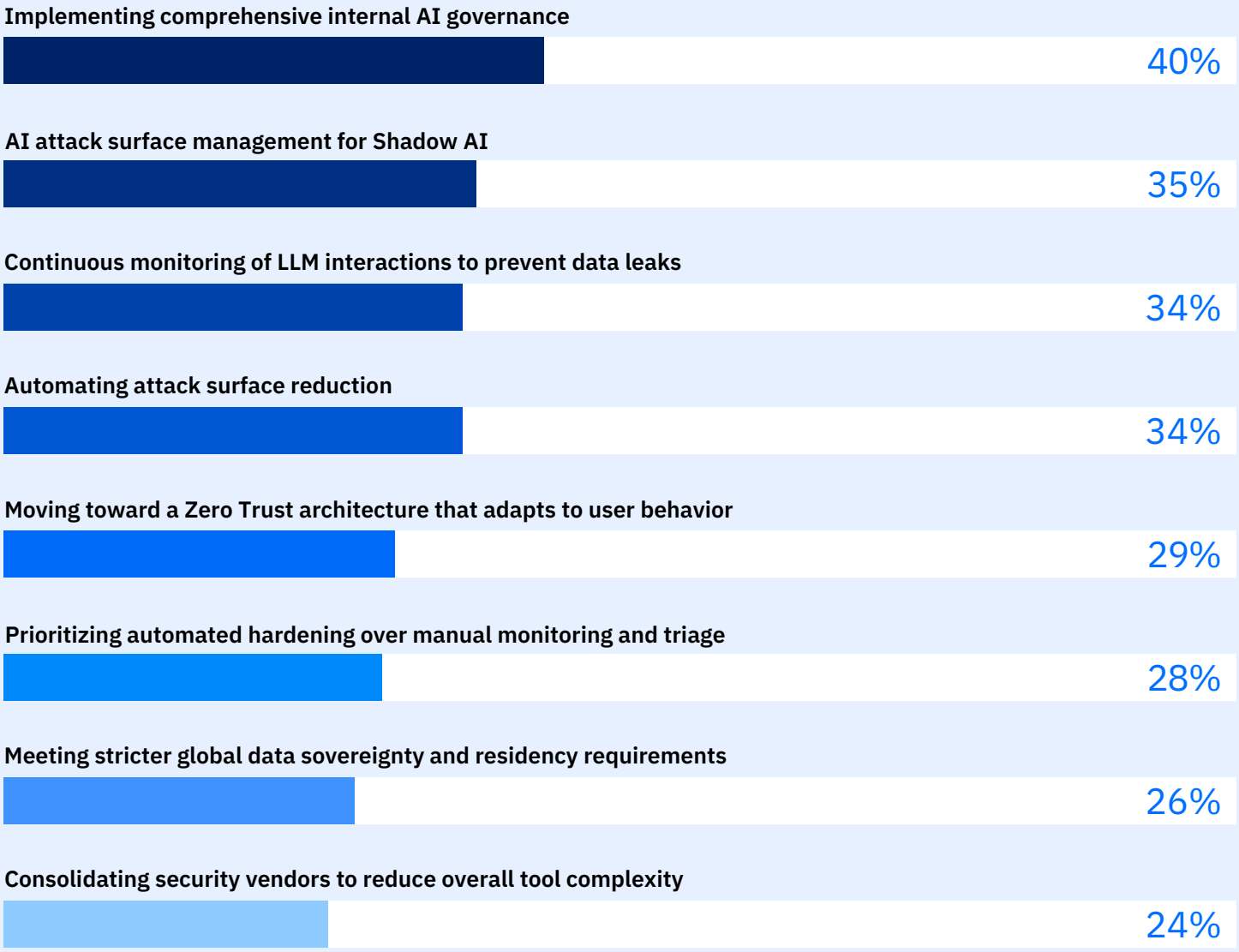
Forward Focus: Top Initiatives

When asked about top security initiatives for the next 12 months, AI leads the pack, reflecting the maturation of AI threats documented throughout this report.

Survey Results

Our Top 3 Cybersecurity Initiatives Over the Next 12 Months

Source: Bitdefender 2026 Cybersecurity Assessment



CONCLUSION

Looking Ahead

The cybersecurity industry is not standing still. Organizations are investing more, modernizing faster, consolidating tools, adopting AI, and placing greater emphasis on resilience, sovereignty, and operational efficiency. In many ways, the findings in this report reflect an industry actively adapting to fast-changing threats.

But the data also reveals a deeper tension. Complexity continues to outpace simplicity. Compliance often overshadows prevention. AI is reshaping both offense and defense. And throughout the report, one theme appears repeatedly: the gap between perception and operational reality. Leaders and practitioners see risk differently. Organizations understand many of the threats they face, yet often struggle to prioritize the ones causing the most damage.

The organizations best positioned for the future will not necessarily be the ones with the most tools or largest budgets. They will be the organizations that reduce complexity, shrink their attack surface, align security with operational reality, and focus relentlessly on outcomes over optics.

The challenge ahead is not simply defending against tomorrow's threats. It is building security programs that can adapt to constant change without losing sight of the fundamentals that still matter most.

About Bitdefender

Bitdefender is trusted and tested.

Trusted by millions of consumers, businesses, and government organizations, Bitdefender protects digital environments against the world's most advanced cyber threats.

Bitdefender is also tested and validated as an industry leader, winning five "Product of the Year" awards from 2013 to 2024, a feat unmatched by any other vendor evaluated by AV-Comparatives. Bitdefender also received a dual recognition from Gartner®: a Visionary in the 2026 Gartner Magic Quadrant™ for Endpoint Protection Platforms and a Customers' Choice in Gartner Peer Insights™ Voice of the Customer for EPPs.

The company is also frequently recognized by IDC.

Bitdefender's unified security platform combines deep threat intelligence, AI-powered protection, attack surface reduction, extended detection and response (XDR), and managed detection and response (MDR) capabilities into a single security ecosystem designed to simplify cybersecurity operations while improving resilience.

With decades of security innovation, hundreds of technology patents, and one of the world's most respected cybersecurity research organizations, Bitdefender continues to help organizations reduce complexity, strengthen defenses, and build cyber resilience in an increasingly unpredictable threat landscape.

You can learn more here:
www.bitdefender.com/business

"The expanding attack surface, the rapid proliferation of AI-powered threats, and persistent operational pressures are forcing organizations to rethink how they approach security from the ground up. The findings in this report make clear that modern security strategies must go beyond reactive defenses to continuously reduce risk, govern AI adoption, and ensure compliance across an environment where adversaries are faster, more adaptive, and increasingly automated."

— Andrei Florescu
President and General Manager of
Bitdefender Business Solutions Group

Why Millions Trust Bitdefender

Bitdefender protects millions across 170+ countries, combining deep security expertise with cutting-edge AI innovation and a commitment to fighting cybercrime alongside global law enforcement.

50B+
threats blocked every year

$1.6B+
in ransom payments prevented

15+
years of AI-driven security innovation

30+
free ransomware decryptor tools released to the public

580+
patents filed, including breakthroughs in machine learning and advanced threat detection

30+
global partnerships with law enforcement to disrupt ransomware operations

50%+
over half of Bitdefender employees dedicated to research and development

Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy, digital identity, and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence. Its technology is licensed by more than 180 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world. For more information, visit **bitdefender.com**.

Trusted. Always.

Methodology and Disclaimer

The survey and analysis took place from April 2026 through June 2026. The study surveyed 1,200 IT and cybersecurity professionals across six countries: France, Germany, Italy, Singapore, the United Kingdom, and the United States. Respondents included management-level professionals (from mid-level managers to executive leadership) and frontline security practitioners.

The findings, statistics, and conclusions presented in this report reflect the perceptions, experiences, and opinions of survey respondents at the time of the research. They do not constitute statements of fact regarding any specific organization, product, or service, nor do they represent audited, verified, or independently validated data about actual security incidents, breach disclosures, or compliance practices of any identified entity.

All survey responses were collected anonymously. No individual respondent or their employing organization can be identified from the data presented. Aggregated results are provided for informational and educational purposes only and should not be construed as legal, compliance, or professional advice.

Bitdefender makes no warranties, express or implied, regarding the accuracy, completeness, or reliability of the information contained herein. Readers are encouraged to conduct their own independent analysis and consult qualified professionals before making any decisions based on the content of this report.

Third-party references, including citations to analyst reports, industry publications, and external research, are provided for context and do not imply endorsement by, or affiliation with, the referenced parties unless explicitly stated.