Bitdefender BUSINESS SOLUTIONS | Cybersecurity Built For Resilience

WHITEPAPER April 2023

Bitdefender 2023 Cybersecurity Assessment

Report shows IT and security leaders instructed to keep data breaches confidential despite obligation to report

Summary

Cybersecurity teams are under immense pressure. Phishing and ransomware attacks are on the rise and they are continuously becoming more sophisticated with over half of companies having experienced some form of cyber threat in the past 12 months. What's more, over half of these companies have experienced a data breach or data leak in the same time period.

It's fair to say that not one organization is immune from cyber attacks. The costs can be daunting, no matter the company's size. In 2022, the global average cost per data breach increased by over two percent to $4.35 million.

The pressure of unpredictable threats is taking its toll. Over 40% of cybersecurity teams have been told to keep a security breach confidential when it should have been reported, and almost 60% admitted to working on weekends. In the United States, these numbers are even higher — 71% and 80%, respectively. And what about the cybersecurity tools meant to help? Those don't live up to the marketing hype, stated over half of the organizations surveyed.

The situation isn't likely to improve over the next 12 months, as widespread layoffs and a slowdown in spending within the tech industry is on everyone's mind. History has shown that a struggling economy often leads to heightened cybersecurity risks as criminals increase activity. As budgets tighten, it's essential for business and technology leaders to realize the detriment a security breach could cause and focus on investing in security solutions designed to ease the burden on their already struggling teams.

The question remains; are IT and cybersecurity leaders prepared for the potential threats which lie ahead? Bitdefender commissioned Censuswide, a third-party research firm, to survey 400 IT professionals ranging in title from IT junior managers to CISOs in various industry sectors who work in organizations with 1,000+ employees. The survey was conducted in the following countries: USA, UK, Germany, France, Italy, and Spain. The results of the survey showcase the top cybersecurity challenges, key practices, and concerns businesses face in today's environment of constantly evolving cyber threats.

Threat Landscape

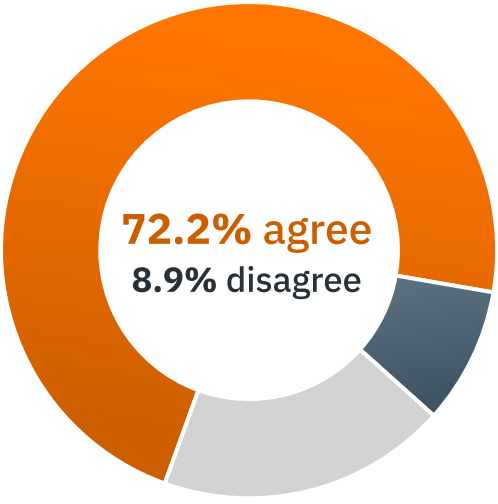
Cyberattacks such as phishing, ransomware, and espionage are on the rise. Adversaries continue to evolve tactics targeting organizations embracing the hybrid working model. Because of this, experts predict that 2023 will be a consequential year for cybersecurity and anticipate the next 12 months will include an expanded threat landscape and increasingly sophisticated cyberattacks.

On a global scale, respondents indicated they are most concerned about software vulnerabilities and/or zero-days threats (53%) and phishing/social engineering threats (52%), with more than 72% of IT and cybersecurity leaders reporting that their company has seen an increase in the sophistication of phishing attacks.

Do you agree or disagree with this statement:

My company is seeing an increase in the sophistication of phishing attacks?

Overall



By country

USA
84% agree
13.3% disagree

Germany
80.9% agree
2.9% disagree

France
74.6% agree
7.5% disagree

Spain
71.2% agree
7.6% disagree

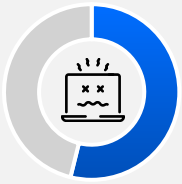
UK
62.9% agree
10% disagree

Italy
58.8% agree
11.8% disagree

Leaders in different regions have varying cybersecurity concerns. Eighty percent of the USA respondents said vulnerabilities were their primary concern, followed by supply-chain attacks (73%) and phishing (58%). On the other hand, respondents in the UK said they were on the highest alert due to supply-chain attacks (47%), while respondents in Spain said they were most concerned about ransomware attacks (60%). Interestingly, over half of surveyed IT leaders based in France said espionage was their primary cybersecurity concern.

What types of threats are you most concerned about?

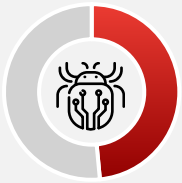
Overall



53.9% software vulnerabilities/ zero-days

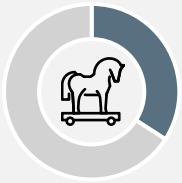
52.2% phishing/ social engineering

49% supply chain attacks

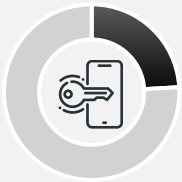


48.5% ransomware

36.5% insider threats

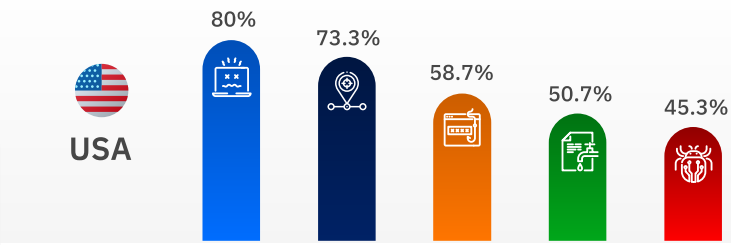


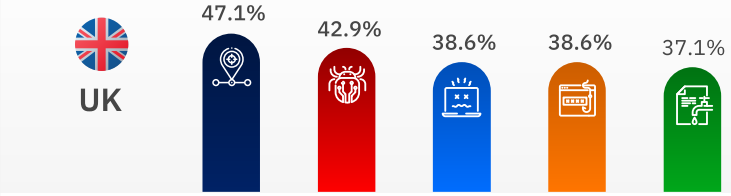
34.1% espionage

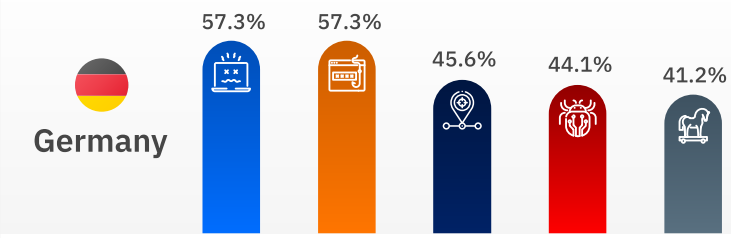


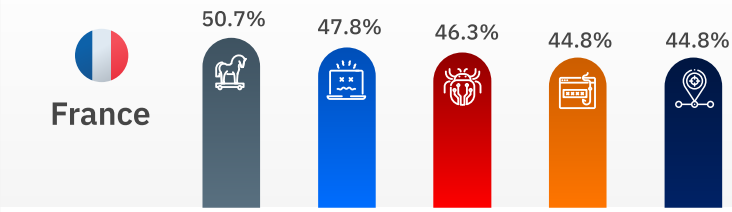
24.1% privilege escalation

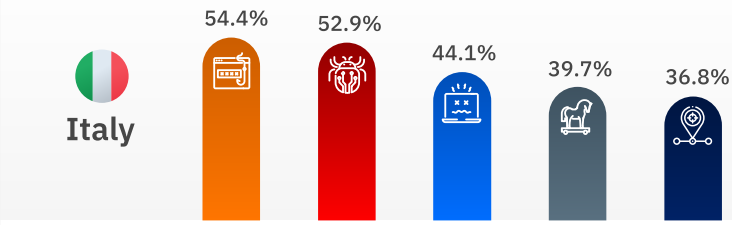
Top 5 by country

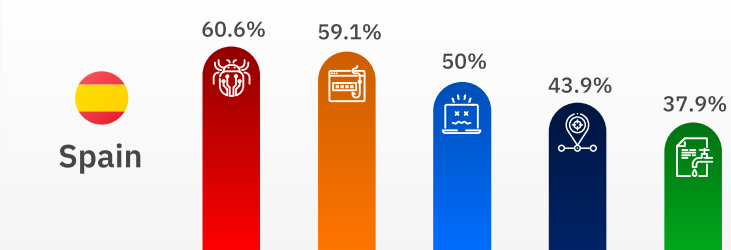












> It's not surprising for us to see that software vulnerabilities have surpassed phishing attacks as the most recognized threat. In recent years, threat actors have learned how to quickly weaponize newly discovered vulnerabilities, and waves of automated attacks are now routinely detected in the wild. Highly scalable opportunistic attacks, combined with a more disruptive, manual extortion phase, is the latest evolutionary stage of the profit-sharing criminal groups.

Martin Zugec, director of technical marketing at Bitdefender

While threat concerns vary between organizations and geographies, it's clear that the human factor remains the biggest worry for most business leaders, as the majority of attack vectors exploit human weakness in order to succeed.

Phishing and social engineering attacks primarily tap into human psychological elements and vulnerabilities, with hackers also taking advantage of employees' lack of awareness and training, negligence, or plain error.

With organizations now employing distributed workforces, whereby staff split their time between home and the office, hackers are increasingly targeting non-corporate approved software and devices.

More than a quarter of IT professionals say they also want to bust the myth that their organization is not the target of cybercriminals — a figure that increases to 43% among USA respondents.

What, if anything, is the biggest security myth you wish you could bust when it comes to your organization's employees?

Overall

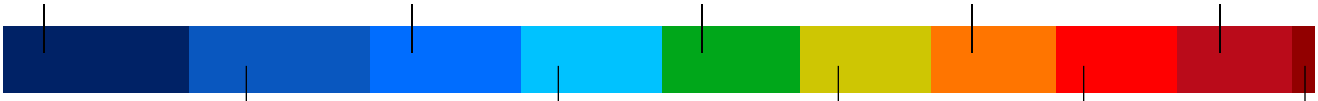
34.3% "security is solely the responsibility of the IT team"

27.8% "mobile devices are immune to malware and threats"

25.6% "our organization is not a target for cybercriminals"

23.2% "MFA/strict password requirements are unnecessary"

21.3% "Apple devices/ products are always secure"



33.6% "using non-corporate approved applications — personal mail, chat, or web-based storage — is not a big deal"

25.8% "an email that comes into the corporate system is always safe to open and click on"

24.1% "mainstream websites are safe to visit"

22.2% "delaying software updates is no big deal"

4.1% there are no security myths in need of busting

Top 3 by country

USA

- **42.7%** "our organization is not a target for cybercriminals"
- **40%** "using non-corporate approved apps is not a big deal"
- **36%** "security is solely the responsibility of the IT team"
- **36%** "an email that comes into the corporate system is always safe to open/click on"

UK

- **40%** "using non-corporate approved apps is not a big deal"
- **25.7%** "security is solely the responsibility of the IT team"
- **24.3%** "mobile devices are immune to malware threats"
- **24.3%** "our organization is not a target for cybercriminals"

Germany

- **39.7%** "security is solely the responsibility of the IT team"
- **32.3%** "mobile devices are immune to malware threats"
- **27.9%** "using non-corporate approved apps is not a big deal"

France

- **44.8%** "using non-corporate approved apps is not a big deal"
- **37.3%** "security is solely the responsibility of the IT team"
- **29.8%** "MFA/strict password requirements are unnecessary"

Italy

- **29.4%** "mainstream websites are safe to visit"
- **27.9%** "MFA/strict password requirements are unnecessary"
- **27.9%** "security is solely the responsibility of the IT team"
- **26.5%** "our organization is not a target for cybercriminals"

Spain

- **39.4%** "security is solely the responsibility of the IT team"
- **33.3%** "mobile devices are immune to malware threats"
- **22.7%** "using non-corporate approved apps is not a big deal"
- **22.7%** "mainstream websites are safe to visit"
- **22.7%** "Apple devices/ products are always secure"

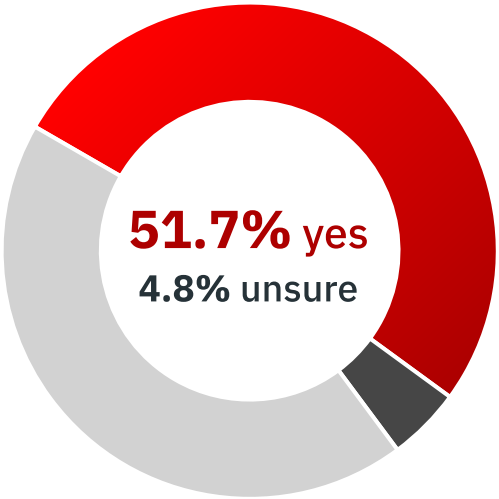
Concealing Data Breaches

Our survey results demonstrate that being concerned about a data breach or a data leak is justified, as more than half (52%) of respondents said they had experienced a data breach or leak due to a cybersecurity incident in the last 12 months.

This figure increases to three-quarters among organizations in the USA, much higher than all other countries (UK 51%, France 42%, Germany 49%, Italy 47%, Spain 44%).

In the last 12 months, have you experienced a data breach or data leak?

Overall



By country

USA
74.7% yes
4% unsure

UK
51.4% yes
4.3% unsure

Germany
48.5% yes
5.9% unsure

Italy
47.1% yes
4.4% unsure

Spain
43.9% yes
6.1% unsure

France
41.8% yes
4.5% unsure

Perhaps even more shocking than the percentage of organizations to suffer a breach is the fact that many IT leaders say they have been told to keep the security breach confidential when they knew they were obligated to report it. More than 40% of all respondents said that was the case, while one in ten said they have kept a breach confidential when they knew it should be reported.

Interestingly, this figure varies depending on the departments of respondents: 66% of human resource (HR) and employees in legal departments were told to keep a data breach quiet, compared to 45% of CTOs and 39% of CIOs.

The figures also shift based on geographical location: more than 70% of USA respondents said they had been told to keep a breach under wraps, while 55% said they had kept a breach confidential when they knew it should have been reported.

By comparison, those from France are least likely to say they have been told to keep a breach confidential when they knew it should be reported (27%), and those from Germany are least likely to say they had kept a breach confidential when they knew it should be reported (15%).

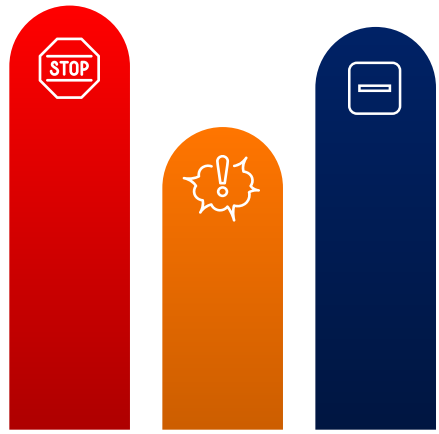
Have you ever been told to keep a security breach confidential, or kept it confidential when you knew it should be reported?

Overall

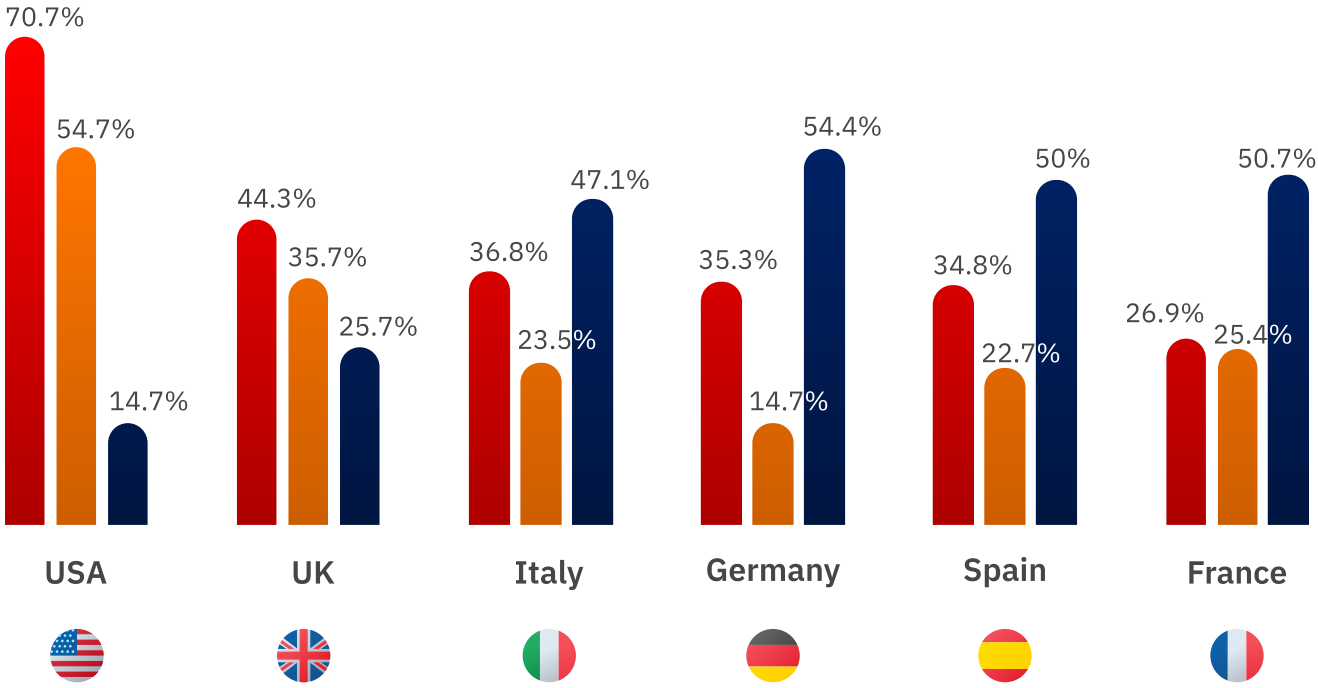
42% have been told to keep a breach confidential — when it should have been reported

29.9% have kept a breach confidential — knowing it should be reported

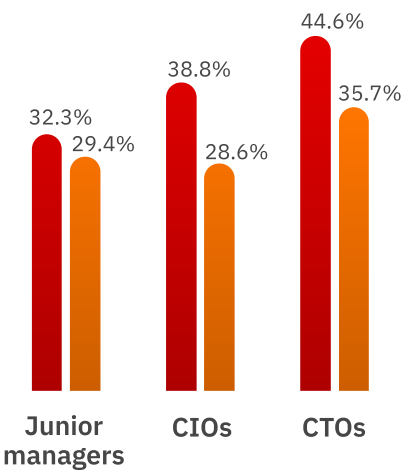
39.9% neither



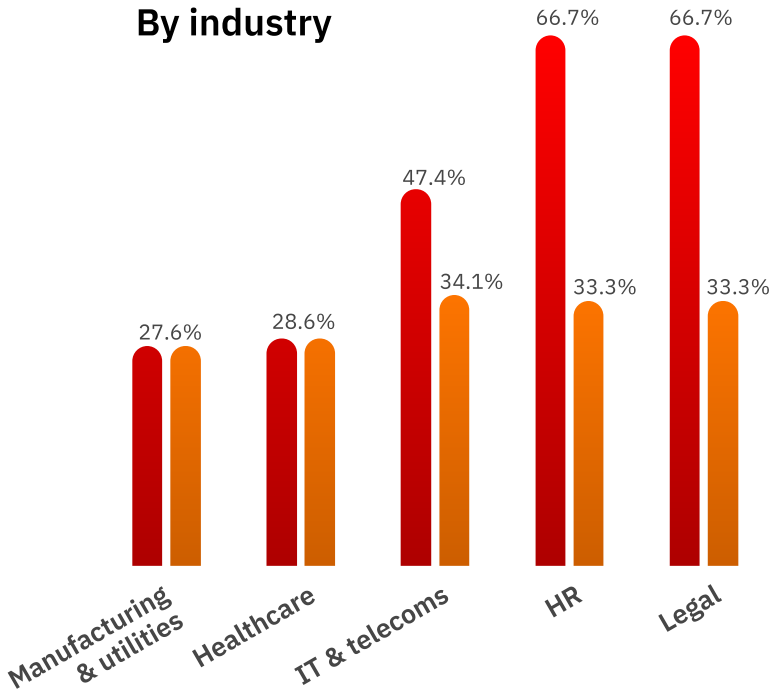
By country



By job role



By industry



> The findings in this report depict organizations under tremendous pressure to contend with evolving threats such as ransomware, zero-day vulnerabilities and espionage, while struggling with complexities of extending security coverage across environments and ongoing skills shortage. These results demonstrate, more than ever, the importance of layered security that delivers advanced threat prevention, detection and response across the entire business while improving efficiencies that allow security teams to do more with less.

Andrei Florescu, deputy general manager and senior vice president of products at Bitdefender Business Solutions Group

Until recently, many companies preferred to keep a security breach private to avoid financial, legal, and reputational damage, or spending resources on reporting instead of mitigating the damage. With more laws requiring cyber breach reporting taking effect (in the USA and the EU) the situation is expected to change. According to our survey, 55% of respondents say they are worried about their company facing legal action due to a security breach being mismanaged, with just 24% disagreeing with this statement.

Do you agree or disagree with this statement: I'm worried about my company facing legal action due to a security breach being handled incorrectly?

Overall

54.3% agree

25.1% disagree

By country

USA
- **78.7%** agree
- **14.7%** disagree

France
- **53.7%** agree
- **25.4%** disagree

UK
- **51.4%** agree
- **22.9%** disagree

Spain
- **48.5%** agree
- **30.3%** disagree

Italy
- **47.1%** agree
- **29.4%** disagree

Germany
- **44.1%** agree
- **29.4%** disagree

Top Cybersecurity Challenges

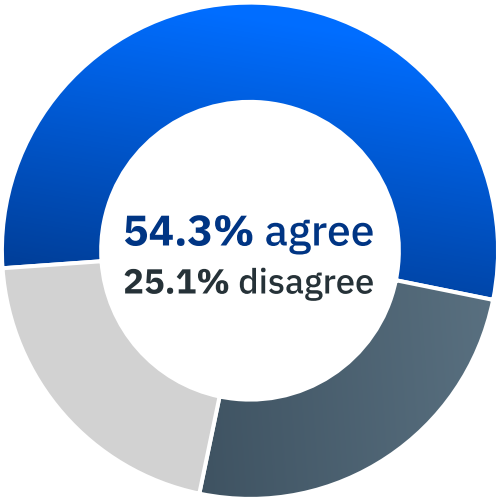
The majority of IT and security leaders surveyed said they had experienced a data breach in the past 12 months. Yet, almost all of those surveyed said they continue to face challenges with their current security solutions.

Just 2.7% of respondents said there are no challenges with their current solution, while more than half said their organization had purchased a security tool that didn't live up to the marketing hype. In the USA, that number is almost 80%.

Do you agree or disagree with this statement:

My company has recently purchased a security tool that didn't live up to the marketing hype?

Overall



By country

USA
78.7% agree
14.7% disagree

France
53.7% agree
25.4% disagree

UK
51.4% agree
22.9% disagree

Spain
48.5% agree
30.3% disagree

Italy
47.1% agree
29.4% disagree

Germany
44.1% agree
29.4% disagree

The most prevalent challenge faced by IT and security leaders is trouble extending security capabilities across multiple environments (44%). These include on-premises, cloud, and hybrid cloud, as organizations continue shifting to a new way of supporting distributed workspaces by leaning heavily on cloud-based collaboration tools.

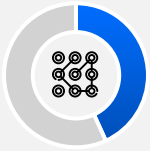
A similar percentage (43%) of respondents said their solution was proving too complex, while 36% said their organization lacked the security skill set to drive full value from the product.

These two issues are being felt across the technology industry as a whole: recent figures show there are more than 3.4 million openings for security professionals globally, an increase of over 26% from 2021.

What are the biggest challenges with your current security solutions?

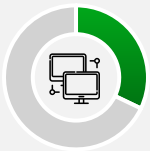
Overall

43.5% extending capabilities across multiple environments



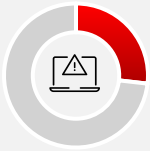
43.2% complexity

36% lack of security skill set to drive full value

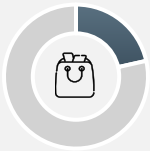


32.1% incompatibility with other security solutions

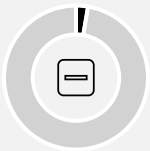
28% reporting capabilities



26.8% too many alerts

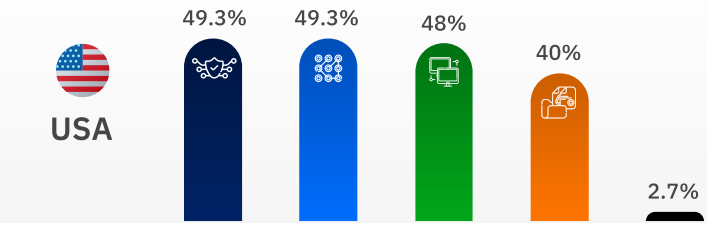


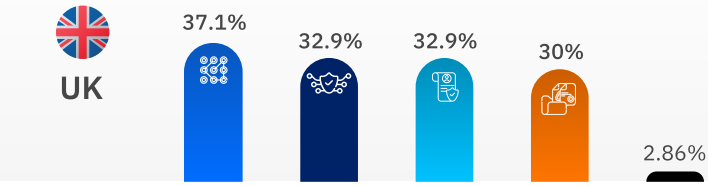
21.5% unnecessary features

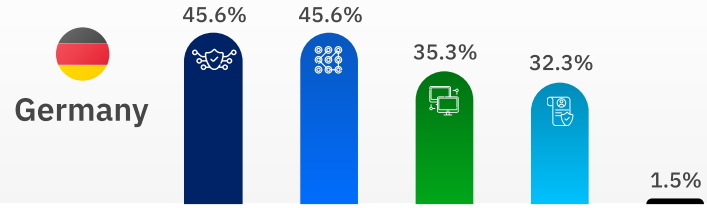


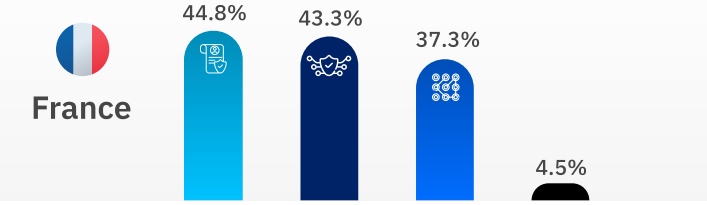
2.7% there are no particular challenges

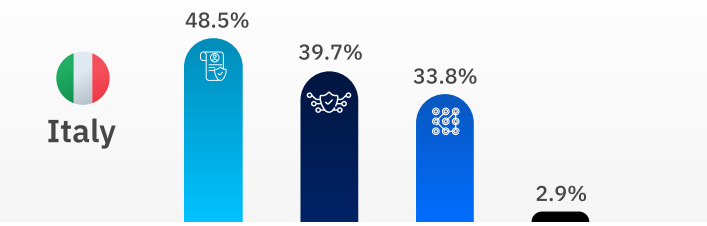
Top 3 + "no challenges" by country

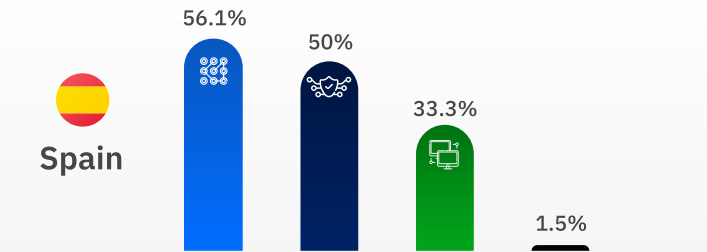












The cybersecurity skill shortage looks likely to worsen for many organizations over the next 12 months. Our report shows a correlation between security professionals who are required to work weekends to keep up and those looking for new jobs.

For example, USA-based respondents said they often have to work on weekends due to security concerns that their company faces (80%), and these same respondents are also most likely to agree they are planning to look for a new job in the next year.

Do you agree or disagree with this statement:

I often have to work on weekends due to security concerns that my company faces?

Overall
59.2% agree
19.3% disagree

USA
80% agree
14.7% disagree

UK
64.3% agree
11.4% disagree

France
58.2% agree
19.4% disagree

Germany
51.5% agree
20.6% disagree

Spain
50% agree
28.8% disagree

Italy
48.5% agree
22.1% disagree

Do you agree or disagree with this statement:

I am planning on looking for a new job in the next 12 months?

Overall
39.4% agree
36.7% disagree

USA
57.3% agree
28% disagree

UK
45.7% agree
25.7% disagree

France
46.3% agree
34.3% disagree

Germany
30.9% agree
39.7% disagree

Spain
28.8% agree
43.9% disagree

Italy
25% agree
50% disagree

Other common challenges faced by those surveyed include incompatibility with other solutions (32%), a lack of reporting capabilities (28%), and too many alerts (27%).

> With 43% of respondents stating the extension of cybersecurity capabilities across various environments is the biggest challenge they face today, it is no wonder XDR continues a meteoric rise. Today's security teams must have a holistic view of their infrastructure (on premises, virtual, cloud) and ability to investigate and verify incidents faster, eliminating threats wherever and whenever they arise.

Daniel Daraban,
director of product management at Bitdefender

However, while 98% of security professionals surveyed said they are not completely happy with their current solutions, it's clear that they know what they want to protect their organizations from cyber threats.

A whopping 93% of respondents said proactive threat hunting is either very important or important to their response plan, a figure that rises to 100% among USA respondents.

Security professionals from companies with 1,500 – 1,999 employees stated that proactive threat hunting is essential (97%), followed by those from a company with 2,500 employees or more (94%) and those from a company with 1,000 – 1,499 employees (92%).

How important is proactive threat hunting to detect and respond to threats in your environment?

Overall

93% important

- **58.7%** very important
- **34.3%** somewhat important

7% not important

- **5.8%** not very important
- **1.2%** not important

By company size

1,000 - 1,499 employees
91.7% important
8.3% not important

1,500 - 1,999 employees
96.9% important
3.1% not important

2,000 - 2,499 employees
90.6% important
9.4% not important

2,500+ employees
93.9% important
6.1% not important

By country

USA
100% important

Spain
95.5% important
4.5% not important

Germany
94.1% important
5.9% not important

Italy
91.2% important
8.8% not important

UK
88.6% important
11.4% not important

France
88.1% important
11.9% not important

Similarly, almost all (99%) IT leaders surveyed said that a managed service provider (MSP) was a key aspect of their security solutions due to their need to have 24x7 security coverage (45%), to free up internal IT/security resources (35%), and to receive actionable intelligence vs. flood of alerts (32%). Respondents also said that using an MSP equips them with security analysts' expertise for peace of mind, as more than one in 5 stated that they can't deal with the complexity of the threat landscape without the assistance of an MSP.

If you use or are considering using a managed security provider, what are the key reasons for doing so?

Overall

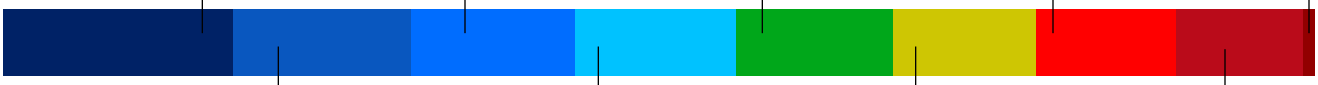
45.4% 24X7 security coverage

32.1% to get actionable intelligence vs. a flood of alerts

30.7% to gain access to security analysts' expertise

27.5% compliance or insurance purposes

1.4% don't use nor plan to use a managed security provider



35% to free up internal IT/ cybersecurity resources

31.9% proactive threat hunting capabilities

28.3% peace of mind

22.2% don't have the capacity to deal with the complexity of the threat landscape

Top 3 by country

USA

- **46.7%** 24X7 security coverage
- **44%** actionable intelligence
- **41.3%** access to security analysts' expertise

UK

- **41.4%** 24X7 security coverage
- **30%** access to security analysts' expertise
- **28.6%** peace of mind

Germany

- **44.1%** 24X7 security coverage
- **42.6%** freeing up internal resources
- **33.8%** actionable intelligence

France

- **47.8%** 24X7 security coverage
- **37.3%** freeing up internal resources
- **32.8%** actionable intelligence
- **32.8%** proactive threat hunting
- **32.8%** peace of mind
- **32.8%** compliance/insurance

Italy

- **50%** 24X7 security coverage
- **32.3%** freeing up internal resources
- **30.9%** proactive threat hunting

Spain

- **42.4%** 24X7 security coverage
- **37.9%** proactive threat hunting
- **37.9%** peace of mind
- **36.4%** freeing up internal resources

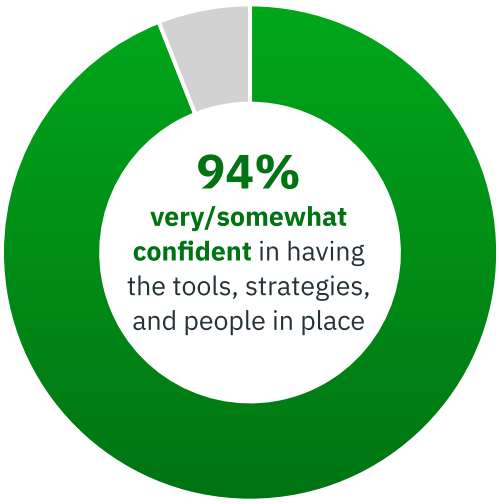
Security Response

While almost every security professional we surveyed said they face challenges due to their current security solutions, the majority remain confident in their organization's ability to respond to cyber threats. Almost 94% said they are very, or somewhat, confident they have the tools, strategies, and people in place to respond to threats, with just 6% saying they are not confident in their response plan.

This sentiment is unlikely to differ between different-sized companies: over 9 in 10 security professionals surveyed from a company with 1,000 – 1,499 employees (93%), 1,500 – 1,999 employees (95%), and 2,500 employees or more (94%) said they are confident about the current state of their organization's ability to respondent to security threats. Confidence does, however, shift among job titles: 0% of HR professionals said they were not confident, increasing to 2% among directors and 13% among junior managers.

How confident, if at all, are you about the current state of your organization's ability to respond to cybersecurity threats?

Overall



By country

Germany
98.5% very/somewhat confident

USA
97.3% very/somewhat confident

France
95.5% very/somewhat confident

Spain
92.4% very/somewhat confident

Italy
91.2% very/somewhat confident

UK
88.6% very/somewhat confident

Despite this confidence and the global economic crisis that has led to widespread layoffs and a slowdown in spending, most security professionals say they plan to increase their security budgets in 2023 to respond to the evolving threat landscape.

Nearly three-quarters (74%) of respondents said they plan to increase their budget over the next 12 months. This figure rises to more than 78% among US respondents and dips to around 70% among European businesses.

How has economic uncertainty impacted your security budget for 2023?

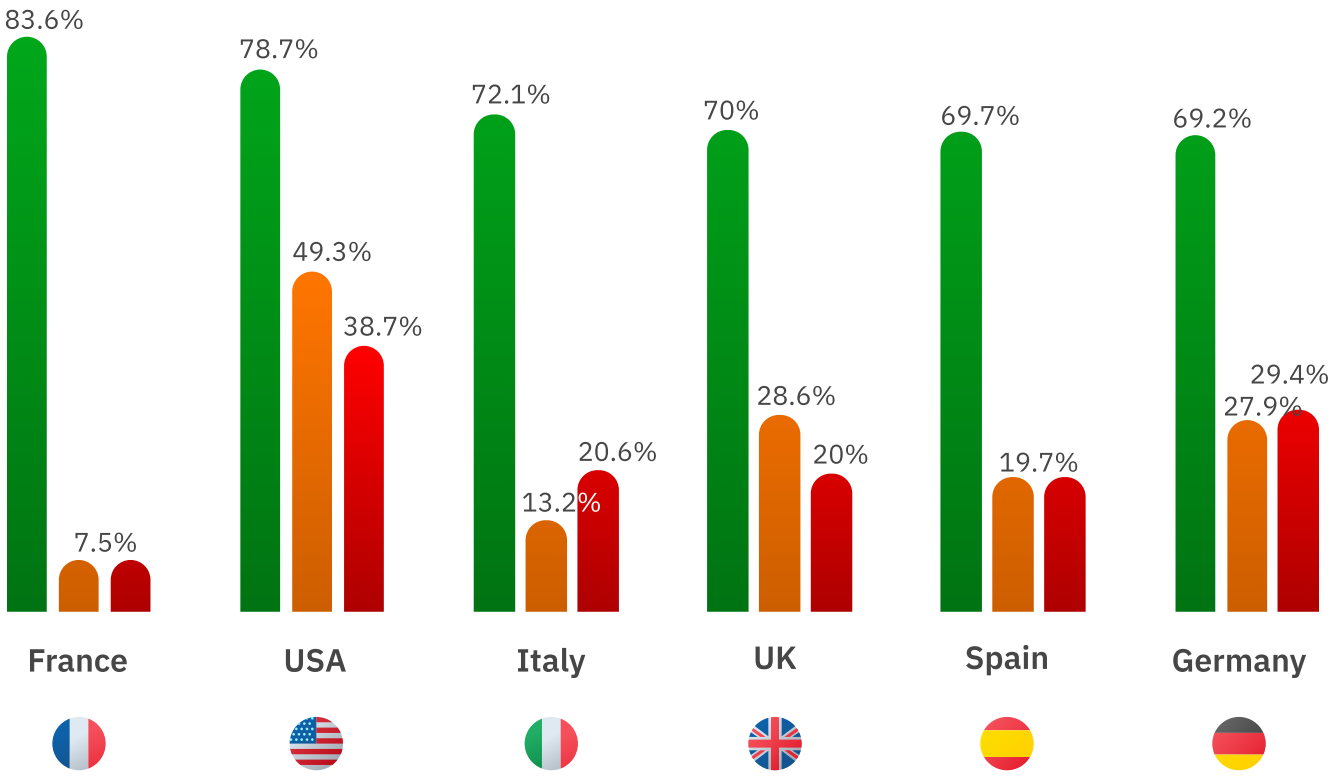
Overall

73.9% plan to increase their budget

24.8% plan to cut back on new cybersecurity tech purchases

22.9% plan to cut back on new cybersecurity hires

By country



Similarly, over three-quarters (76%) of respondents agree they are looking to onboard more security vendors in 2023, with over a third (35%) saying they strongly agree.

Interestingly, while 49% of USA respondents plan to cut back on new cybersecurity tech purchases, almost 95% are looking to onboard more security vendors. Over 90% of our USA respondents are also planning to consolidate their existing vendors, meaning they are looking for holistic, all-in-one solutions.

Fewer IT and cybersecurity leaders in European countries plan on cutting back on cybersecurity tech purchases (7% in France, 13% in Italy, and 20% in Spain), yet also fewer are looking to onboard more security vendors (75% in France, 71% in Spain, and only 59% in the UK).

Do you agree or disagree with this statement:

We are looking to onboard more security vendors in 2023?

Overall
75.8% agree
4.8% disagree

USA
94.7% agree
1.3% disagree

Italy
79.4% agree
7.3% disagree

Germany
75% agree
7.3% disagree

France
74.6% agree
6% disagree

Spain
71.2% agree
4.5% disagree

UK
58.6% agree
2.9% disagree

Do you agree or disagree with this statement:

We are looking to consolidate our existing security vendors in 2023?

Overall
77% agree
5.6% disagree

USA
90.7% agree
4% disagree

France
80.6% agree
4.5% disagree

Italy
77.9% agree
2.9% disagree

Spain
72.7% agree
4.5% disagree

UK
71.4% agree
4.3% disagree

Germany
67.6% agree
13.2% disagree

How XDR and MDR Can Help

Our report shows that businesses remain on high alert due to the evolving threat landscape. While security professionals remain confident in their ability to respond to cyber threats, it's clear that current security solutions are not ticking all of the boxes as attackers continue to evolve their tactics and exploit human weaknesses to compromise organizations of all shapes and sizes.

With organizations looking to increase their cybersecurity budgets into 2023 and with proactive threat hunting a necessity for almost all of the security professionals we surveyed, a couple of complementary ways a business can enhance its cyber resiliency is through the use of eXtended Detection and Response (XDR) and Managed Detection and Response (MDR).

Not only will these technologies and services equip organizations with the ability to stay on top of prevention, protection, detection, and response by providing on-demand access to full-time threat analysts, investigators, and incident response experts, but they also help businesses bridge the talent gap by combating advanced forms of cyber threats that exploit the human weakness, including social engineering attacks.

A native XDR solution observes and detects attacks across an organization's environment: physical and connected devices, virtual and cloud platforms, and their hosted workloads are all covered, while MDR — backed by XDR — combines endpoint, network, cloud, identity, and productivity application telemetry into actionable security analytics, augmented by the threat-hunting expertise of a fully staffed security operations center (SOC).

Together these tools equip organizations with around-the-clock monitoring, sophisticated threat detection, and remediation capabilities, all while helping security teams struggling with staffing shortages, alert fatigue, and a need to streamline operations.

Learn how MDR and XDR can enhance cyber resilience

Bitdefender®

BUSINESS SOLUTIONS | Cybersecurity Built For Resilience