Bitdefender

EXECUTIVE SUMMARY

Dec 2022

Cybersecurity Posture Survey
Looking Towards 2023

For the third consecutive year, Bitdefender conducted a global survey to assess the current cybersecurity posture in the business sector, identify relevant patterns and predict future trends in cybersecurity consumption.

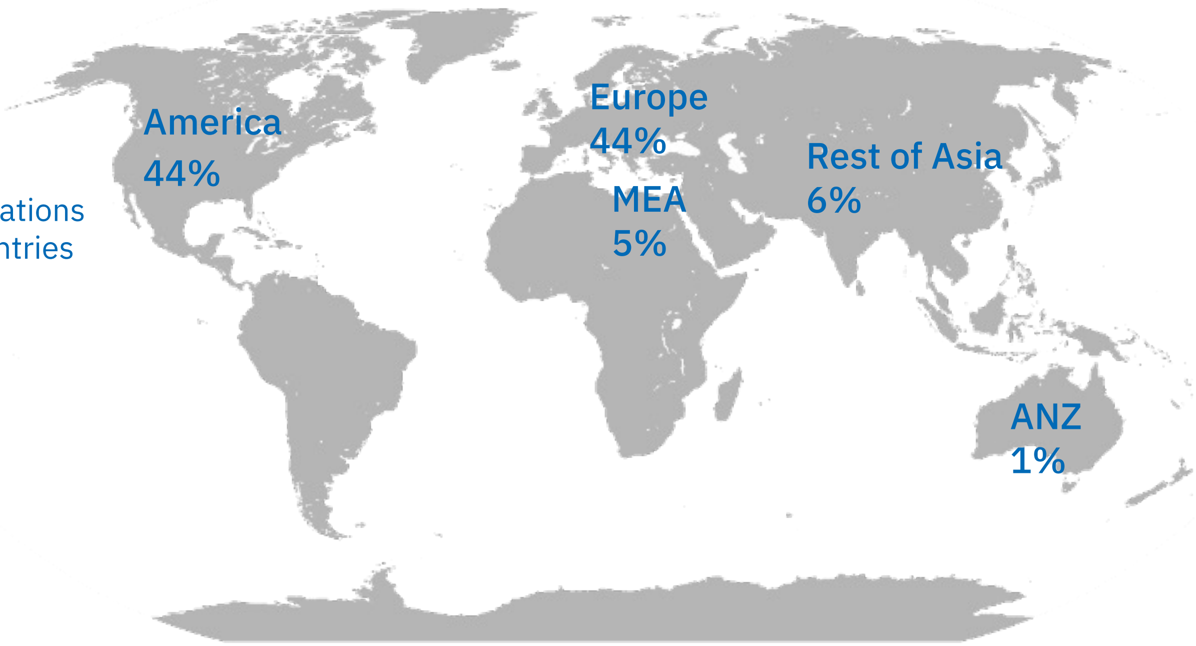
As usual, our survey took place from September through November and included companies from all industries and sizes. A total of 1,693 organizations responded from 100 countries across the globe.

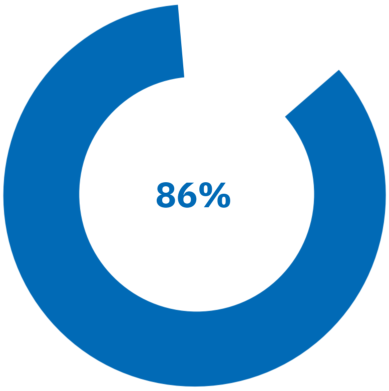
The findings from our past three surveys can help business decision-makers benchmark their current cybersecurity status and improve their cybersecurity posture in the future.

2022 Firmographics

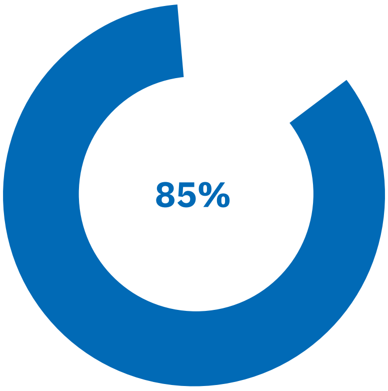
Respondents by Geography

1,693 organizations from **100** countries



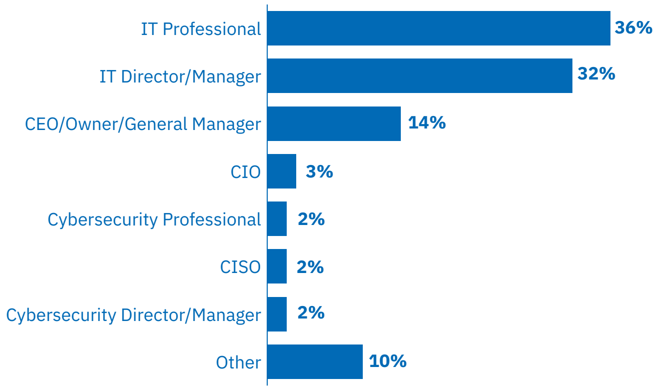


of respondents work in mature organizations founded more than 10 years ago

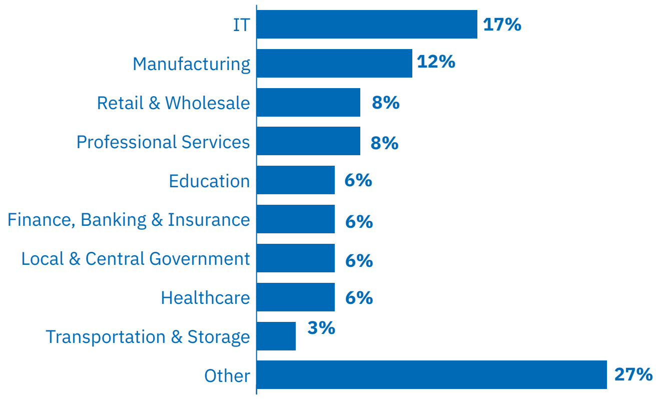


of respondents have less than 500 employeess

Respondents by Role



Respondents by Industry

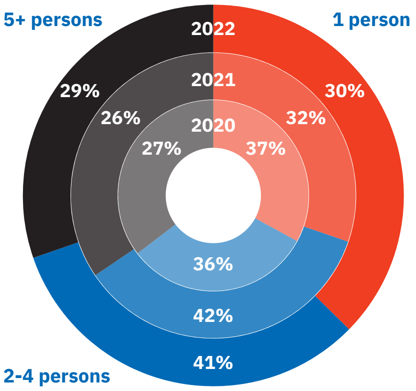


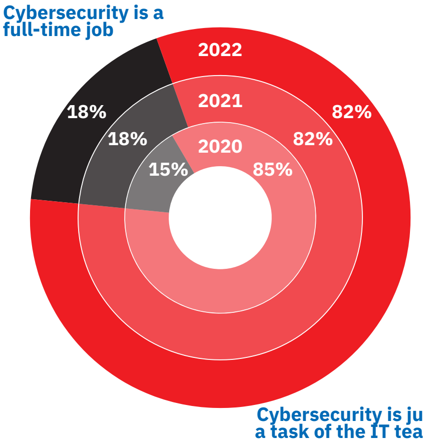
Cybersecurity

IT teams are slowly growing, but about 30% of organizations still have only one person responsible for IT while another 41% have a small IT team of 2-4 people.

Cybersecurity is just a task of the IT team, among others, for 82% of respondents, as opposed to only 18% for whom **cybersecurity is a full-time job** with dedicated cybersecurity personnel in place.

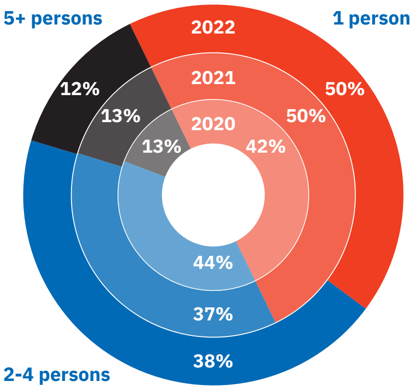
IT Team Size

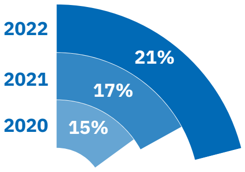




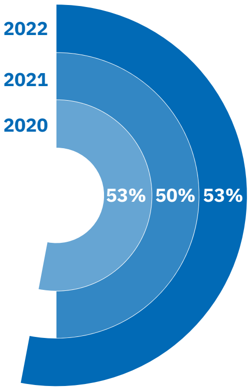
Even when dedicated cybersecurity personnel exists, it is often just one person (50%) or 2-4 persons in the cybersecurity department (38%).

Size of Cybersecurity Department

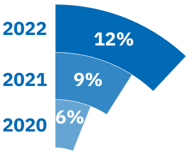




of organizations without dedicated cybersecurity personnel plan to recruit such personnel in the future

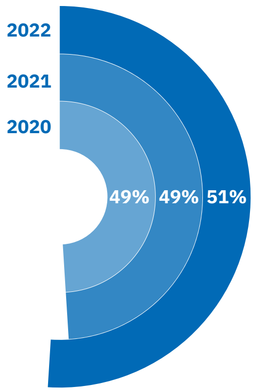


of organizations have already moved from a Prevention-only approach to Prevention, Detection and Response

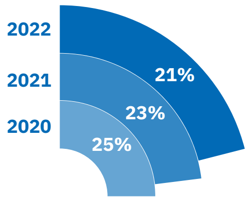


% of those who are still in Prevention-only mode are currently testing a Detection and Response solution; in 2022, another 32% are considering the adoption, but 56% of them still have no plans to adopt a Detection and Response solution

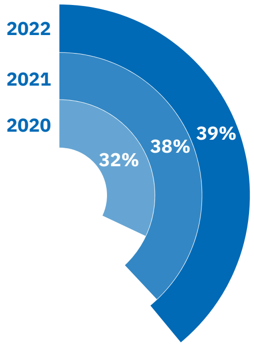
Over half of 2022 respondents say they have never been the target of an advanced threat attack. Perception of the likelihood of an advanced threat attack is optimistic, with only 21% of respondents considering this is likely to happen in the near future.



of organizations have never been the target of an advanced threat attack in the past



of organizations consider an advanced threat attack is likely to happen to them in the near future



of organizations have a Cybersecurity Incident Response Plan already in place

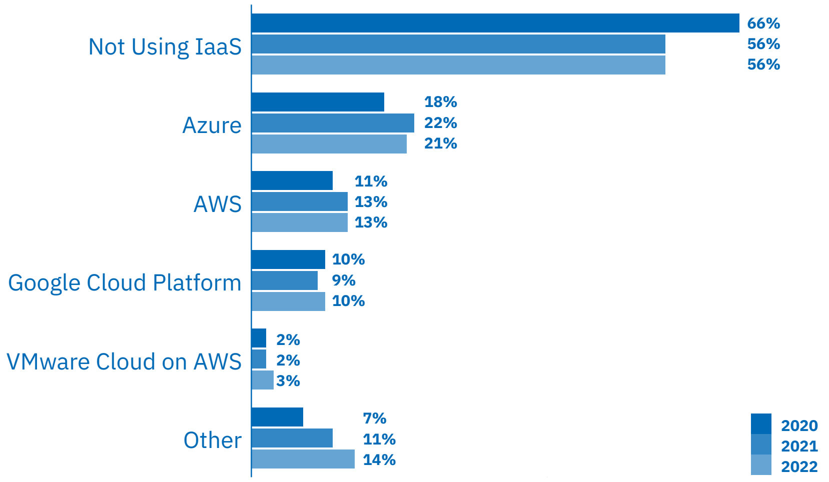
Cloud Security

Work from home brought a surge in public cloud adoption, with adoption rates increasing 10pp from 34% in 2020 to 44% in 2021; since then, adoption rates have stayed the same.

Microsoft Azure is the most frequent IaaS choice (21%), followed by AWS (13%) and Google Cloud Platform (10%).

Most IaaS users (84%) use less than 50 public cloud instances per month, and Windows is the most frequently used OS for public cloud instances.

IaaS usage

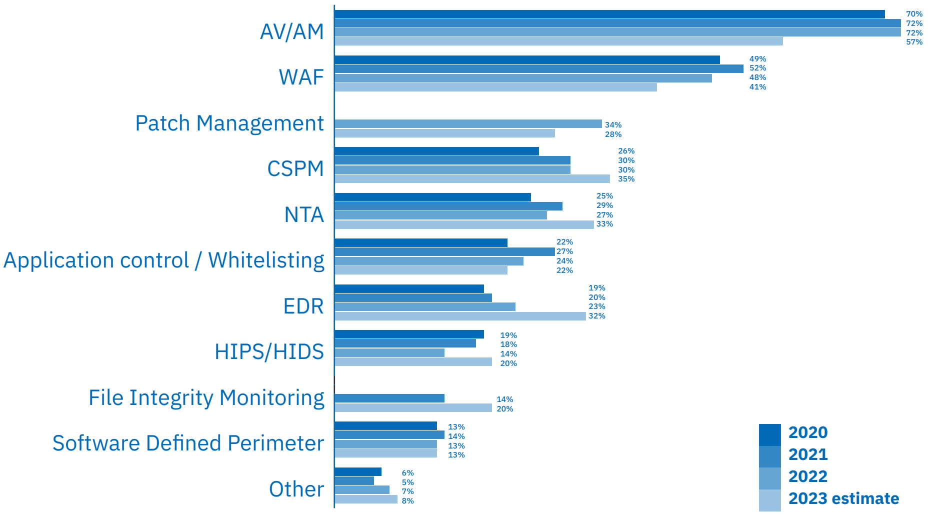


On average, companies use three or more tools to secure their public cloud workloads.

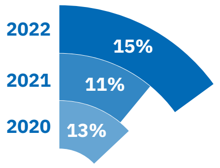
Antivirus/Antimalware (AV/AM) is currently the most adopted protection layer for IaaS (72%), followed by Web Application Firewall - WAF (48%), Patch Management (34%), and Cloud Security Posture Management – CSPM (30%).

However, as per respondents' own estimates, adoption will decline for AV/AM (-15 pp), WAF (-8 pp), and Patch Management (-6 pp). Adoption will increase for Server Workload EDR (+10 pp), Network Traffic Analytics – NTA (+6 pp), HIPS/HIDS (+6 pp), File Integrity Monitoring (+6 pp) and CSPM (+5 pp).

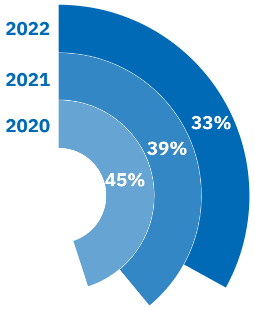
IaaS security technologies in use



Only 15% of IaaS users are currently using containers, while another 32% of them plan to start using containers in the future. Kubernetes remains the most used container orchestration platform (33%), with other container platforms often used in parallel.



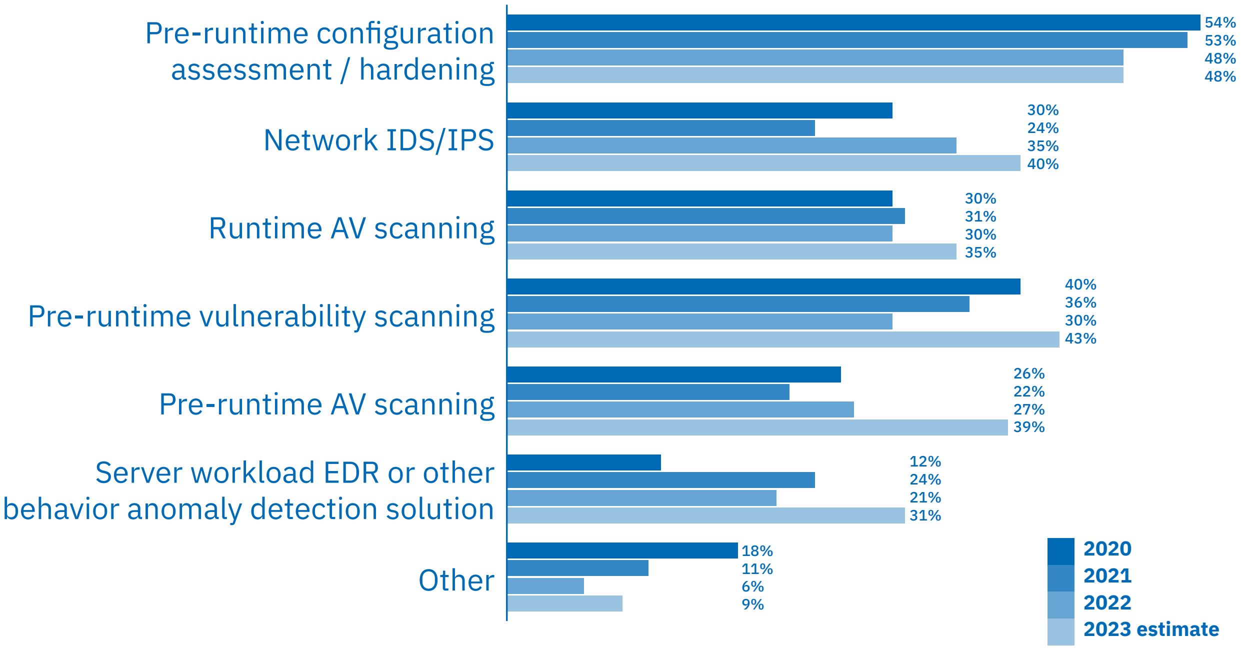
% of IaaS users are currently using containers



% of those using containers are using Kubernetes

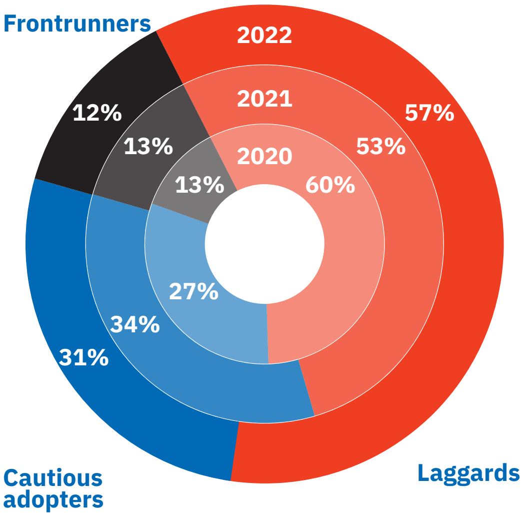
Most companies use two or more tools for container security. Pre-runtime configuration assessment / hardening is the container's most used security control (48%). Adoption of several other container protection technologies will increase in the near future as they better serve their purpose when working together: Pre-runtime vulnerability scanning (+13 pp), Pre-runtime AV scanning (+12 pp), EDR or other behavior anomaly detection (+10 pp), Network Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS) (+5 pp), and Runtime AV scanning (+5 pp).

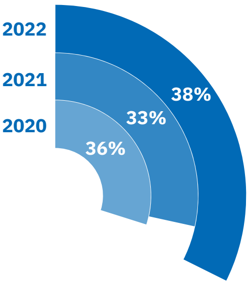
Container security technologies in use



Patterns in technology adoption

Most organizations (57%) are laggards in terms of cybersecurity technology adoption. Only 12% are at the forefront of technology adoption and are willing to adopt new cybersecurity technologies as soon as they become available, while 31% are open minded but cautious.

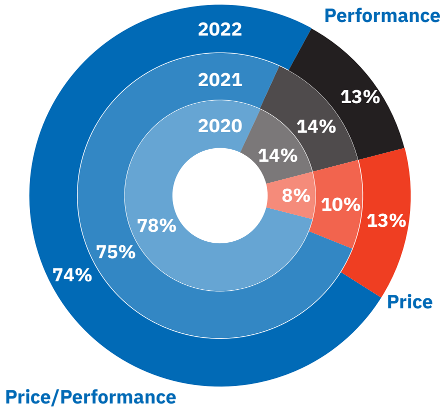




of organizations use three or more security vendors

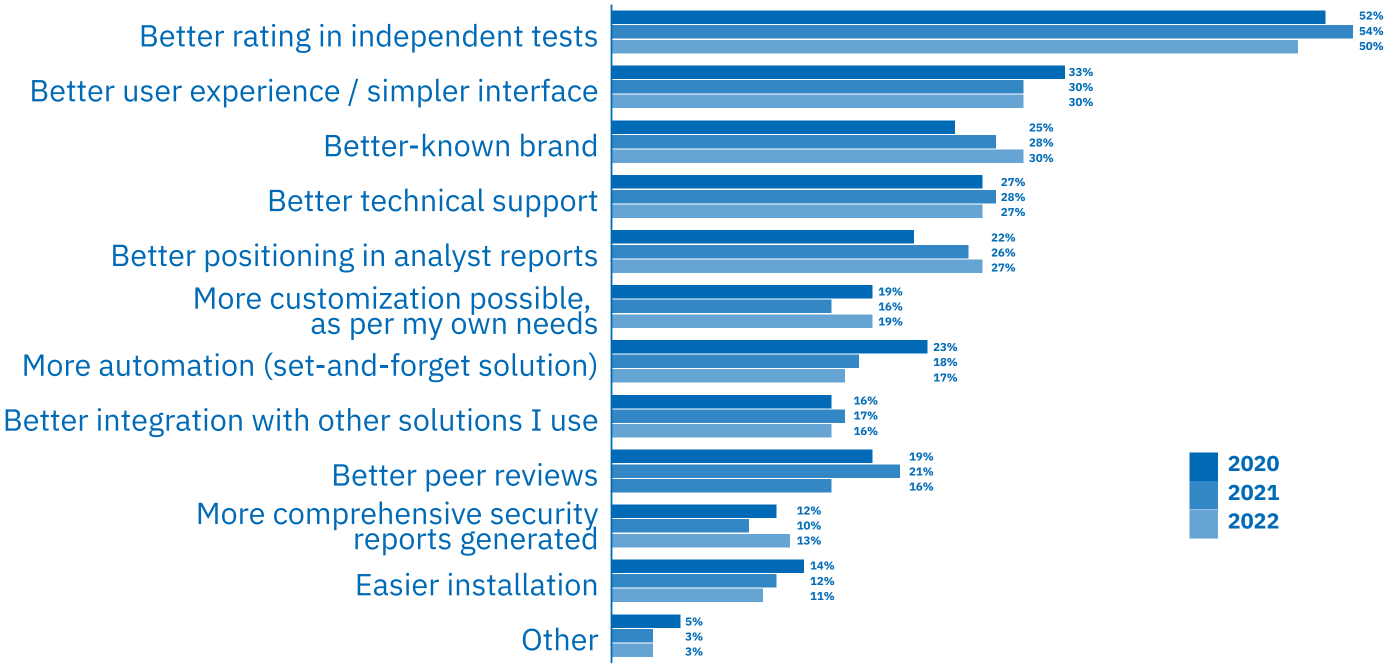
While 52% of respondents are pursuing a vendor consolidation strategy now or plan to in the future, the share of organizations using more than three cybersecurity vendors has increased by 5 pp since last year as vendor and tool consolidation goals often collide with the complex realities of safeguarding security.

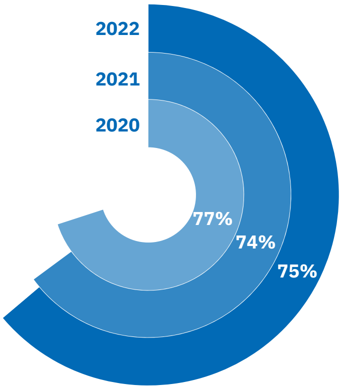
The price/performance ratio guides the vast majority of respondents (74%) when buying new cybersecurity solutions, with only 13% of respondents willing to disregard the price when making new acquisitions.



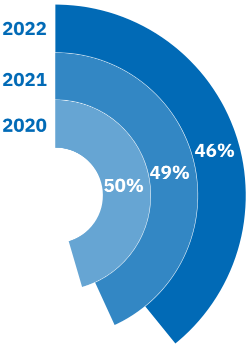
Rating in independent tests remains by far the most important criterion when choosing a cybersecurity solution, followed by user experience, and brand reputation.

Top criteria used when choosing a new cybersecurity solution



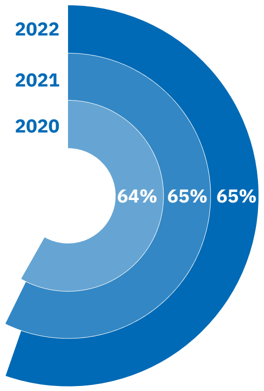


of organizations prefer integrated solutions that cover everything in one suite (endpoint, cloud, and network security)

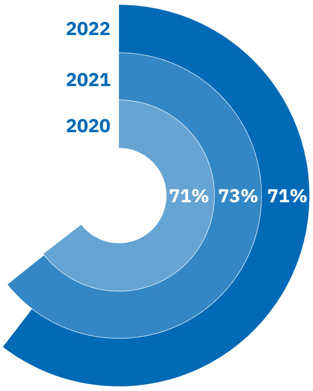


of organizations prefer bundled solutions that include all the required cybersecurity layers/ components / features

Organizations favor partially automated solutions, and they prefer the “per device/machine” billing mode.

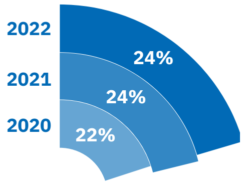


of organizations prefer partially automated solutions, as they keep the advantages of an automatic solution while also allowing for some form of granular control

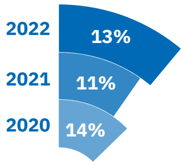


of organizations prefer the “per device/machine” billing mode

Outsourcing security operations is not yet very common among respondents.

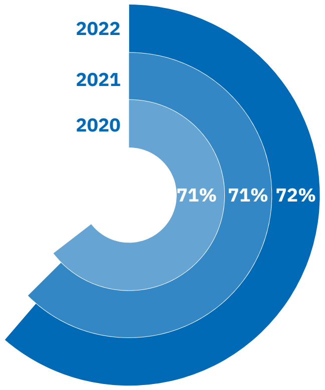


of organizations are already outsourcing parts of their security operations to an MSP/ MSSP/MDR provider

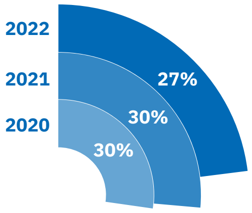


of organizations are planning to outsource in the future

IoT adoption is still in its early stages.



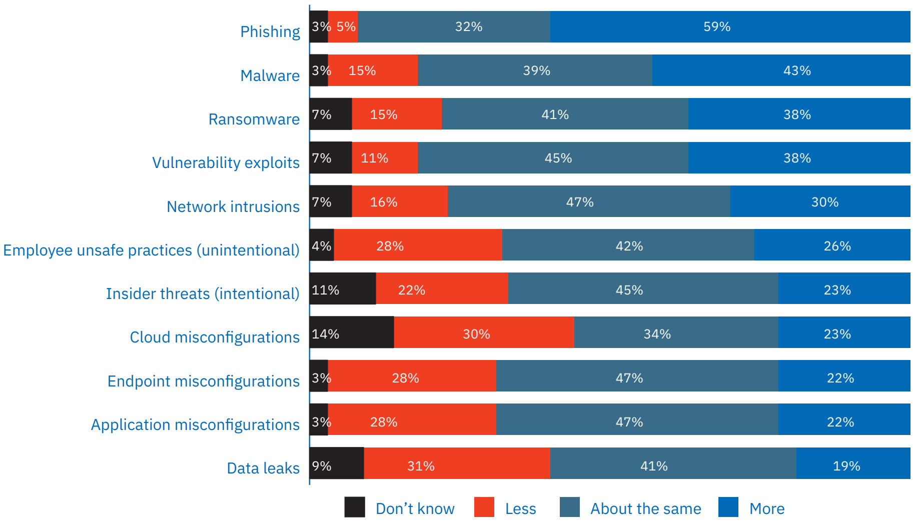
% of respondents say IoT devices represent less than 5% of their total devices



% of respondents have a BYOD policy in place

Challenges

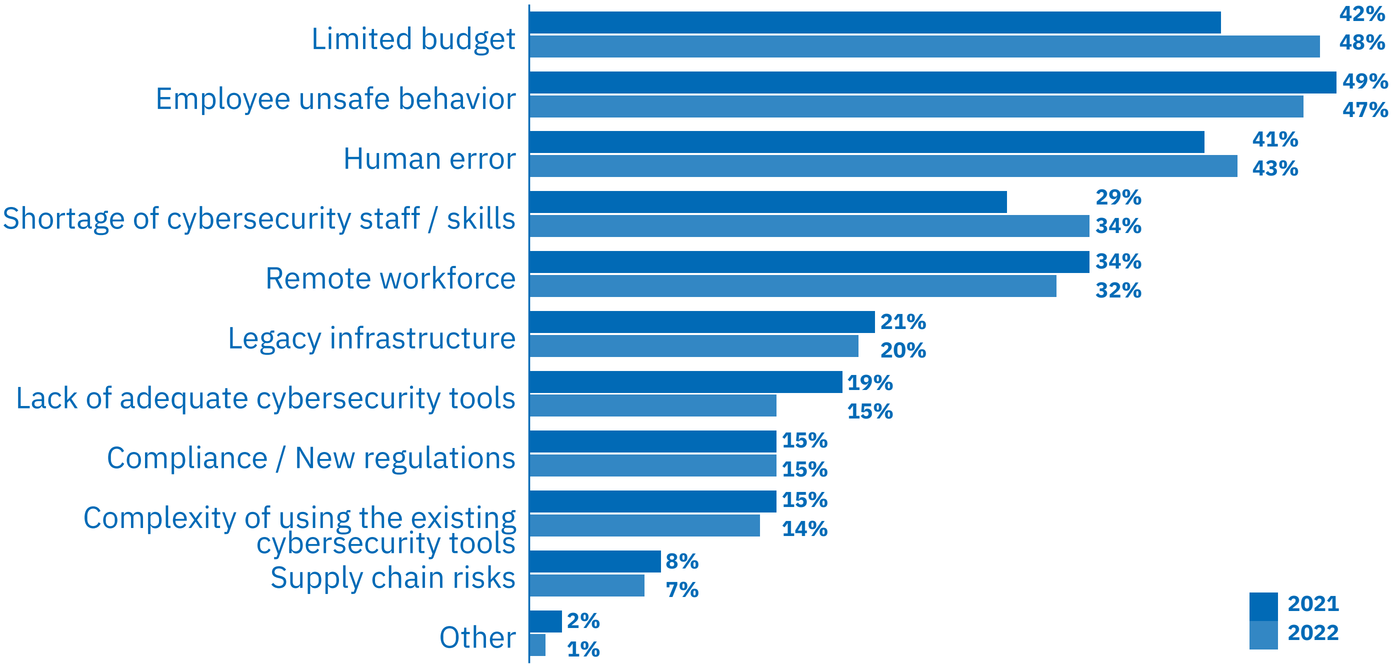
2022 Records of security alerts and events, as compared to last year



Alerts for Phishing, Malware, Ransomware, Vulnerability exploits, and Network intrusions grew in frequency over the past year. This growth continues a trend recorded in previous surveys and is a clear indicator that the pressure cybersecurity teams are facing never ceases to amplify.

Against the backdrop of a worsening economic environment, respondents are more concerned about budget constraints than they were a year ago (+6 pp). Nevertheless, they still consider the human factor (unsafe employee behavior, human error, shortage of cybersecurity skills/staff, remote workforce) a pervasive challenge.

Top cybersecurity challenges perceived

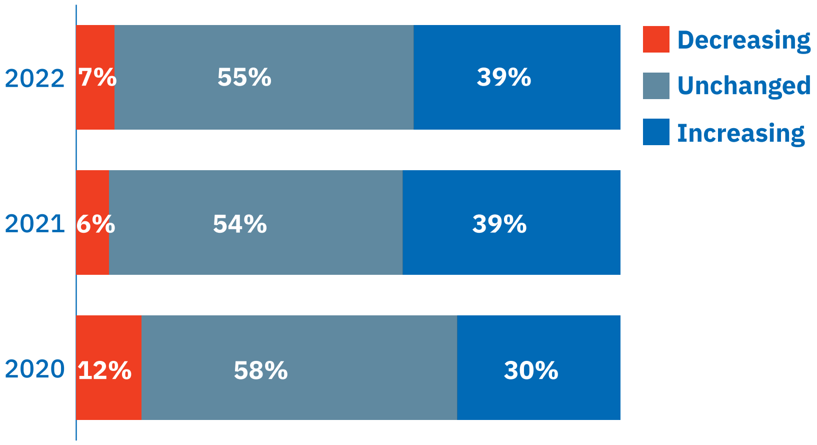


Future Outlook

Despite budget constraints, plans for increased spending on cybersecurity technologies continue almost unabated. Overall, cybersecurity budgets will continue to expand over the next 12 months, as the share of respondents who say their budget will increase (39%) vastly outpaces the percentage of those who say it will shrink (7%).

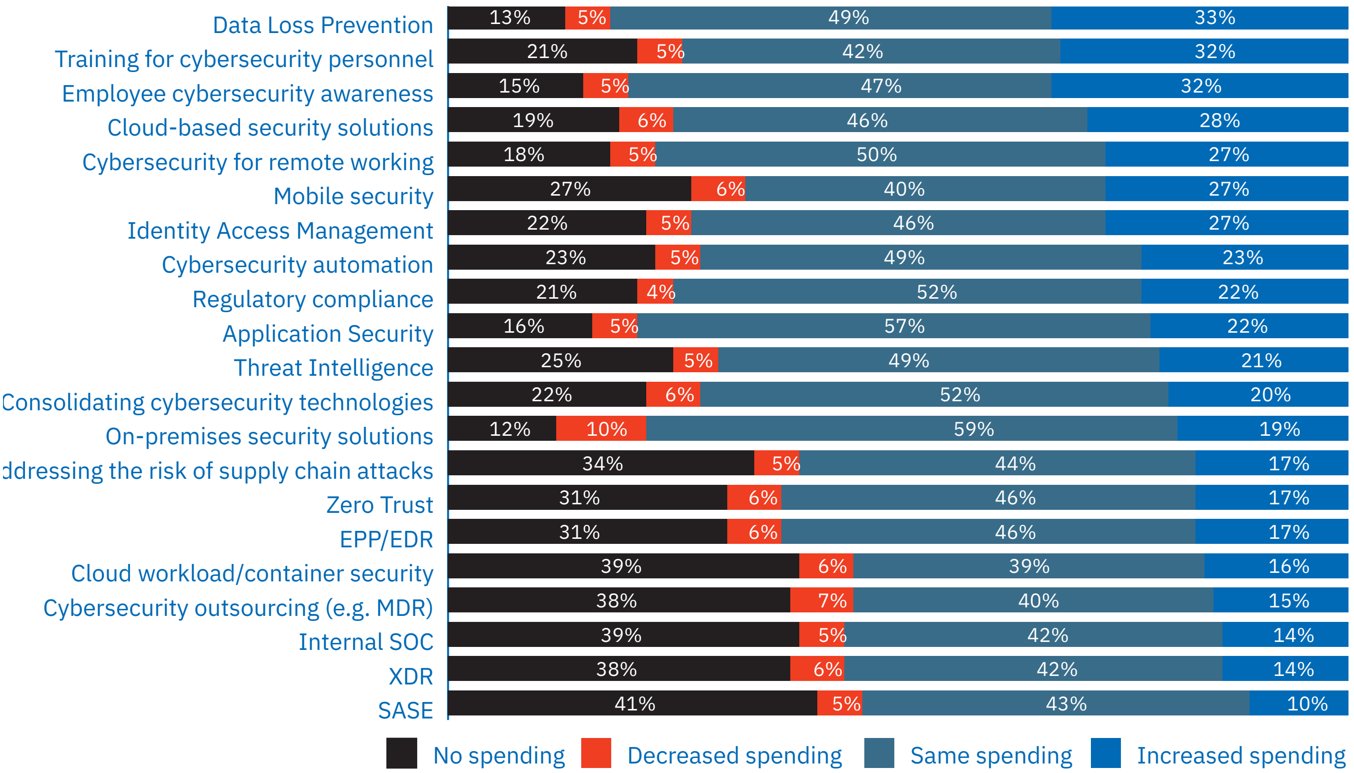
These numbers remain true for organizations of all sizes, proving that companies see cyber resilience as crucial to the survival and prosperity of their business.

Cybersecurity budget over the next 12 months



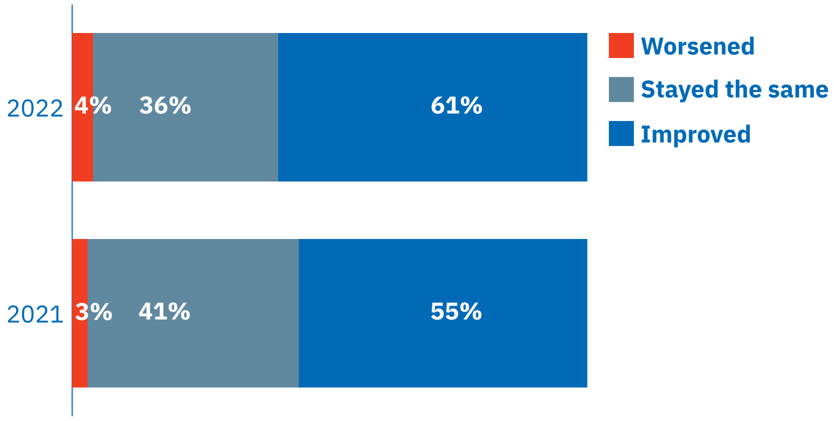
All cybersecurity technologies will see an increase in spending, as the share of those who say they will spend more in the future largely outruns the percentage of those who say they will spend less. Over the next 12 months, the highest increase in spending is forecast for DLP, training for cybersecurity personnel, security awareness training, cloud-based security solutions, and cybersecurity technologies for remote working. For these technologies, the share of respondents who say they will spend more outruns the cumulated share of those who say they will spend less or nothing.

Expected changes in cybersecurity spending over the next 12 months



Despite continued challenges, most organizations saw their cybersecurity posture improving in 2022, and only a few (4%) consider their security posture has worsened. Furthermore, the share of organizations who saw an improvement in their cybersecurity posture grew by 6pp from 2021, demonstrating the value of a wise investment in cybersecurity.

In your view, how has your organization’s overall cybersecurity posture evolved over the past 12 months?



ABOUT THIS RESEARCH

The Bitdefender Cybersecurity Posture Survey 2022 was conducted among 1,693 organizations during September-November 2022. The survey reached a broad spectrum of organizations of all sizes across all industries, from 100 countries across the globe. Over 90% of respondents are either decision makers or active users of cybersecurity solutions and software security products.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com