# **Next-gen Cybersecurity: Overview**



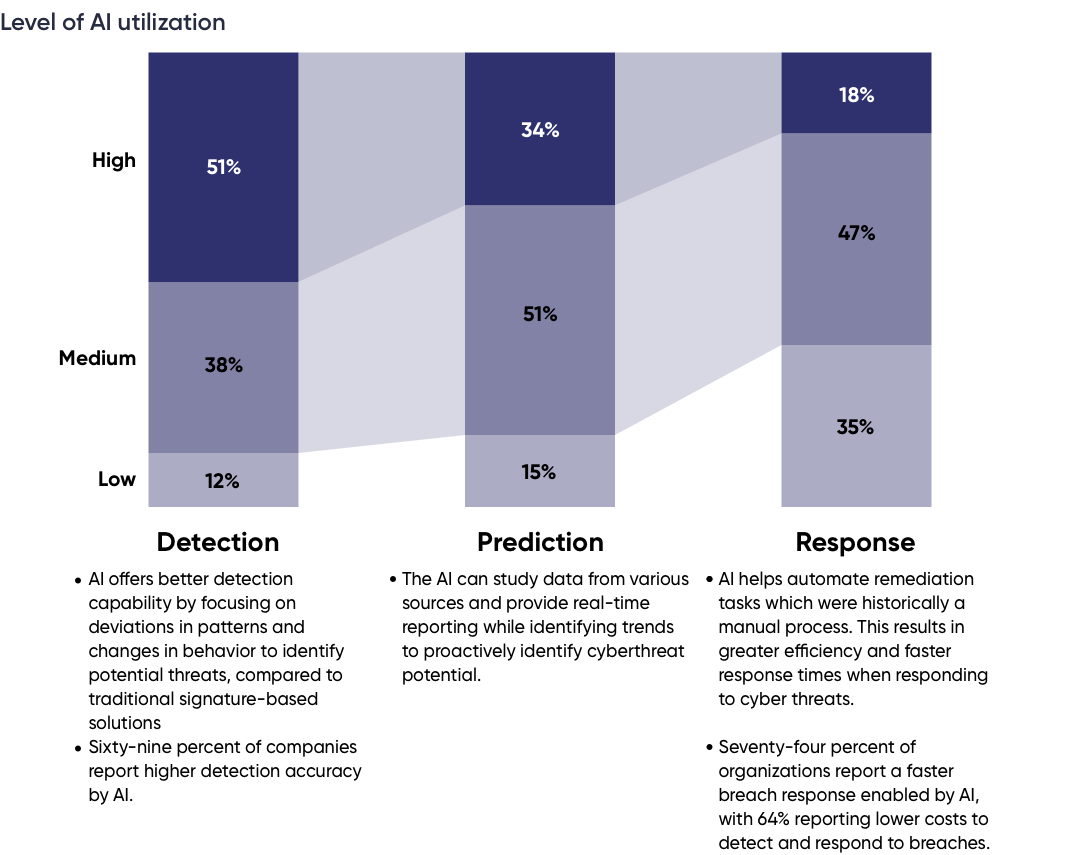
The traditional enterprise network perimeter is fading, and enterprise workflows are increasingly reliant on the internet and cloud applications. Businesses often rely on multiple cloud platforms from different providers, distributing their workloads, data, and applications across not only private networks but also public cloud infrastructure, leaving many potential entry points for malicious actors. Operational technology, such as manufacturing equipment, critical infrastructure, and healthcare devices, are also growing increasingly connected across all industries, providing cybercriminals yet another expanding target. This evolving threat landscape requires a holistic approach to cybersecurity that considers an organization's entire network landscape.

Advances in AI help companies bridge this gap by detecting threats using behavioral analysis. Companies can now use behavior-based methods to identify threats proactively, even unknown ones which would have otherwise gone undetected by traditional applications such as antivirus programs. AI also allows for efficient monitoring, investigation, and automation of common remediation tasks that would have been traditionally carried out manually—a time-consuming process prone to error.

## **The application of AI across different stages of a cybersecurity program**

AI, combined with machine learning (ML) and deep learning algorithms, has significantly bolstered the capabilities of cybersecurity platforms and improved the detection and responding capabilities of organizations. The use of analytics and big data makes it possible for algorithms to self-learn the workings of an organization's information systems by analyzing datasets and identifying trends. This also enables companies to proactively identify threats, devise response strategies, and keep pace with malicious actors who may also use AI to coordinate attacks and avoid detection. Indeed, corporations are using AI for threat detection at a much higher rate than for prediction and response functions.

### **Level of AI utilization**



Source: Compiled by Edge based on surveys by Capgemini and other sources

Large language models (LLMs) and other forms of generative AI are also rapidly becoming popular in the cybersecurity space. These AIs analyze threat data to assess and quantify risk, generate remediation advice and response code, produce threat and security insights, and even function as knowledge sources to alleviate the growing cybersecurity skills gap.

Cyber attackers are growing increasingly sophisticated, using AI to identify brand new vulnerabilities and in record time release malware capable of intelligently eluding all but the most powerful detection tools. Enterprise cybersecurity is at risk of being outpaced by attackers, and most industry players are investing heavily in AI to keep up.

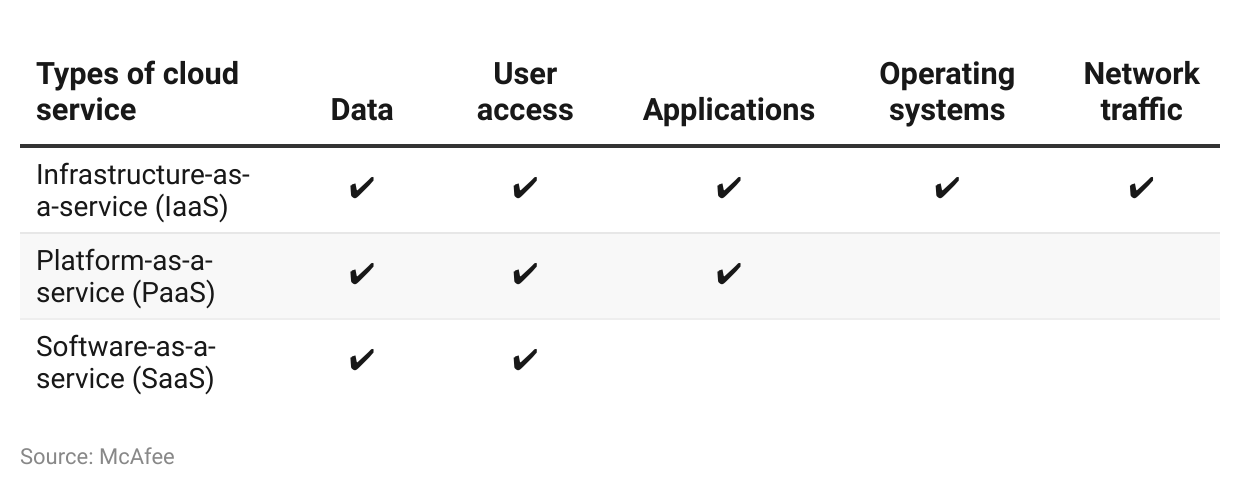
The rapid proliferation of AI has also brought with it new risks and opportunities for cybercriminals, such as vulnerabilities in enterprise AI applications and sensitive data leakage through AI chatbots, sparking investment in solutions to secure AI.

## **AI-based cybersecurity tools focus on the entire enterprise network landscape**

New cybersecurity startups offer solutions to secure cloud networks, cloud-native applications, endpoint protection, monitoring, detection, and response tools powered by artificial intelligence. Some startups are also offering platforms to monitor and protect industrial internet-of-things (IIoT) applications, along with managed services for detecting and responding to cyberthreats, and protecting enterprise application programming interfaces (APIs) and web applications.

**1. Cloud network security:** Platforms and technologies that protect enterprise data and infrastructure in the cloud from internal and external threats. While most public and private cloud providers offer some security features they cannot control how customers configure and utilize their services.

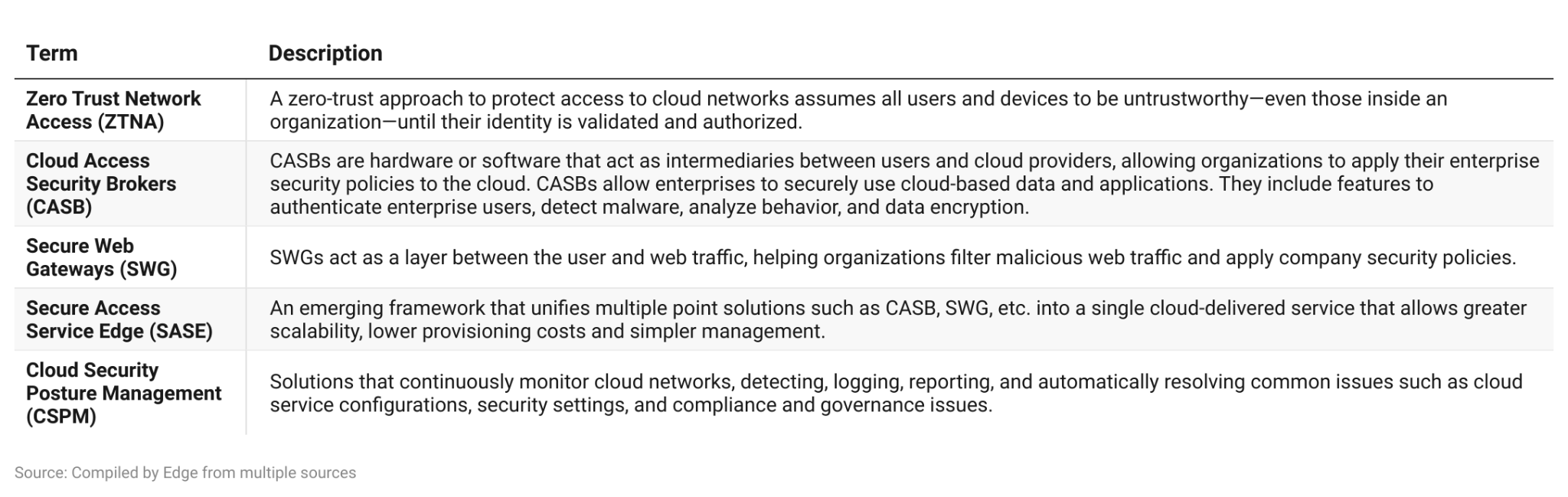
#### **Customer responsibility across cloud service delivery models**



Startups in this segment offer cloud security technologies which use AI to analyze a company’s entire cloud infrastructure to identify vulnerabilities, misconfigurations and any other malicious activity in order to proactively detect threats. Companies in this segment also offer tools such as Zero Trust Network Access (ZTNA), Cloud Access Security Brokers (CASBs), Secure Web Gateways (SWGs), which are delivered through the Secure Access Service Edge (SASE) framework. Growing complexity has led to the popularity of Cloud Security Posture Management (CSPM) solutions to secure cloud infrastructure.

### 

### **Key terms in cloud security**



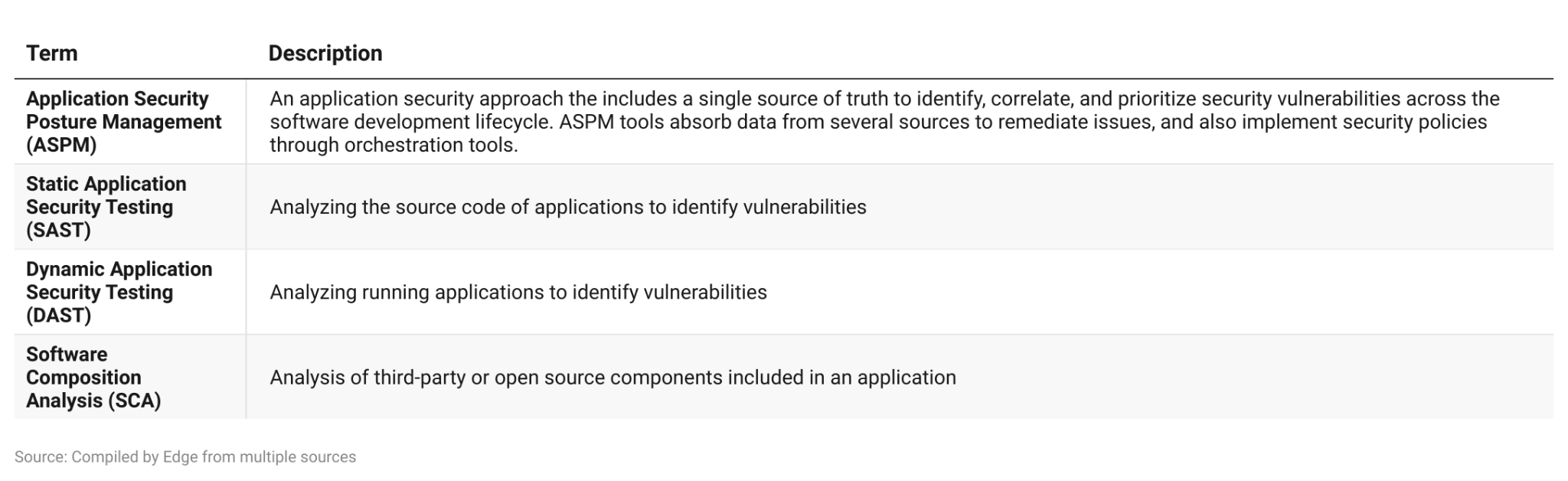
**2. Cloud-native application security:** Companies which provide solutions for enterprises to secure their cloud-native applications and workloads, across the entire development lifecycle—from build to runtime. Platforms offered by companies in this space are targeted for use by developers and integrate with DevOps tools, to find vulnerabilities and other security issues in the code for cloud-native applications. With the growing popularity of “Shift-Left” and DevSecOps, application security is integrated directly into the continuous integration/continuous delivery (CI/CD) pipeline throughout the development life cycle.

**3. Endpoint security:** The security of any device that connects to a corporate network including computers, mobile devices, ATM machines, Point of Sale (POS) devices, etc. Endpoints are a prime target for malicious actors to infiltrate a network and inject ransomware or steal sensitive data. Endpoint security is a company’s first line of defence.

Startups in this space offer Next-gen Anti-viruses (NGAVs), Endpoint Detection and Response (EDR) solutions, and Endpoint Protection Programs (EPPs). These all use AI and machine learning to detect zero-day threats, analyze activity data to identify trends, and automate responses and remediation in real-time. Compared to legacy endpoint protection software, which focuses on a single endpoint and relies on signature-based methodologies to identify threats, newer endpoint solutions focus on macro-level factors and rely on behavioral analysis to identify advanced threats.

### 

### **Key terms in endpoint security**



**4. Industrial IoT and Operational Technology security:** Companies in this space protect connected industrial hardware and operational technology (OT) with tools that obtain full visibility into connected industrial IoT (IIoT) devices, monitor the behavior of IIoT and OT assets, detecting vulnerabilities, and anticipate attacks to critical infrastructure.

**5. Detection and response tools:** Leverage AI to monitor an organization’s entire infrastructure to identify threats, provide tools for incident investigations, and help automate remediation tasks. Most startups in this segment offer extended detection and response tools (XDR) that extend beyond EDR platforms to collect data from non-endpoint sources such as networks, cloud infrastructure, etc.

**6. Managed detection and response:** MDR is an emerging branch of managed security service providers (MSSP). Unlike traditional MSSPs, MDR providers offer in-depth threat hunting and resources to detect and respond to both known and unknown cyber threats. MDRs support businesses with AI-based cybersecurity platforms and human resources for 24/7 threat monitoring and response.

**7. API and web application security:** Companies that offer solutions for the protection of enterprise APIs and web applications against external threats such as scripting, bots, denial of service attacks, skimming, Personally Identifiable Information (PII) harvesting, etc.

# 

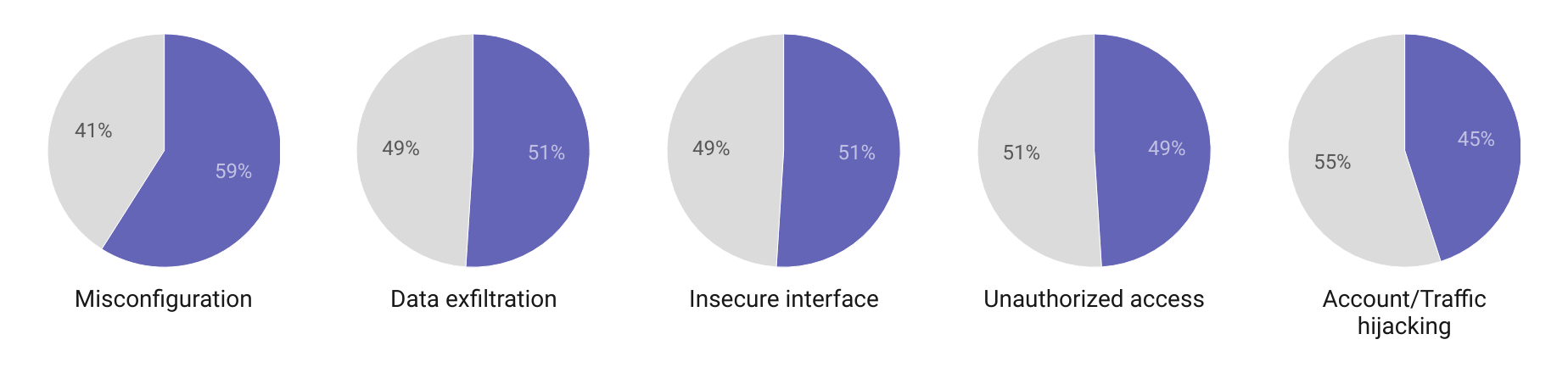
# **Driving factors**

## **1. Greater threat of data breach due to increased cloud adoption**

An overall corporate shift to cloud-based applications and SaaS products such as file servers, storage applications, business applications (such as customer relationship management and enterprise resource planning software), disaster recovery, and high availability applications, offer greater reliability, accessibility, and on-demand scalability for companies—helping to drive down associated IT overheads by up to 40%.

Organizations using cloud services are responsible for securing access to these services and the underlying data, especially under SaaS models. As a result, the threat of unauthorized access and data leaks resulting from poorly configured cloud environments or identity theft are among the key security threats facing cloud usage.

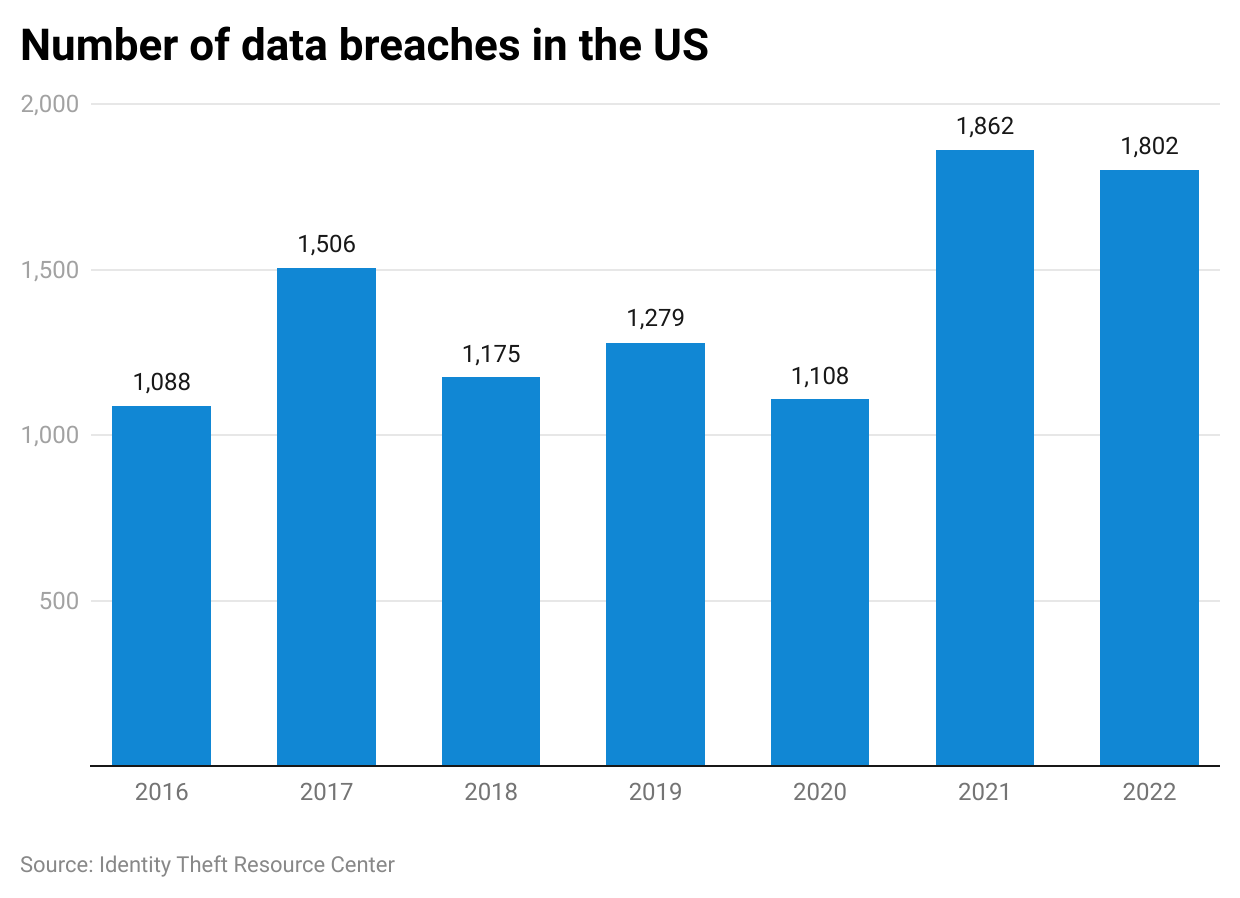
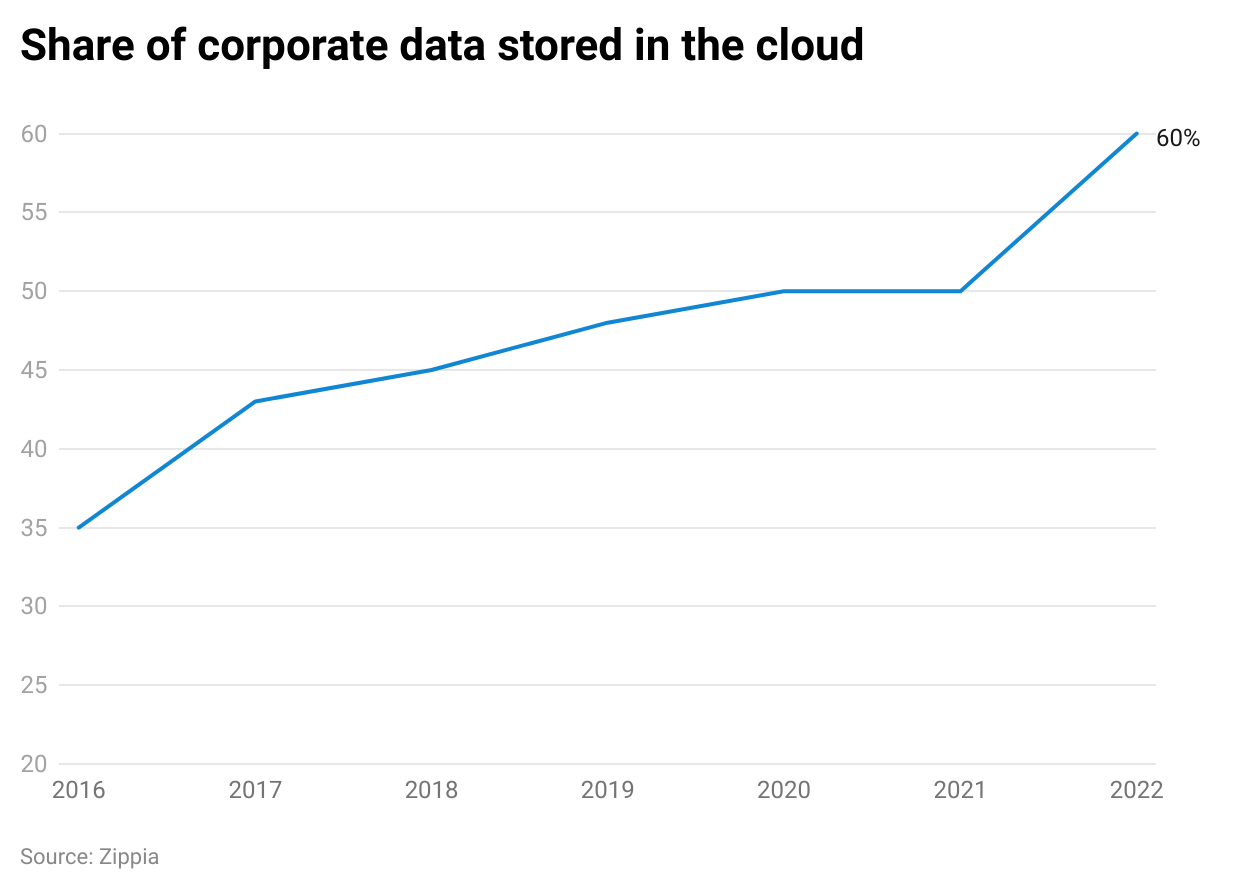
### **Biggest cloud security threats reported by organizations**



The cloud also poses new cybersecurity challenges due to the involvement of third-party providers and the use of public networks, resulting in very limited visibility and control over the data and infrastructure.

* 76% of cybersecurity professionals reported they were extremely or very concerned about the security of public clouds, and 24% reported they had experienced a public cloud-related incident in a 12-month period.
* In 2022, more than 420 million individuals were affected by 1,802 data breaches and exposures in the US, representing an increase of almost 42% in the number of individuals affected compared to 2021. The figure is inflated by a breach at Twitter in December that affected over 221 million users, having trended downward for the first 11 months of 2022.
* Cyberattacks per organization grew 38% from 2021 to 2022, mostly driven by smaller ransomware groups; 30% of all attacks contained ransomware in 2022.

### **Data breaches have been growing as enterprises move workloads to the cloud**



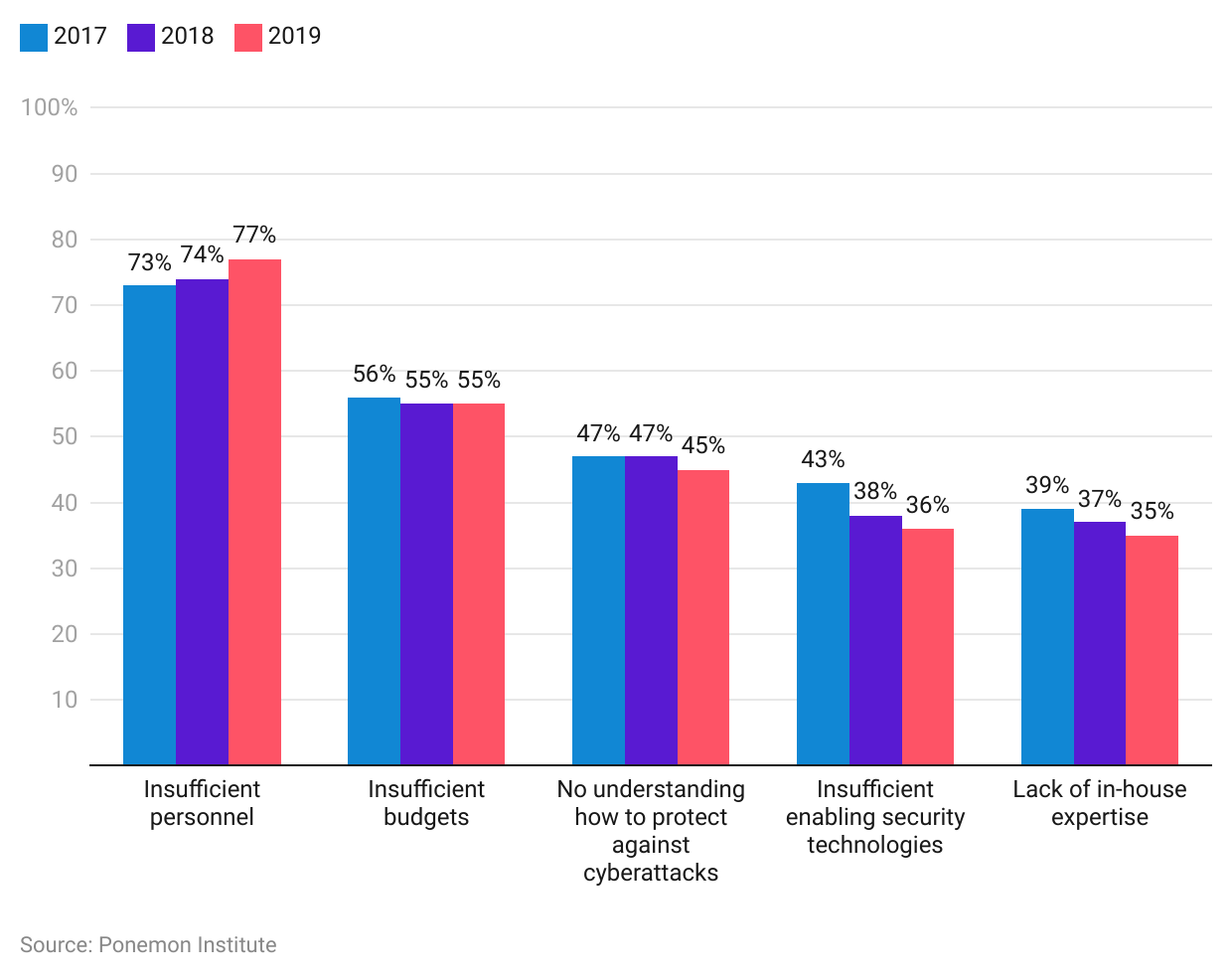
## **2. Two out of three SMEs are victims of a cyberattack. Lack of personnel and limited budgets result in ineffective protection**

Nearly two-thirds of US small and mid-sized businesses reported a cyber attack of some sort in 2021. SMEs—which represent 99% of all US corporations—often rely on consumer-grade protection solutions while some companies do not use any endpoint protection whatsoever, leaving employee laptops and mobile devices vulnerable to malicious actors.

While almost a third of SMEs rate their internal security postures highly, most SMEs are struggling, citing a lack of staff and budgetary constraints as the primary roadblocks to tackling cybersecurity threats.

### 

### **Challenges for SMEs against an effective cybersecurity posture**



Nearly 70% of SMEs reported the use of at least one cybersecurity tool, and more than 40% expect to increase cybersecurity budgets. Few SMEs reported using AI or equivalent technology. Lower adoption by SMEs is largely due to cost considerations, lack of knowledge, and little to no experience with AI-based technologies.

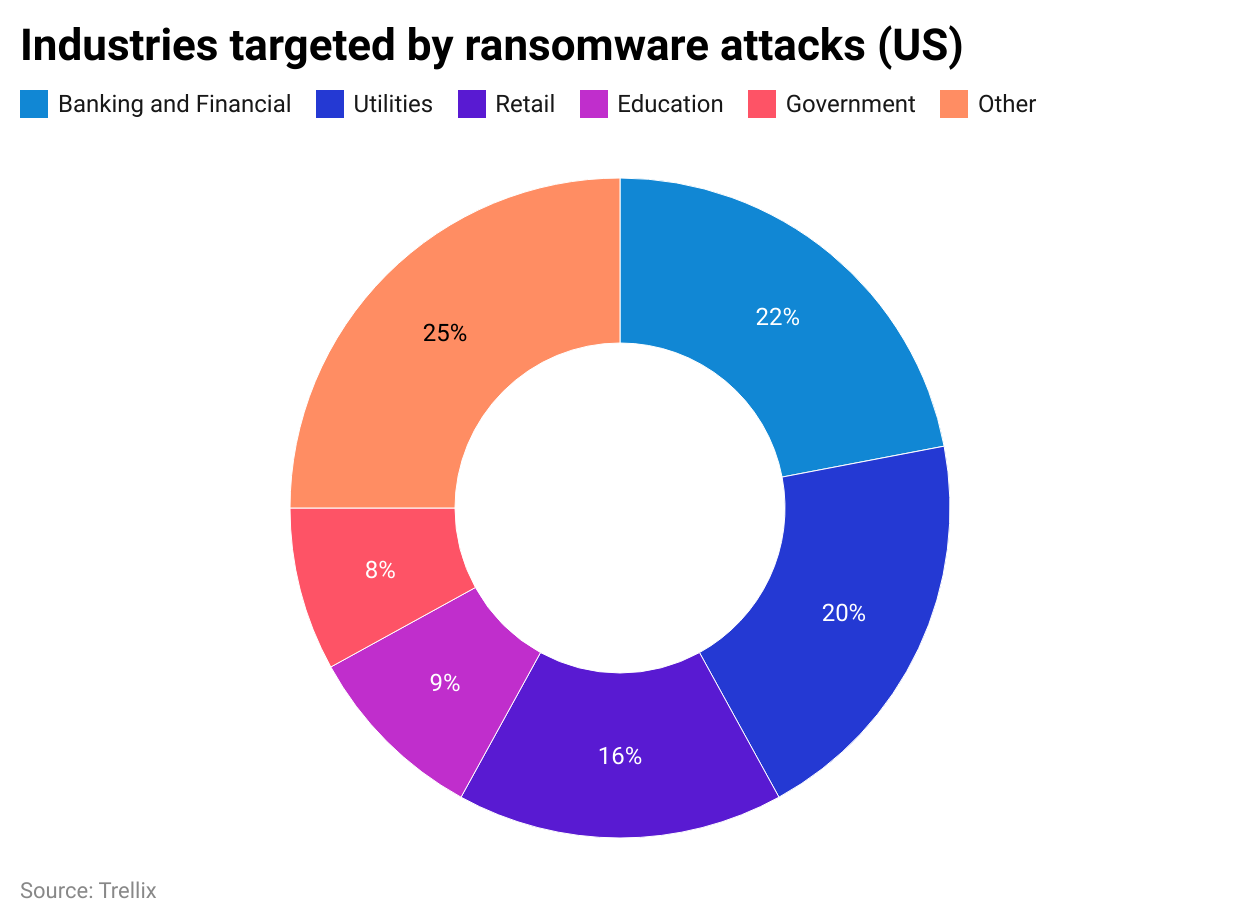
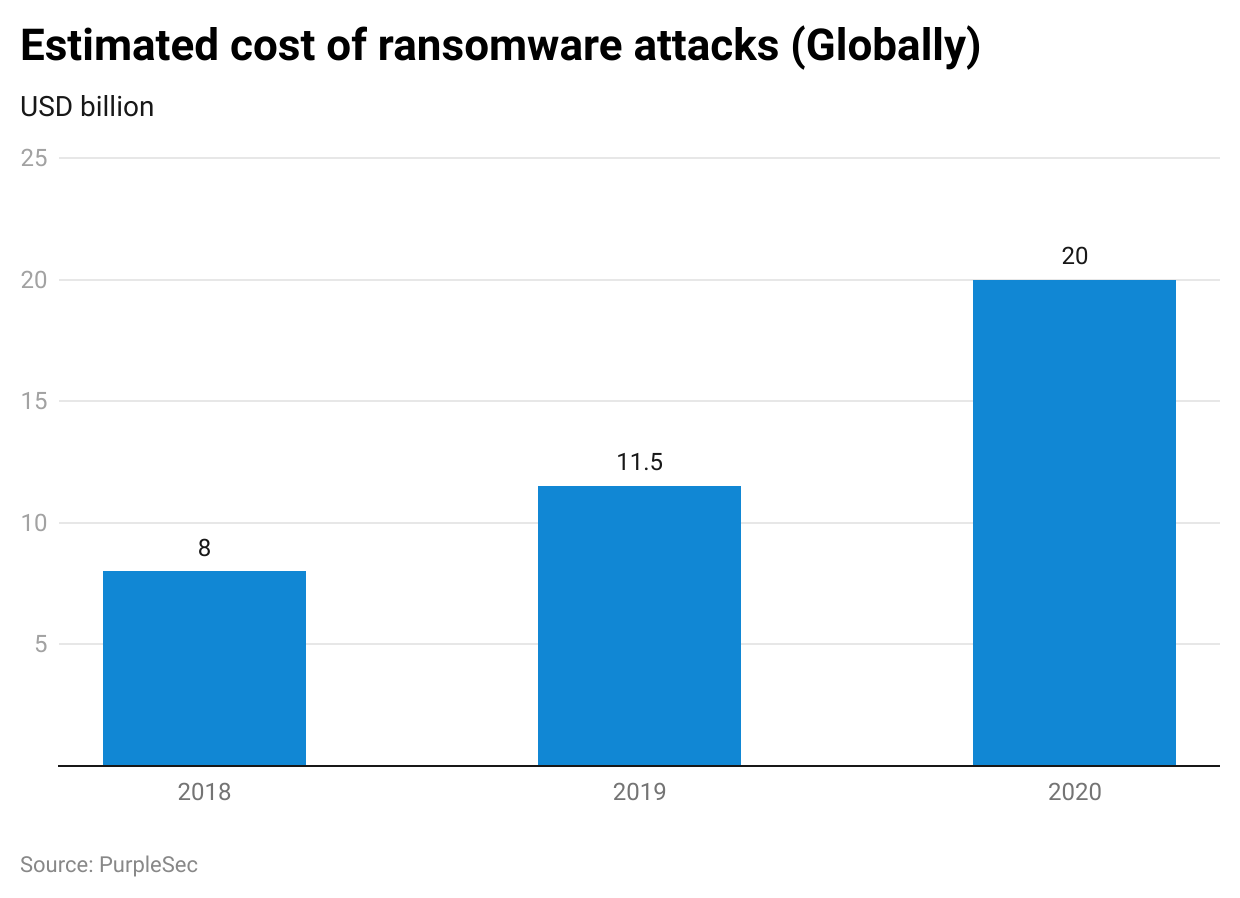
Managed security service providers (MSSPs) such as MDR vendors also stand to benefit as SMEs are increasingly looking at them as an option to support their security within staffing and budgetary constraints. MDR vendors operate a model at scale with fully-trained staff that allow them to apply learnings from multiple clients. In addition, these companies are also able to obtain better deals from solution vendors given their volume. This generally results in lower costs, especially for small businesses, compared to managing in-house cybersecurity teams.

## 

## **3. Ransomware and other “smarter” malware are becoming harder to detect**

Ransomware is becoming more common with the emergence of Ransomware-as-a-Service and ransomware kits, which are available on the darkweb and can be deployed with little to no technical knowledge. Organizations risk permanently losing the data or having confidential data leaked online in the event of non-payment. Ransomwares have grown to become a very popular form of attack, with the number of attacks increasing by more than 100% year-over-year in 2021.

Only 35% of security professionals believe that their organizations are prepared to fight a ransomware attack. The financial impact from ransomware attacks globally was estimated at USD 20 billion in 2021, growing 57x from 2015, and downtime resulting from ransomware attacks increased by 23% YoY.

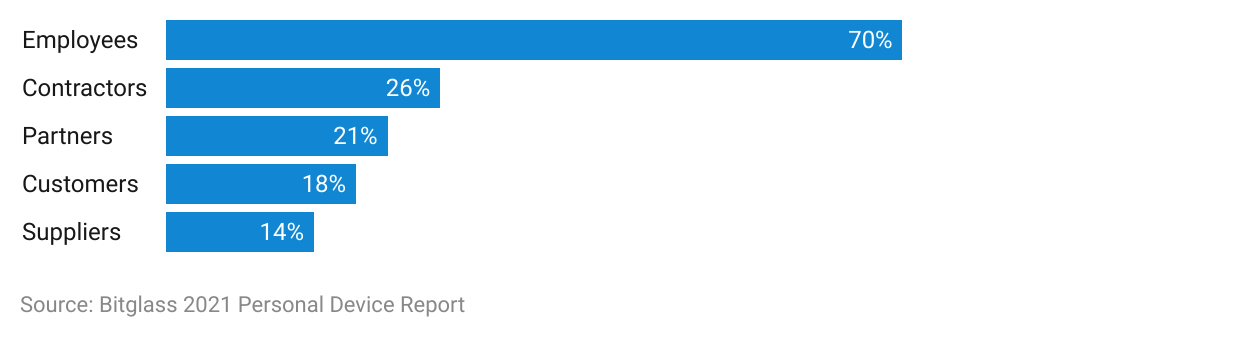


Seventy-five percent of companies which were infected with ransomware were running the latest versions of their endpoint protection software. The endpoint protection company Malwarebytes predicts that new kinds of malware will use AI to carry out precisely targeted attacks and employ built-in self-learning mechanisms to avoid detection. These sophisticated threats will require advanced endpoint protection solutions that rely on AI and behavioral analysis to identify malicious behavior and previously unknown threats proactively by blocking them prior to execution, automatically isolating suspected endpoints, and rolling back data following an attack.

## **4. New cyber attack vectors develop from a new reality of networked corporate devices**

Corporate networks are now serving more than just traditional endpoint devices. With remote work becoming the norm, the bringing your own device (BYOD) trend is surging and employees are increasingly using personal, unmanaged devices to connect to corporate applications from unsecured networks. This is further exacerbated by extended stakeholders such as contractors, suppliers, and customers who require access to company systems. Overall, 82% of organizations have enabled BYOD policies, with most organizations allowing employees to use their personal devices for work.

### **Percentage of organizations that enable BYOD by user group**



While BYOD is said to increase employee productivity, it can also pose security challenges such as risks of data retention by former employees, lost devices, unauthorized access to systems, and risky data transfers. Cloud security solutions such as zero-trust access and CASBs can act as a layer between unmanaged devices and enterprise cloud applications to protect access and unauthorized use of data.

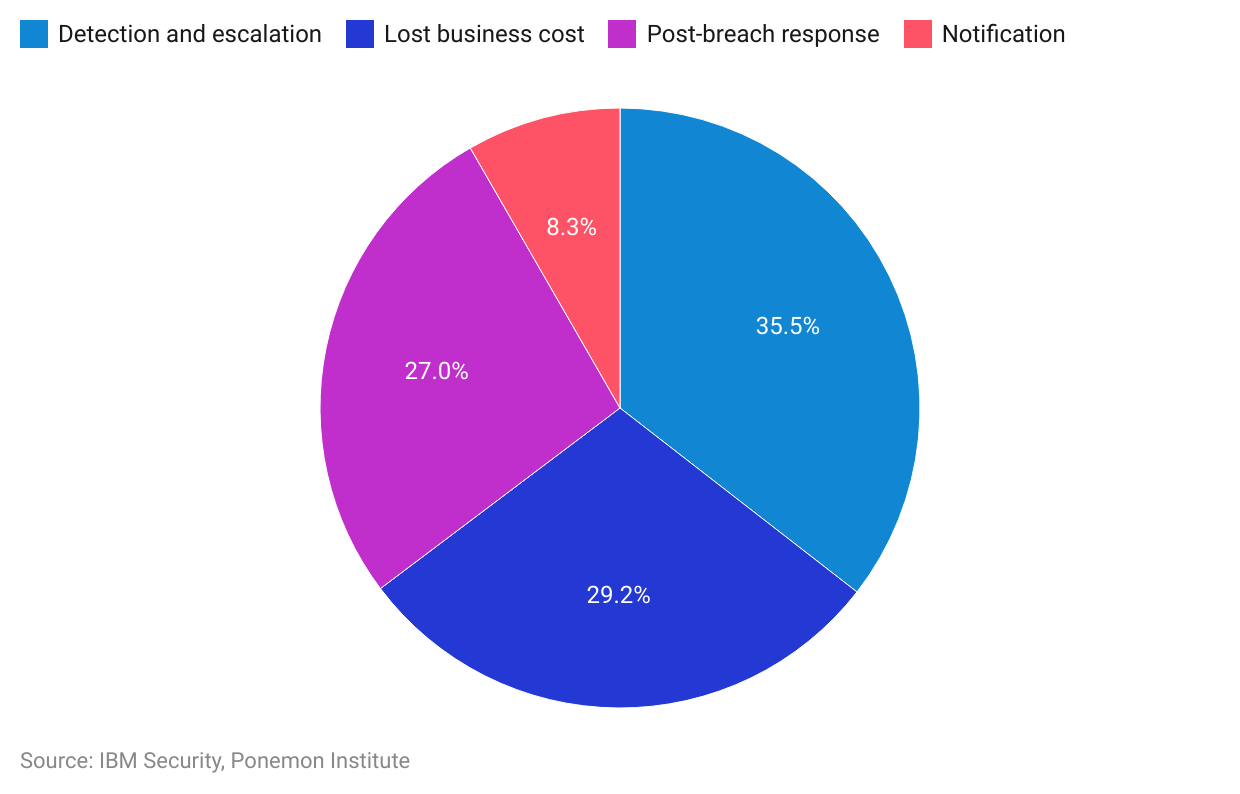
Organizations also use operational technology (OT) and industrial internet-of-things (IIoT) devices in their corporate networks, exposing them to cybersecurity risks resulting from distributed denial-of-service (DDoS) attacks, unpatched software vulnerabilities, remote access trojans (RATs) and other critical infrastructure attacks. Alarmingly, two out of every three devices use IoT, and an average of 48% of enterprise endpoints are at risk due to not being discoverable by IT departments or due to outdated operating systems.

## **5. High costs of breach can be significantly offset by effective cybersecurity tools**

The average cost of a data breach in the US totalled USD 9.5 million in 2022, compared to a global average of USD 4.5 million. The largest cost contributor is detection and escalation activities including breach detection, forensic and investigative actions, assessments, audits, crisis management, and communication to boards. In the US, 75% of consumers will stop spending at a business for months following a breach, with 12% claiming they will never return to an affected business.

### 

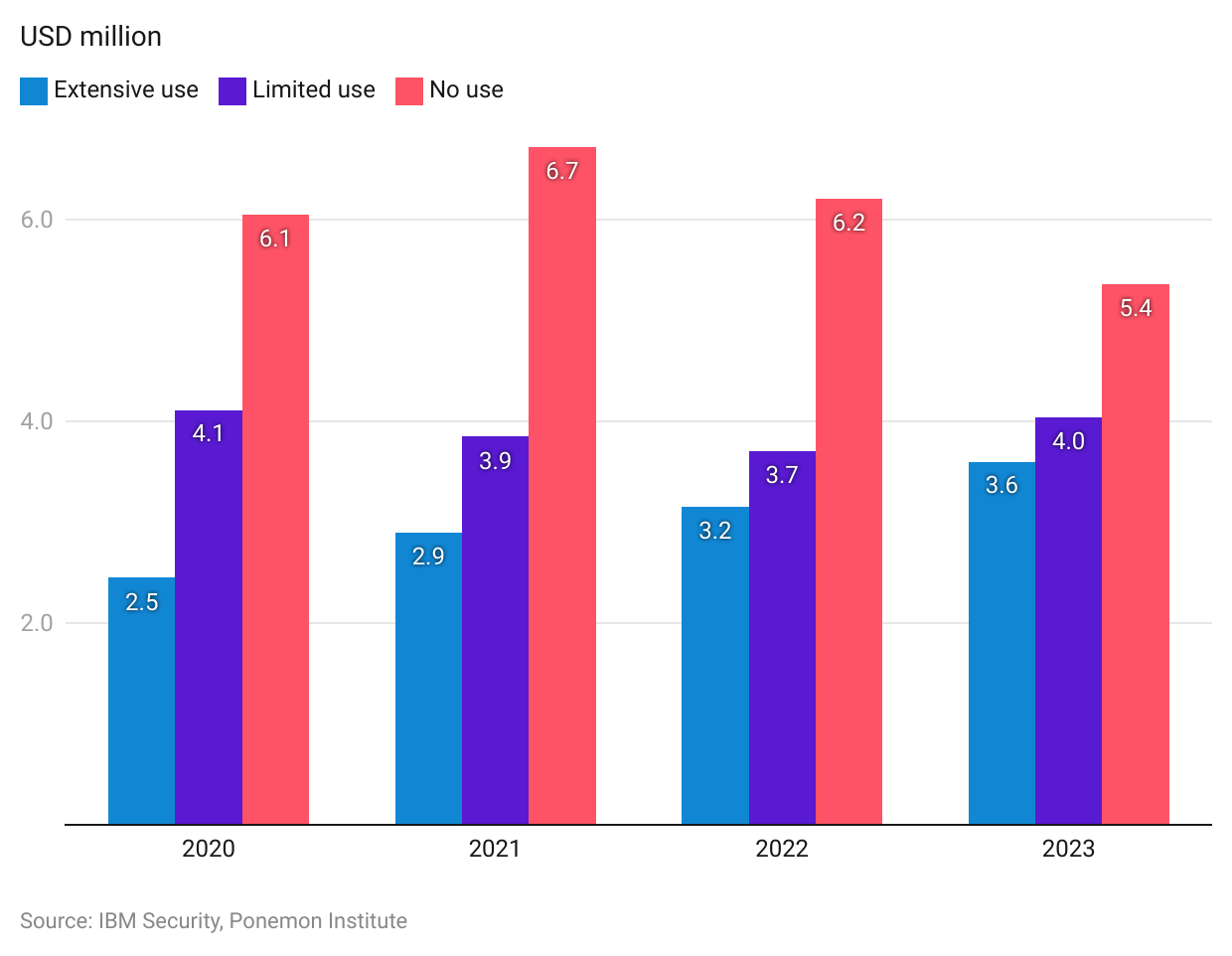
### **Contributors to data breach costs**



Globally, companies that had not deployed any cybersecurity AI and automation tools incurred USD 5.4 million in breach expenses on average in 2022. Companies with extensive use of AI and automation saved USD 1.8 million in breach costs, a difference of nearly 40%, and organizations that used these technologies to a limited extent also saw savings of nearly 30%. Extensive security automation reduced time to identify and contain a breach by 108 days compared to no use.

### 

### **Cost of breach and savings gap by AI and automation deployment levels**

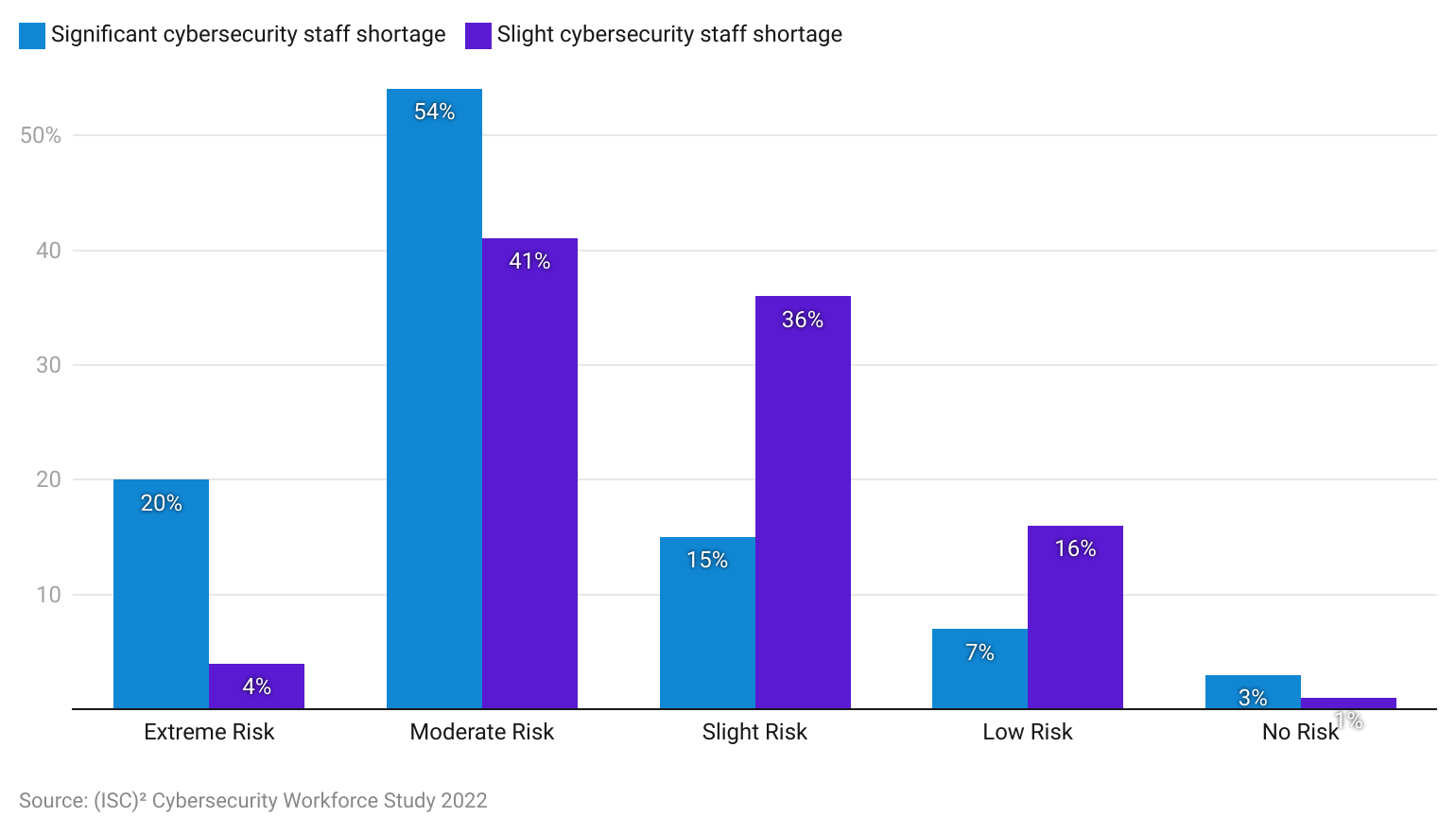


More than 80% of breach attacks originated from web applications, as cyber criminals continue to exploit application weaknesses and software vulnerabilities to access corporate databases. Examples of web application attacks include cross-site scripting (malicious scripts injected to websites), SQL injection (to access and modify content from company databases), distributed denial of service (DDoS) attacks, skimming, and web scraping.

## **6. Shortages in cybersecurity skills drive companies to explore automation and MDRs in order to support cybersecurity efforts**

As the demand for cybersecurity services increases, companies are experiencing a shortage of specialists. Nearly 70% of cybersecurity professionals reported staff shortages in their own organizations, with more than half stating that these shortages directly place organizations at a higher risk of cyberthreats.

### **Cybersecurity risk according to severity of staff shortage**



The cybersecurity workforce grew 11.1% to nearly 4.7 million in 2022, adding more than 464,000 workers. Shockingly, demand grew twice as fast as supply; an additional 3.4 million cybersecurity professionals would be needed to fill all necessary positions globally, a growth of 26.2% compared to the previous year. The US accounted for over 410,000 of the global gap.. In addition to important human resource actions to train and retain existing staff, organizations will need to deploy automation across all aspects of their cybersecurity programs to make efficient use of any available staff.

Small businesses are also looking at MDRs to access talent at a lower cost. The MDR model allows these companies to operate at scale by serving multiple clients. Organizations can use technical and human resources from these MDR vendors to protect their systems with 24/7 threat monitoring and remediation support instead of having to manage this function internally.

# **Risks to growth**

## **1. Lack of awareness and training lead to inefficient use of cybersecurity tools**

More than half of companies indicate inadequate staff training and/or a shortage of skilled team members put them at risk of a cybersecurity attack. Further studies show that cloud security tools, such as Cloud Access Security Brokers (CASBs) are underutilized, largely due to a lack of knowledge and training to effectively use these services. This is exacerbated by the already existing skills gap in the sector, with 50% of companies lacking staff to operate cloud security tools.

In addition, one out of four SMEs does not trust AI for cybersecurity due to inexperience and a lack of awareness of its enhanced capabilities. This could restrict uptake as companies might not be fully aware of newer solutions or the limitations of existing solutions.

Organizations have to prioritize staff training to bolster their cybersecurity defense capabilities as affirmed by the fact that 93% of organizations rank training of IT staff as a key element of maintaining a strong security posture. MDR vendors can capitalize on this gap by offering support to companies to manage threat detection and response with a skilled workforce.

## **2. Limited cybersecurity budgets**

Limited cybersecurity budgets are still a key constraint for enterprises, though this has fallen behind IT complexity and the security skills gap in recent years, with 29% reporting it as a barrier for adoption. 73% of organizations forecast an increase in cybersecurity budgets in 2023.

## **3. Privacy concerns can inhibit adoption of certain cybersecurity solutions**

Cybersecurity professionals see a loss of privacy as a potential risk of using AI in due to the volume of data ingested by these algorithms. Thirty-seven percent see data privacy concerns as a key barrier to cloud security adoption. In addition, privacy concerns can also be expressed by end users for endpoint security applications. This is especially the case in BYOD environments as 59% of organizations require physical access to devices and 52% require device pin codes to implement security policies. Some users may see this as a violation of their privacy.

*Last updated: September 2023*

©2024 Uzabase, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Uzabase Inc. and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Uzabase Inc. nor its content providers are responsible for any damages or losses arising from any use of this information.