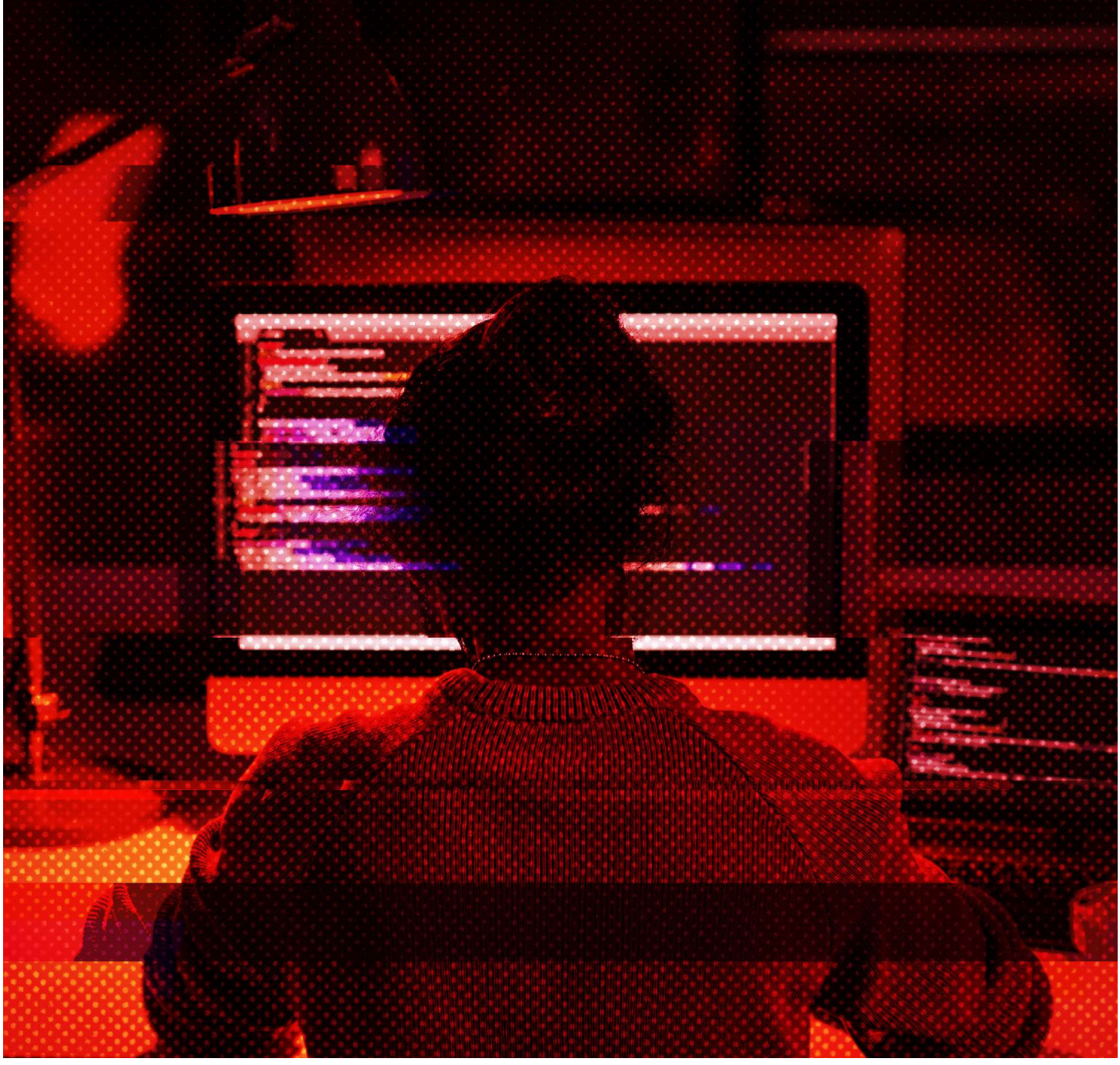
Trend Research

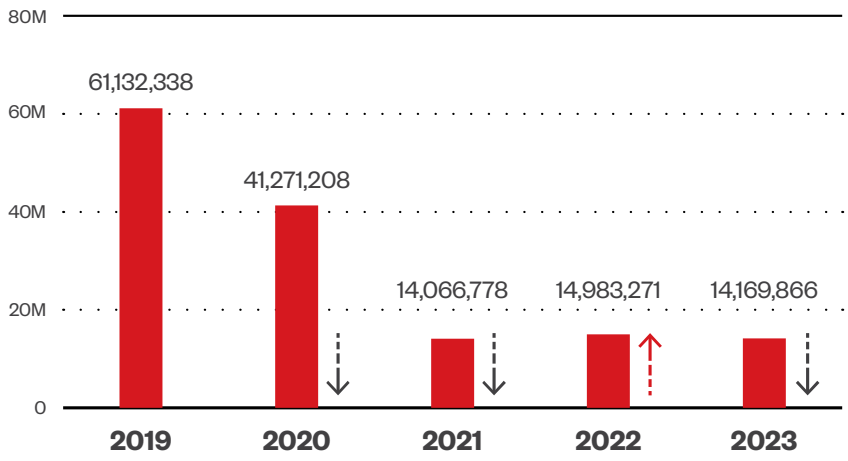
TREND MICRO

CALIBRATING EXPANSION

2023 ANNUAL CYBERSECURITY REPORT

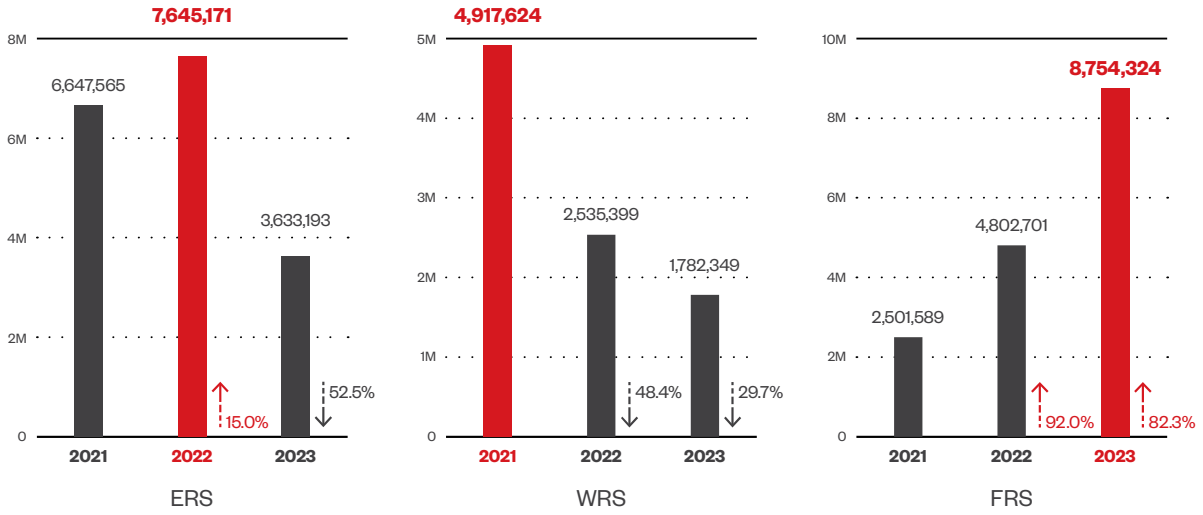


Total Ransomware Detections

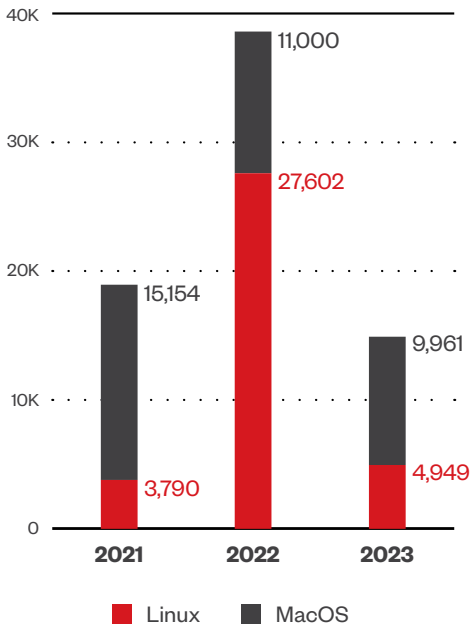


There has been a general downward trend in ransomware detections, with detections from 2021 to 2023 averaging less than half of the recorded detections in 2020; however, this should not be misconstrued as a cue for security operations centers and decision-makers to lower their guards. Historically, ransomware attacks were launched in "bulk," such as spam campaigns with malicious links, but attacks that focus on quantity can more easily be blocked, as shown in our ransomware ERS and WRS data in the following figure. These figures show a general downward trend consistent with the total ransomware detections.

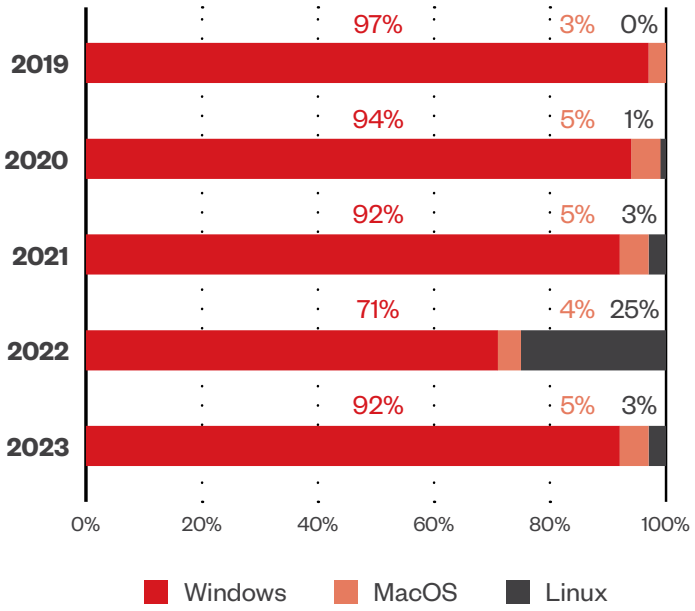
However, a continued increase in FRS detections could suggest that attackers are using more effective ways to evade preliminary detection by focusing on arrival and defense evasion techniques such as Living-Off-The-Land Binaries and Scripts (LOLBINs/LOLBAs), Bring Your Own Vulnerable Driver (BYOVD), zero-day exploits, and AV termination. We detect and identify ransomware payloads as malicious at endpoint as the ways they get into systems become more complex. This pattern is also observed in SPN data for overall threats blocked.



Operating Systems Affected by Ransomware



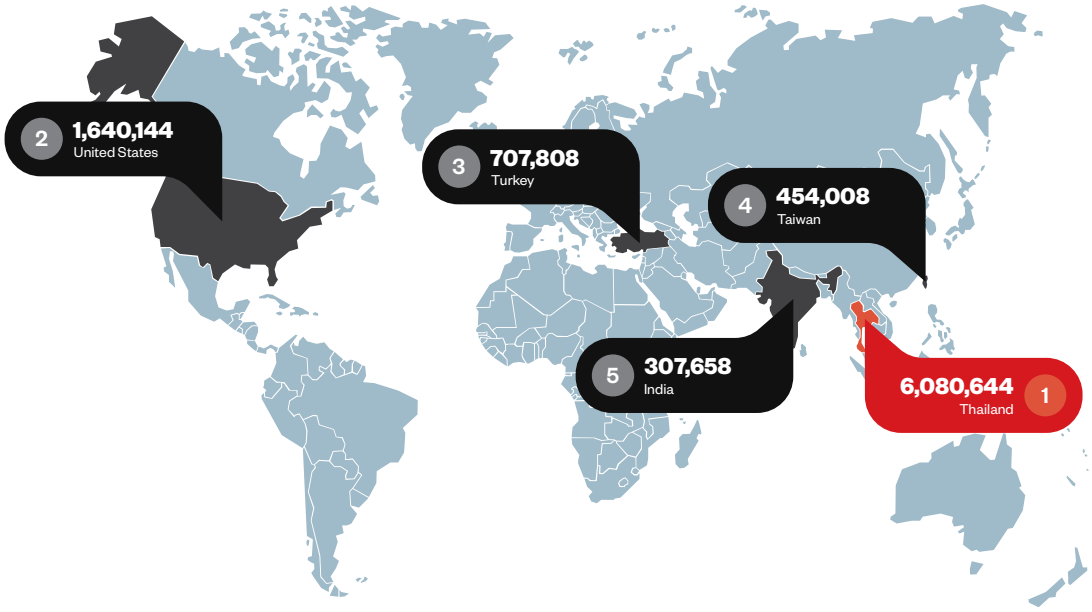
Based on data from our midyear report, customer detections on Linux-targeted ransomware attacks from the first half of 2023 continues to overshadow MacOS attacks. This is consistent with data gathered from 2022, which was an exceptional year for Linux-based malware detections, making up 25% of our telemetry; previously, Linux-targeted attacks only made up two to three percent of the OS ratio. It should be noted that Windows continues to take the bulk of our ransomware detections, with the only significant decrease in 2022.

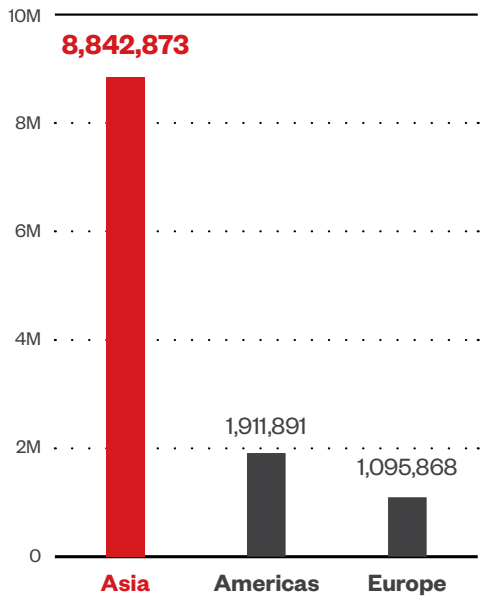


However, as our data for 2023 was completed, MacOS ransomware attacks came out higher with 9,961 detections, while Linux detections were finalized at 4,949. This could suggest that Linux-targeted attacks are stabilizing after the influx of novel Linux variants in 2022 to early 2023, but it could also be influenced by the overall decrease in ransomware activity.

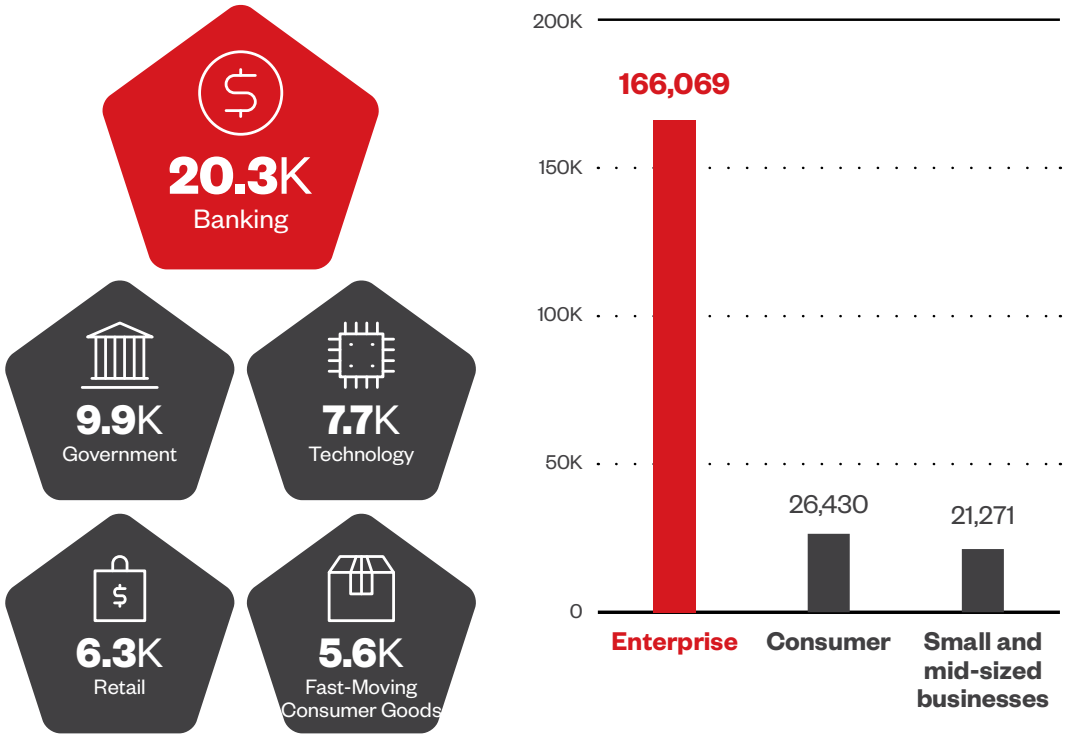
Top Countries and Regions by Detected Ransomware Attacks

Thailand made up 68% of ransomware detections in Asia.





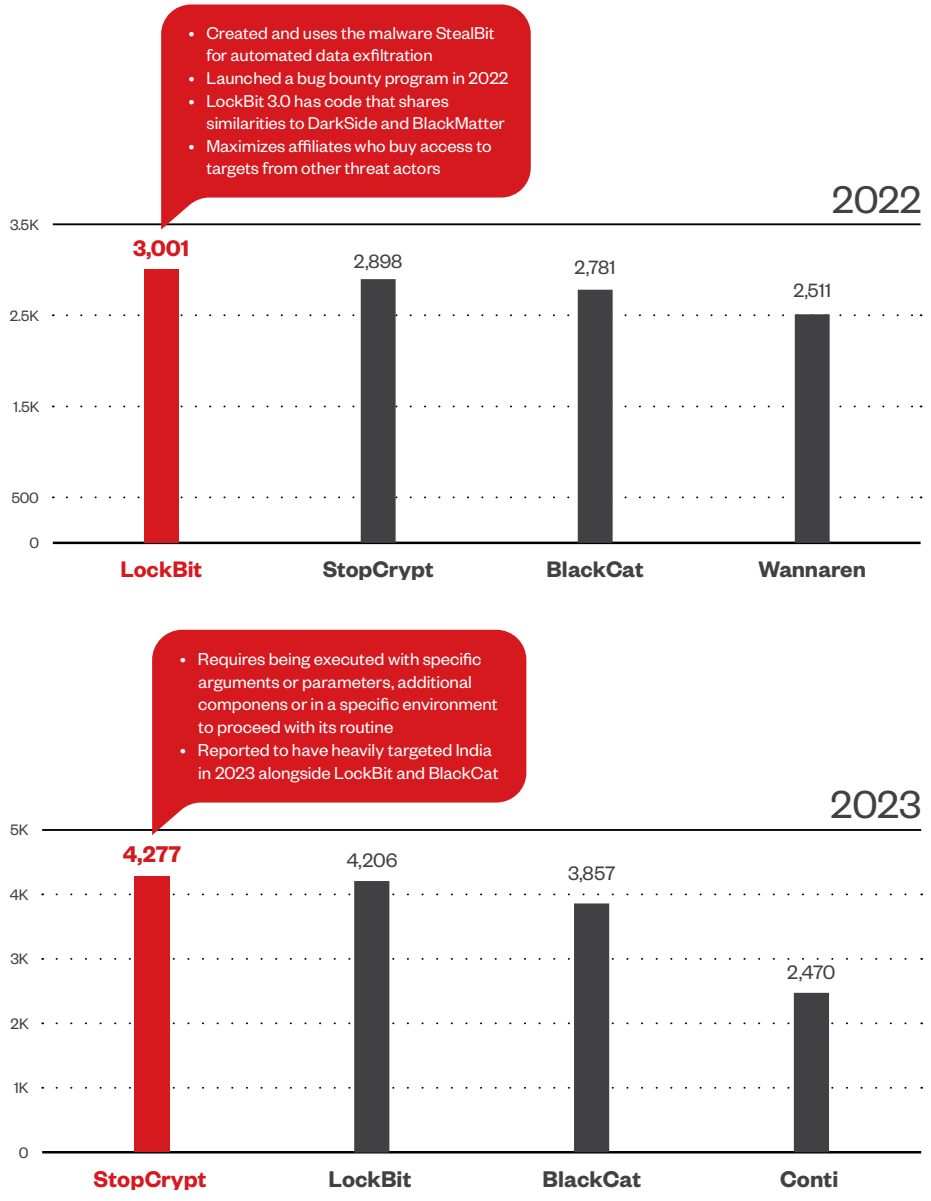
Top Industries and Segments by Detected Ransomware Attacks



Industry rankings and segment breakdowns based on unique detection counts at the endpoint shows that enterprises are the primary targets, with significant interest in the banking sector in 2023.

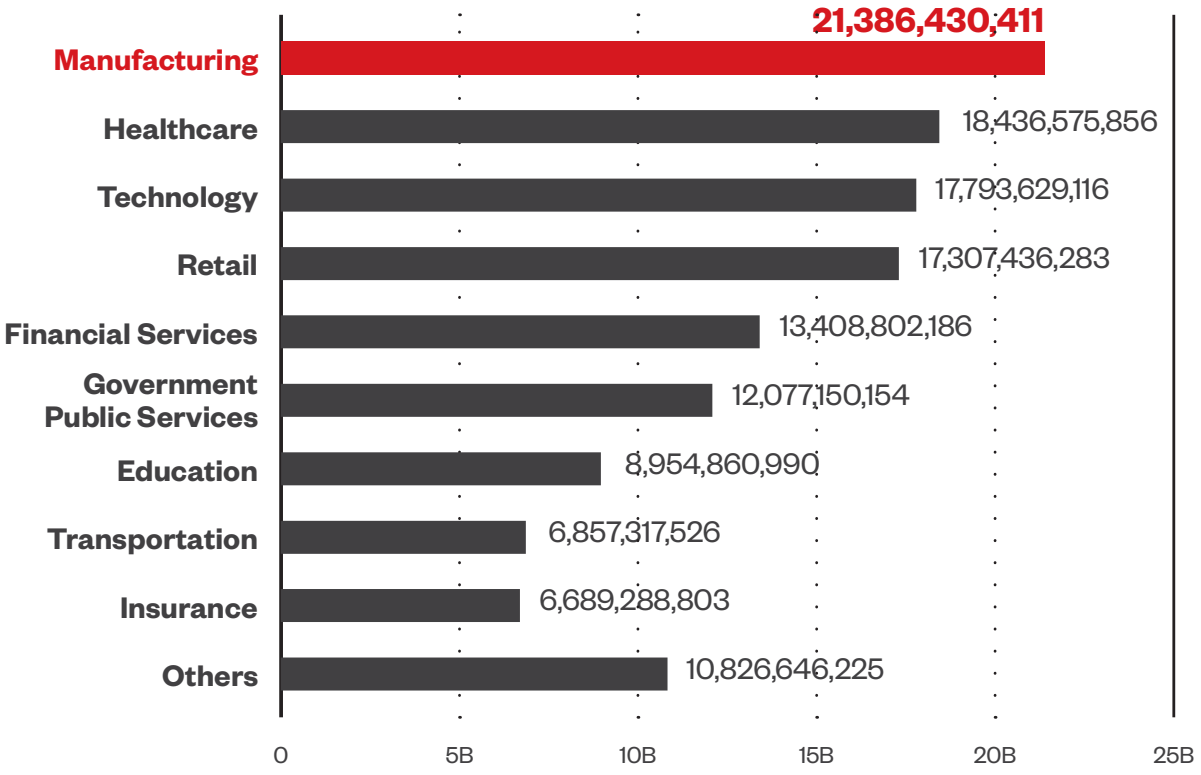
Top Ransomware Families

StopCrypt and LockBit maintain the top spots in terms of most prolific ransomware families for 2023 as it did in the previous year, but the former overtook the latter by a narrow margin this year. Note that this data does not include legacy ransomware families.



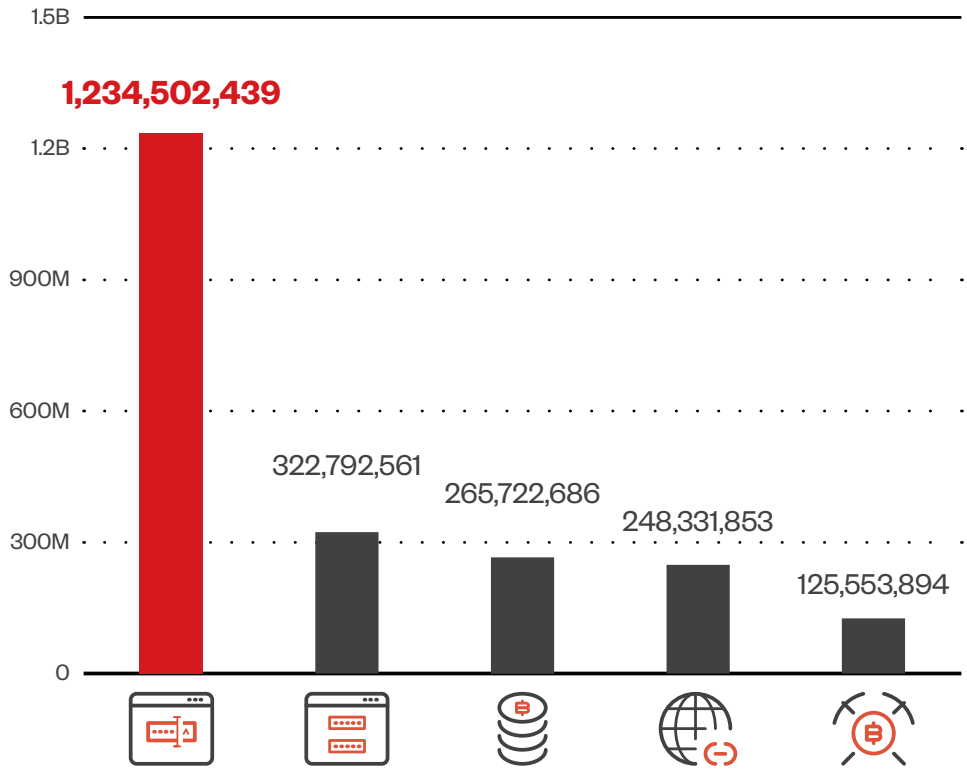
Risk Events

Top Industries by Risk Events (ASRM)



Home Network Security Top Events

With hybrid work now established as part of business operations, we looked at our Home Network Security telemetry to see what specific events cybercriminals particularly favor to use and what devices they target to maximize the larger attack surface created by remote and home workspaces.



Brute-Force Login

- Might be RDP via port 3389, FTP via port 21, or SSH via port 22 to repeatedly attempt to log in to target hosts using a dictionary of common usernames and passwords

TELNET Default Password Login -6

- Detects when a user within the network uses the default password to log in

MISC Bitcoin/Litecoin/Dogecoin Mining Activity -1

- Related to information disclosure and possibly to Bitcoin/Litecoin/Dogecoin Mining Activity

WEB HTTP Invalid Content-Length -2

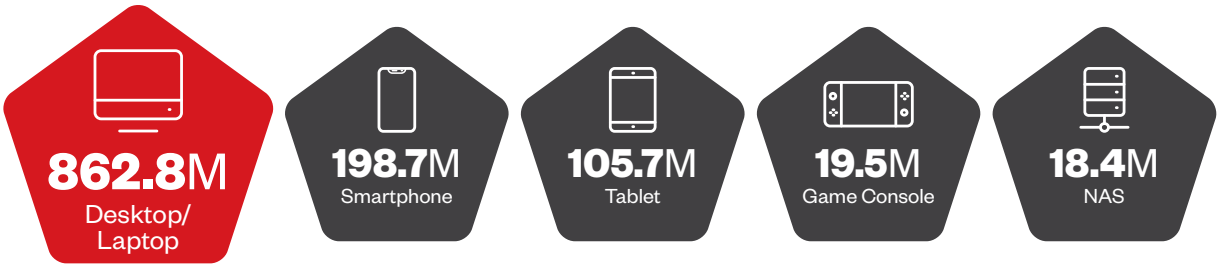
- Caused by an error in processing HTTP packets containing negative Content-Length header field values that result in a heap buffer overflow

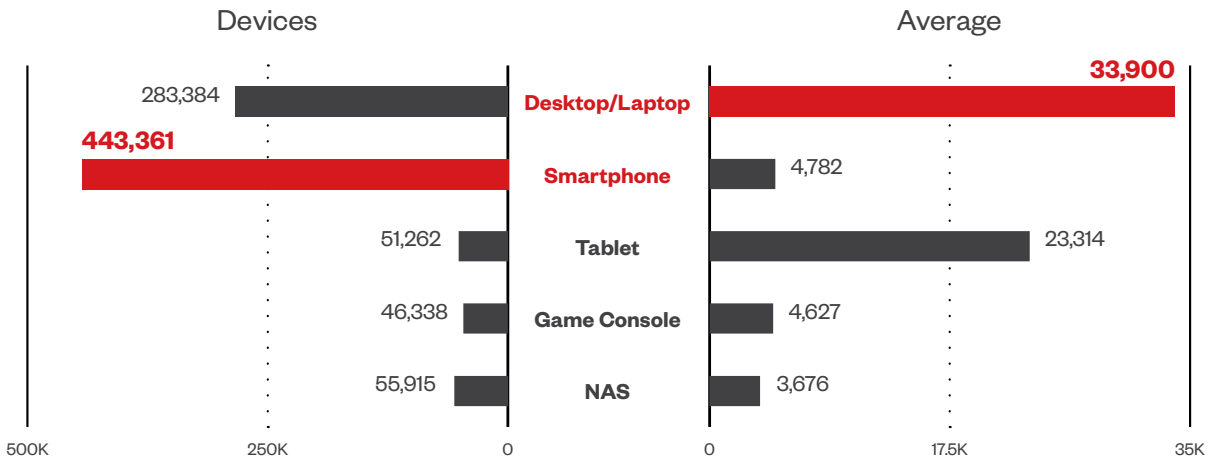
MISC Cryptocurrency Monero Mining Activity -1

- Possible Monero (XMR) cryptocurrency mining activity

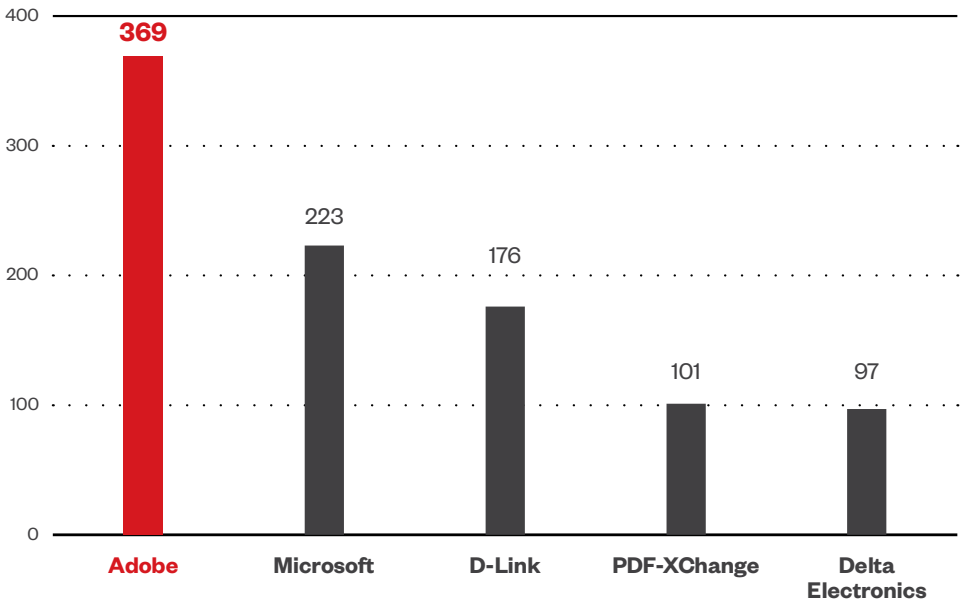
Home Network Security Top Affected Device Types

Desktops and laptops recorded the most inbound attack detections based on our Home Network Security telemetry data.



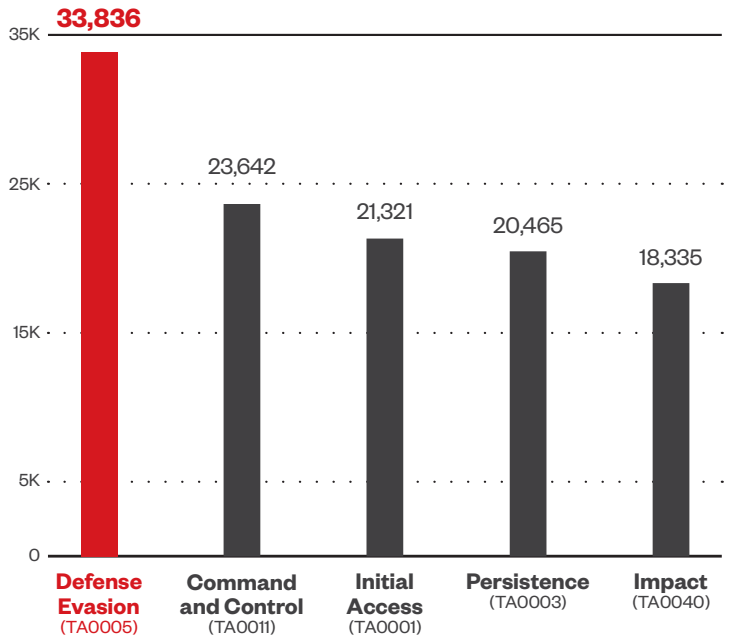


Vulnerability by Vendor

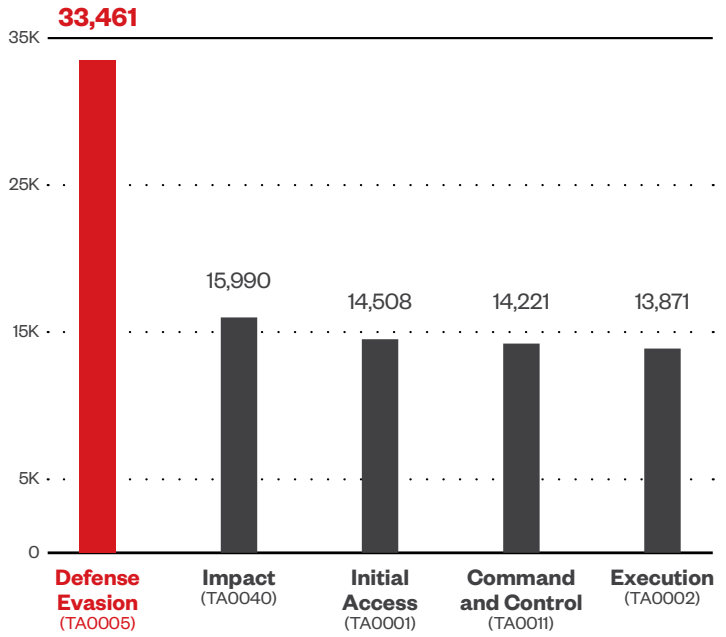


Top 5 Tactics Detected (Overall)

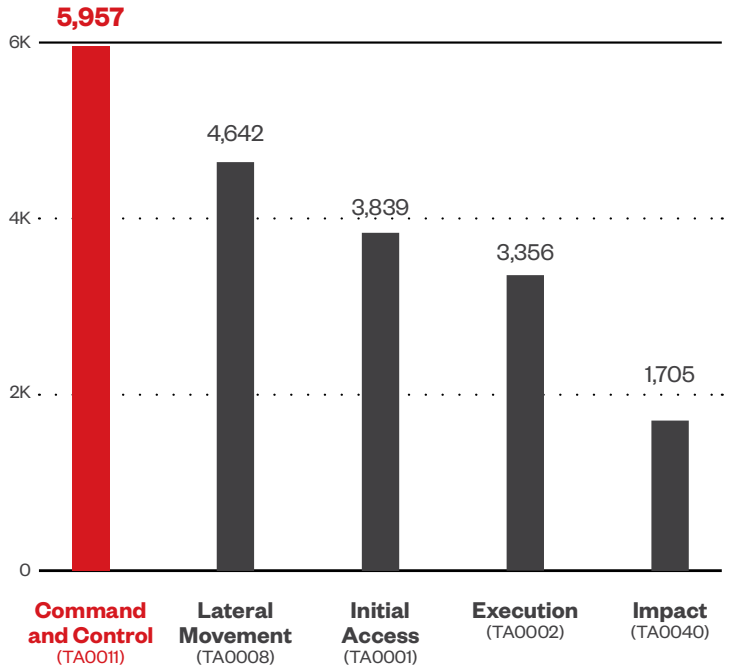
Dodging security tools, communication and control of compromised systems, and gaining a foothold within victim's systems and networks are the most used TTPs (overall, endpoints, network, and email)



Top Tactics, Techniques, and Procedures (TTPs) Endpoint



Top TTPs Network

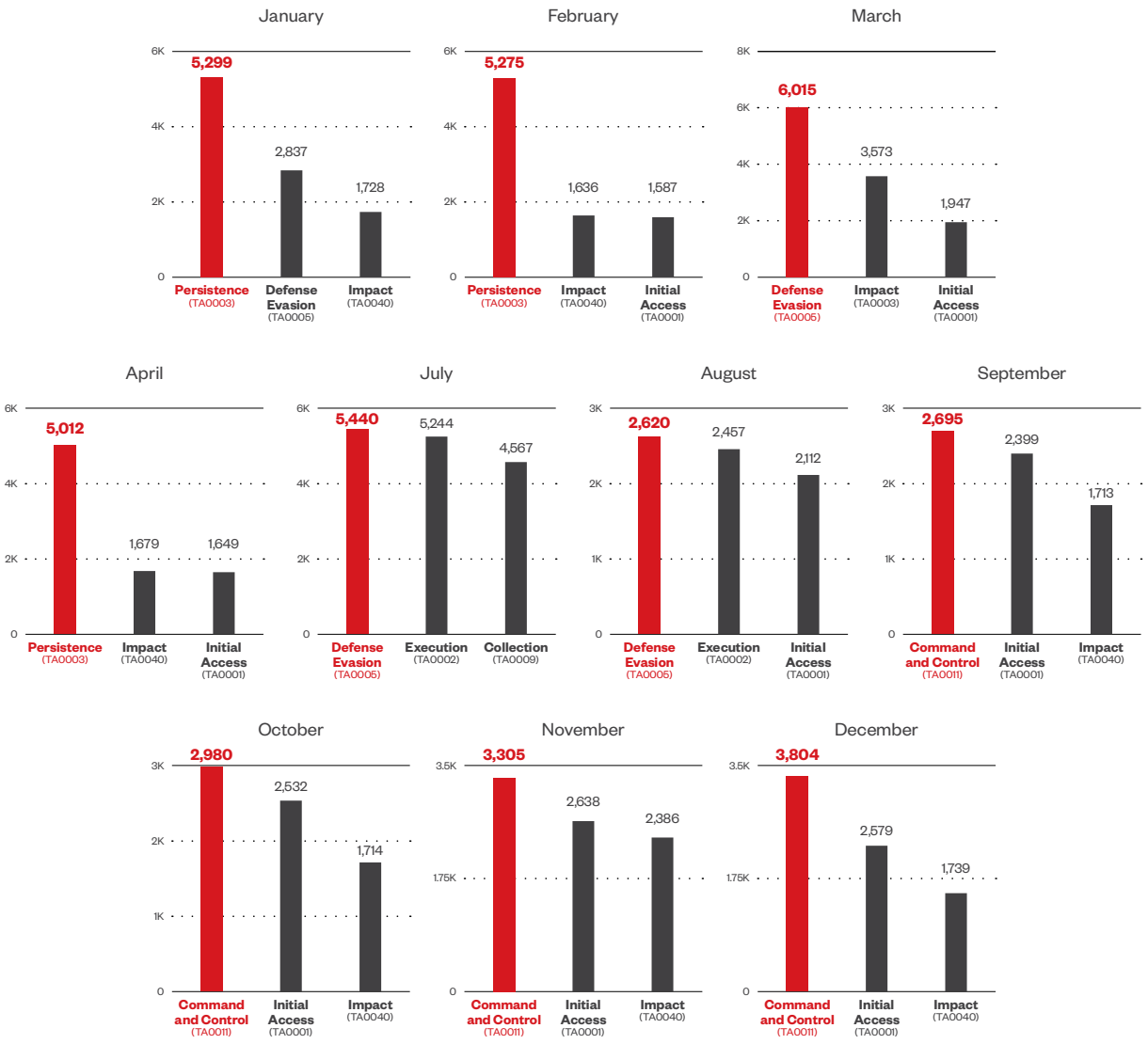


TTPs Overall Trend by Detections

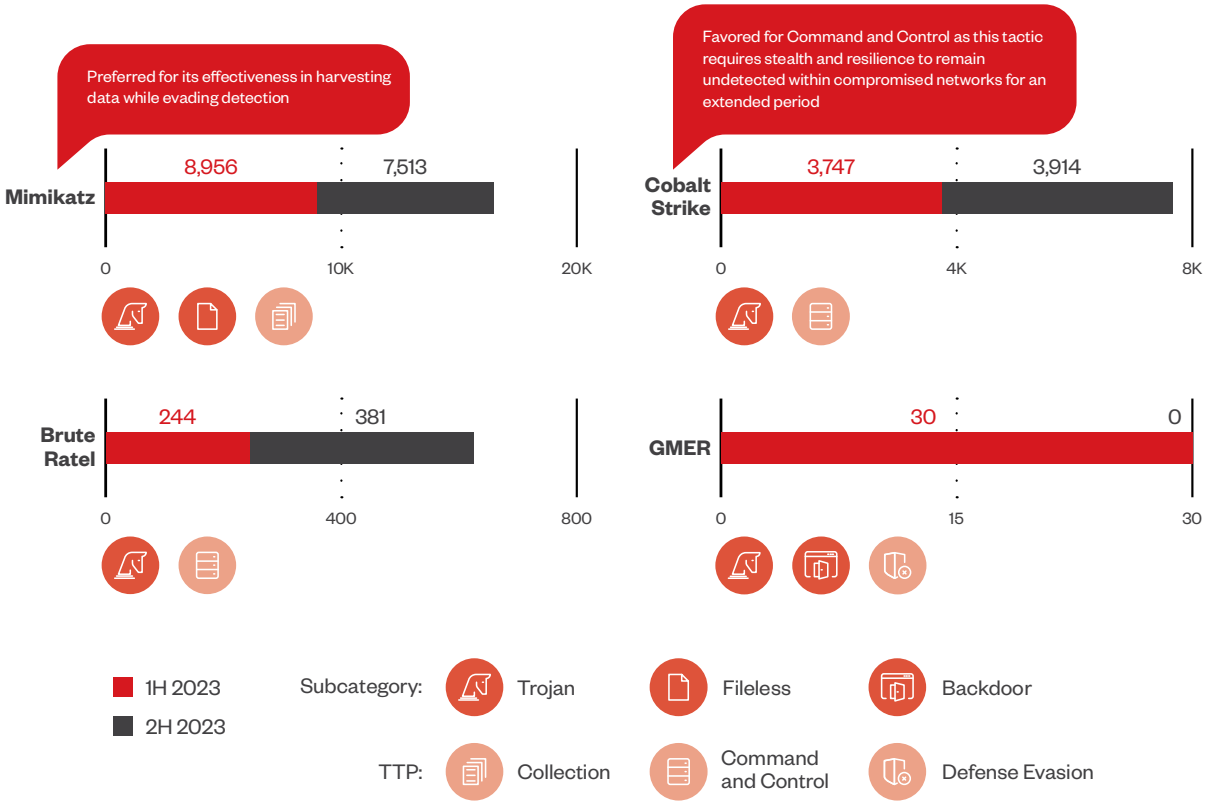
Command and Control showed a gradual increase from September to December, while Defense Evasion peaked in March and July before declining in customer detections in subsequent months. Execution entered the top three TTPs detected in July and August, while Impact showed no clear trend despite a spike in November.

Persistence only entered the top three in the first quarter of the year but was in a downward trend before dipping below the top three. Despite fluctuations, Initial Access maintains a moderate number of detections, since it is the primary goal of threat actors to gain a foothold in target victim systems and networks.

Note that the monthly detections do not show data for May and June due to a system error experienced during that period.



Living-Off-The-Land Tactics

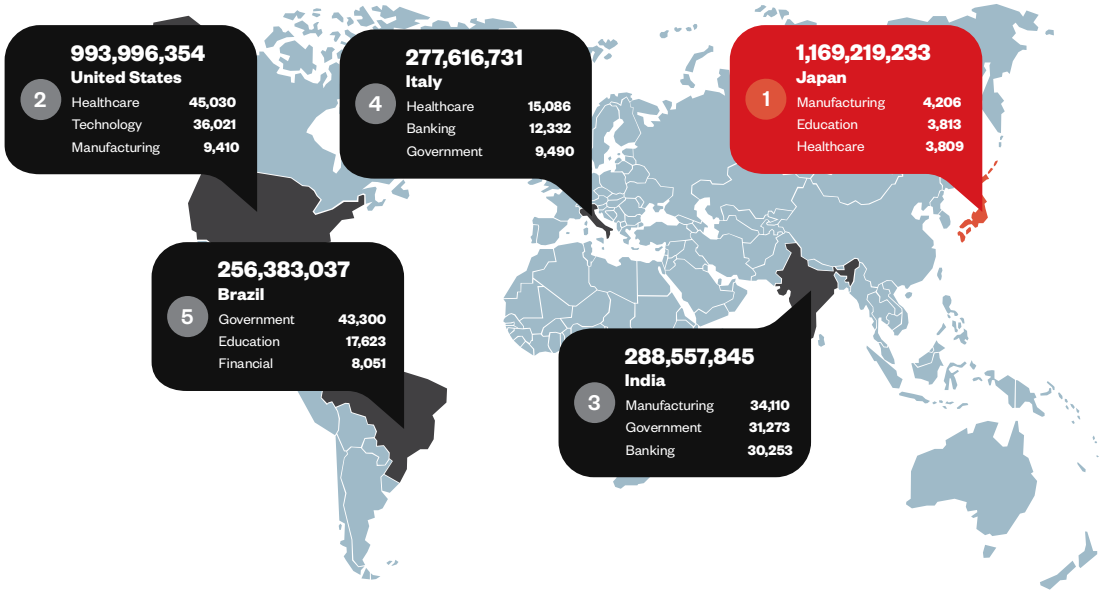


There is no clear trend in the detections, though Mimikatz and Cobalt Strike continue to be the preferred legitimate tools to abuse to aid criminal activity. It can be assumed that threat actors prefer to use well-known tools instead of exploring novel ones, a logical behavior that is commonly observed as it guarantees more likelihood of success with less effort.

Malware Detection

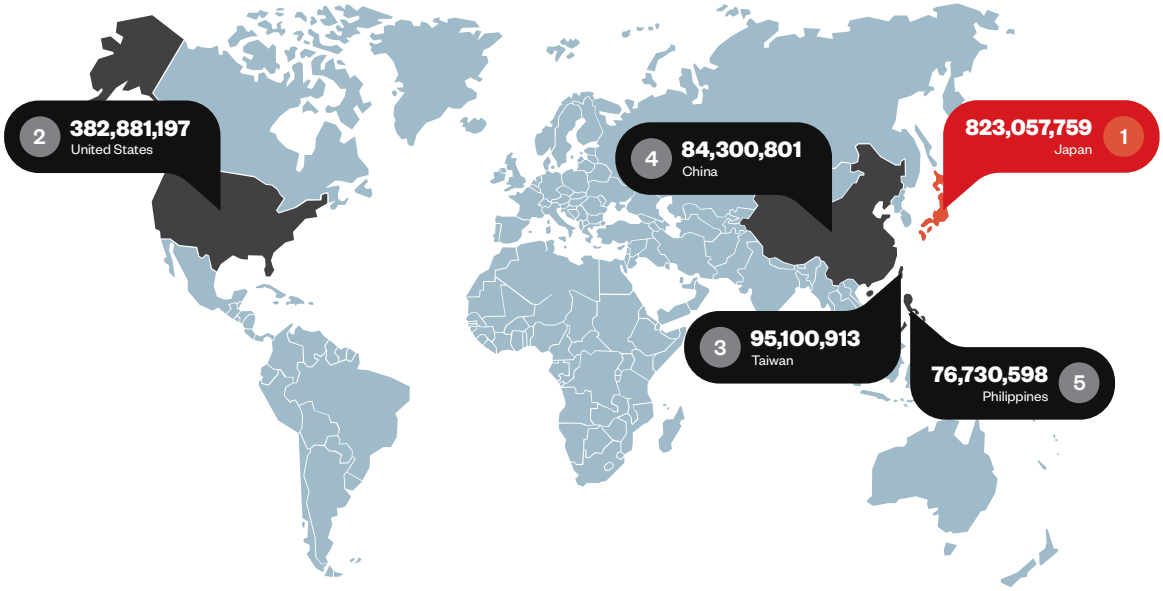
Countries With the Most Malware Detections

and the corresponding top industries targeted for each



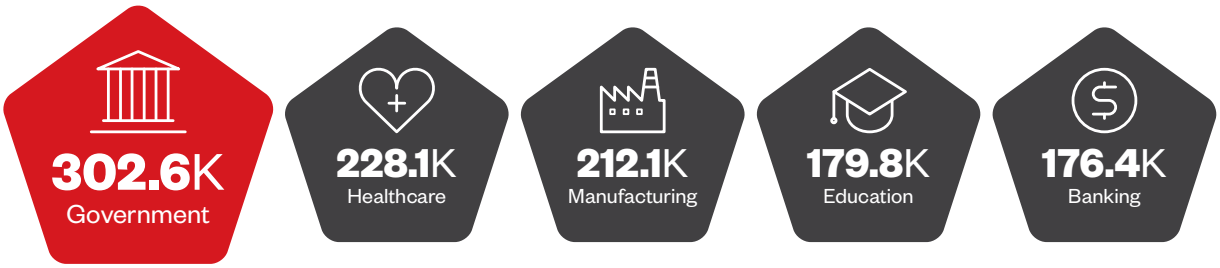
Note that industry data counts are limited to customers who have elected to provide details pertaining to the business sectors in which they belong. Total malware detection counts include customers who did not provide any information on their industries.

Top Countries Accessing Malicious URLs



Top Industries Affected by Malware Campaigns

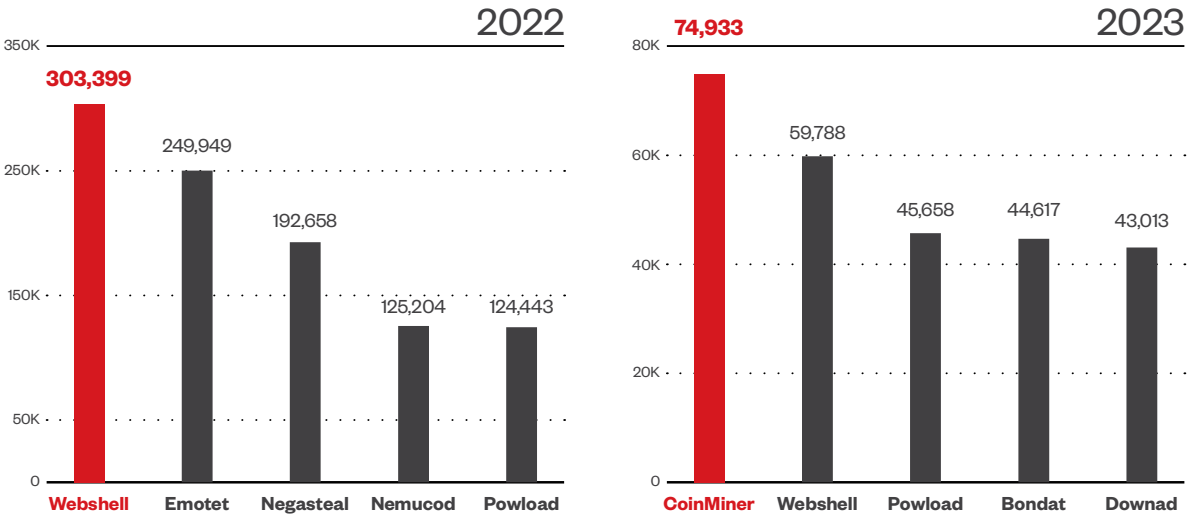
From the aggregate average of our Smart Protection Network (SPN) data, malware campaigns targeted government organizations the most with 302,555 detections.



Top Malware Families

A cryptocurrency mining malware surpassed prolific names in 2023.

Personal data remains the most valuable commodity in underground criminal communities; cryptocurrency wallets and crypto-related data are the most actionable data that can be stolen by malicious actors, equivalent to cash that can immediately be spent without traceability.



Cryptocurrency mining malware CoinMiner takes the lead over notorious Webshell

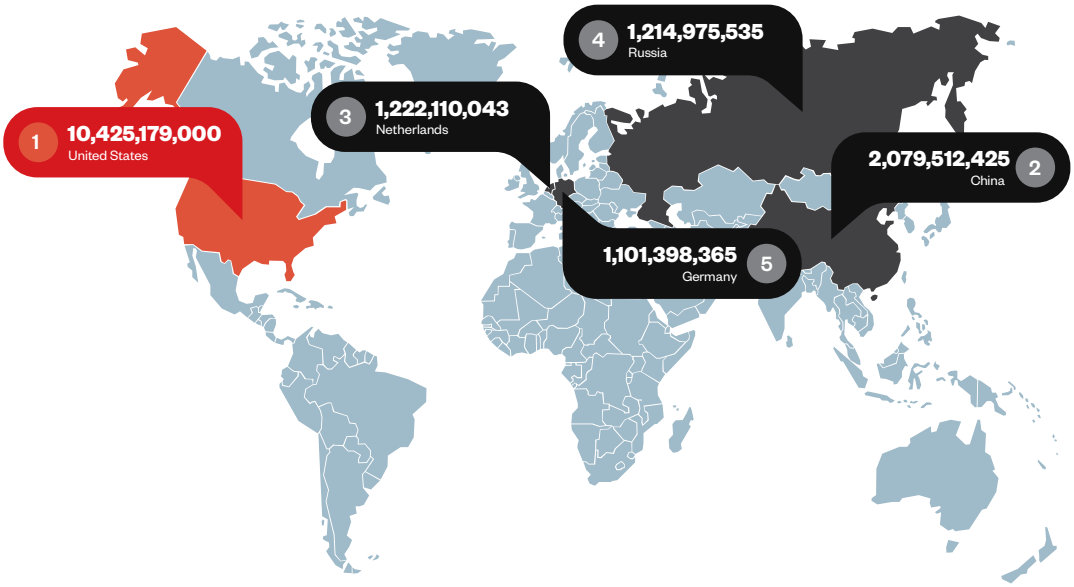
- Last reported exploit: Oracle WebLogic Server vulnerabilities (CVE-2020-14882)
- Reported to have been deployed by malicious Python Package Index packages targeting Linux
- Uses the victim system's central processing unit (CPU) and/or graphical processing unit (GPU) resources to mine cryptocurrency
- The following can be observed during the infection:
  - High CPU utilization either with powershell.exe or schtasks.exe
  - Monero.Cryptocurrency.Miner app detection from the network
  - Execution source can be identified during service installation
  - WMI powershell scripts on the DC server

Despite being overtaken, Webshell remains a go-to for threat actors

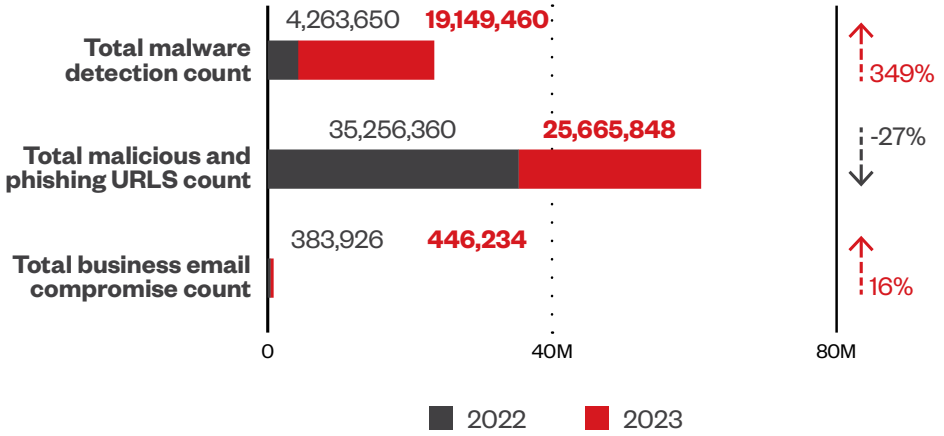
- Exploits vulnerabilities in internet-facing web servers

Email Threats

Top Countries by Detection

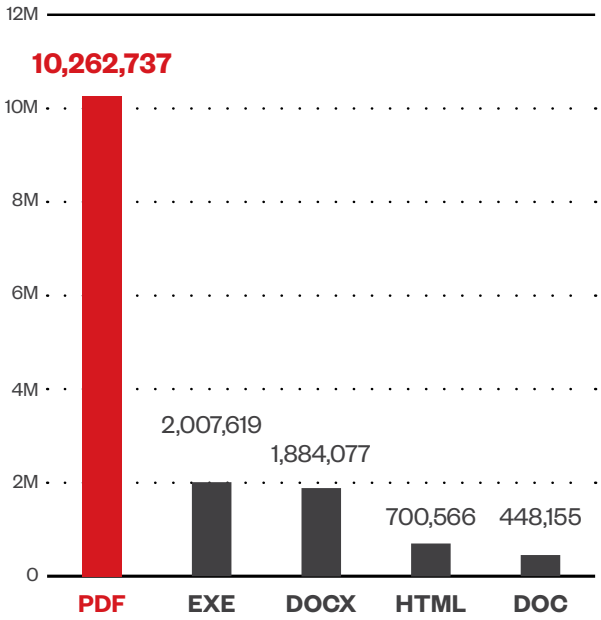


High-Risk Email Threats

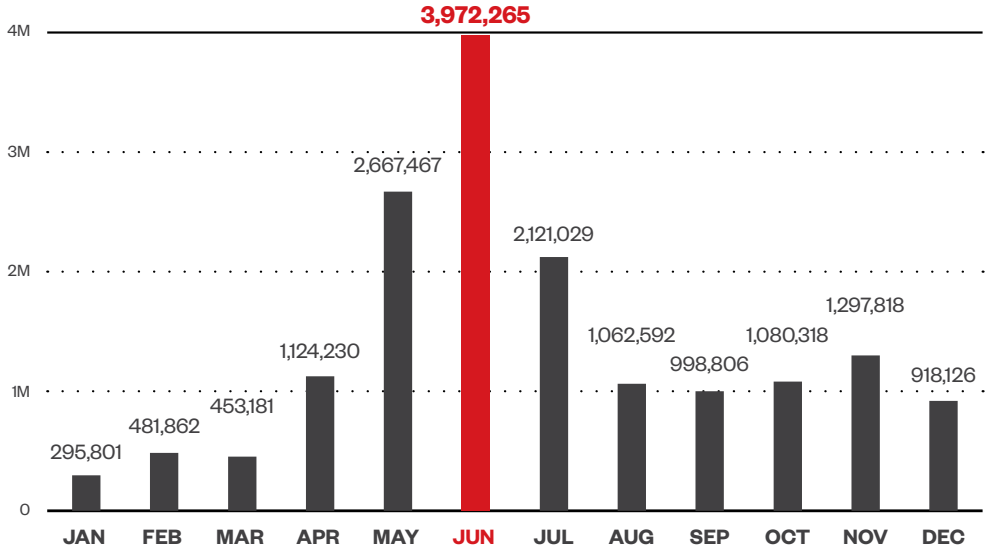


While there is a decrease in malicious and phishing URL detections from 2022 to 2023, the increase in malware detection count and BEC count suggests the change in the threat landscape that finds attackers making use of more sophisticated ways to avoid detection. In this case, instead of focusing on malicious and phishing URLs to randomly victimize users, BEC schemes suggest more targeted operations, while a closer look at our malware detection count includes phishing links embedded within the attachments. This is consistent with patterns observed in our SPN data on threats blocked from 2021 to 2023, where detections that rely on attribution of URLs (WRS) and emails (ERS) show a decrease, while endpoint detections that directly identify malicious files have consistently increased.

Top 5 Spam Attachments

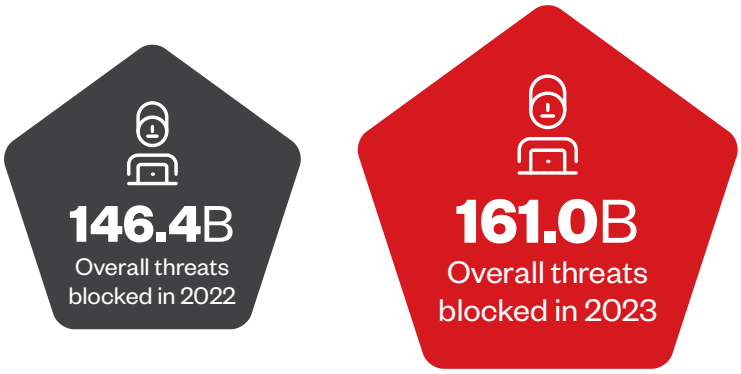


Spam attachments per month of 2023

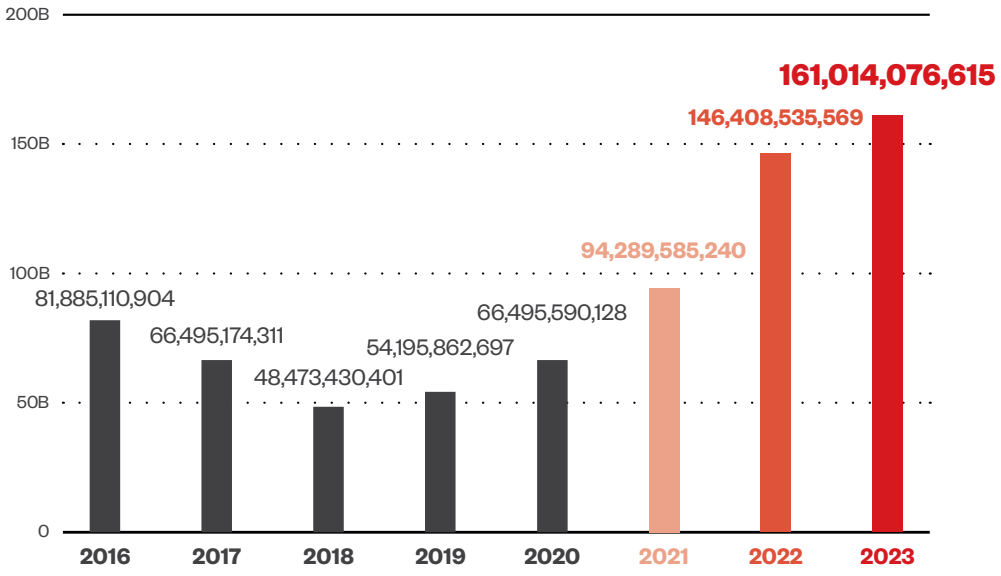


There is a general increasing trend for the first half of the year, where malicious spam attachment detections peaked in June. This is followed by fluctuations in the second half of the year, that eventually decline until December. Despite more cunning ways to lure victims into clicking malicious links, spam campaigns remain a go-to for cybercriminals.

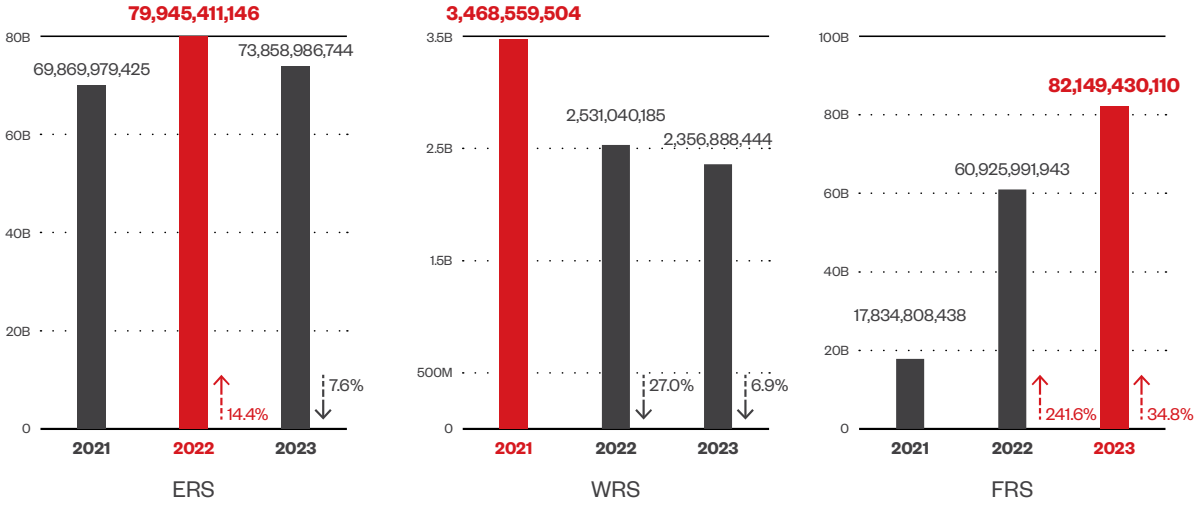
Threats Blocked



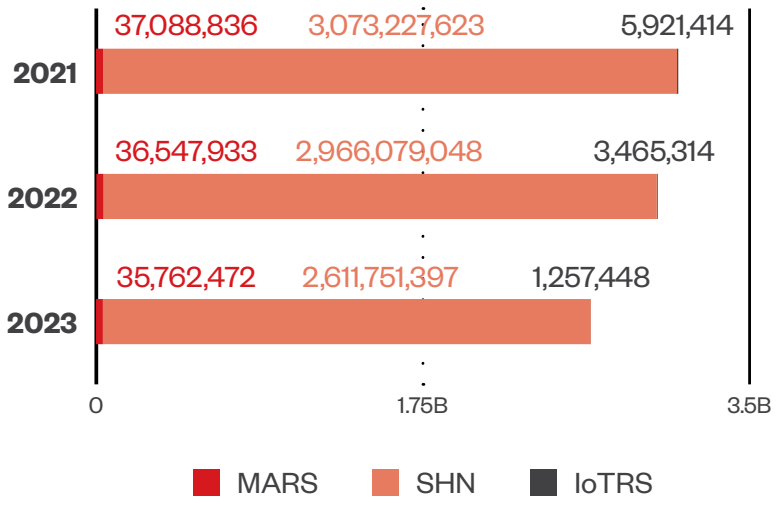
The total number of threats blocked based on our SPN reached a record high in 2023, 10% higher from the previous year. It also continues the dramatic climb of threats blocked that began to be recorded in 2021, the first year that surpassed the previous peak of 82 billion in 2016. This coincided with the pandemic, strongly suggesting its role in driving the upswing.



Despite the overall threats blocked peaking in 2023, there is a fluctuating and downward trend in threats blocked under our Email Reputation Service (ERS) and Web Reputation Service (WRS), indicating that threats in these areas are being better managed or are less frequent. However, there is a continuous increase in threats blocked under our File Reputation Service (FRS).

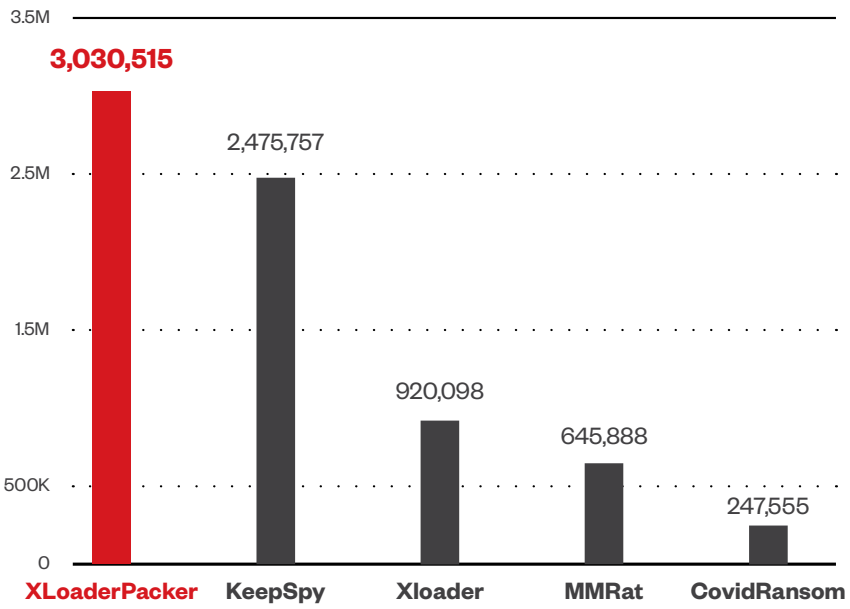


This could be indicative of the changing threat landscape where it can be assumed that threat actors are now opting for quality over quantity: Instead of launching attacks on a wider range of users and relying on victims clicking on malicious links in websites and emails, more sophisticated attacks are launched using specificity to trick a narrower field of high-profile victims. This also allows them to bypass early detection layers like network and email filters. It could be speculated that this contributed to the continuous increase in malicious file detections that are detected at endpoints.



There is also a continuous decrease in threats blocked under our Mobile Application Reputation Service (MARS), Smart Home Network (SHN), and Internet of Things Reputation Service (IoTRS), suggesting that cybercriminals are choosing their targets carefully rather than randomly. It remains crucial to protect all layers of the attack surface, and SOCs should realize that understanding the attackers' targeting strategies is important for effective defense.

Android Malware Families

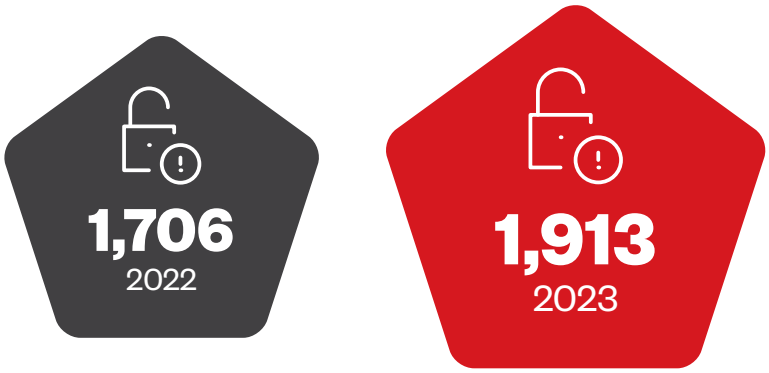


- XLoaderPacker is a spyware that can be manually installed by a user. It poses as an Android app using different app names, and, once installed can monitor incoming and outgoing calls, and lock the screen of the affected system.
- KeepSpy is sideloaded through a TianySpy malware delivered via smishing messages. It also poses as an Android app using different app names, and, once installed, can collect banking credentials and Wi-Fi settings.

Vulnerabilities

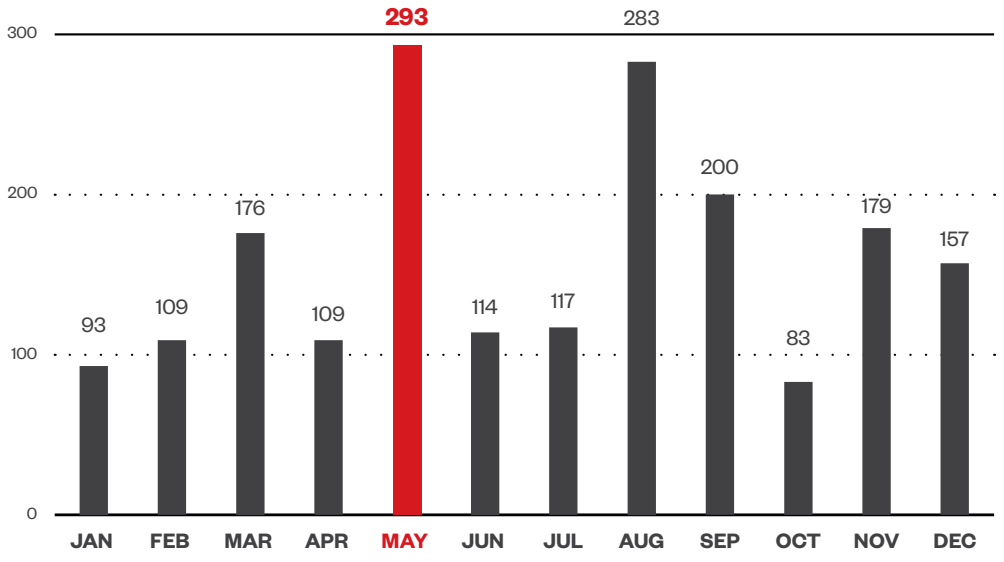
Total Vulnerabilities

(Number of published Zero-Day Initiative (ZDI) vulnerability advisories)

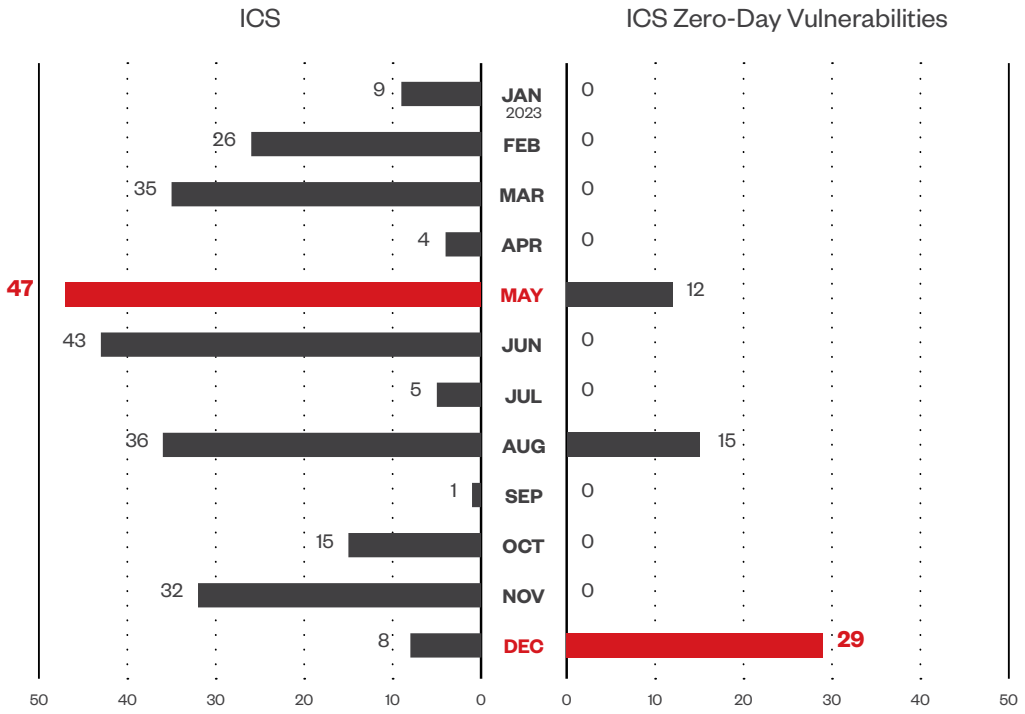


Zero-Day Exploits (ZDI) Advisories

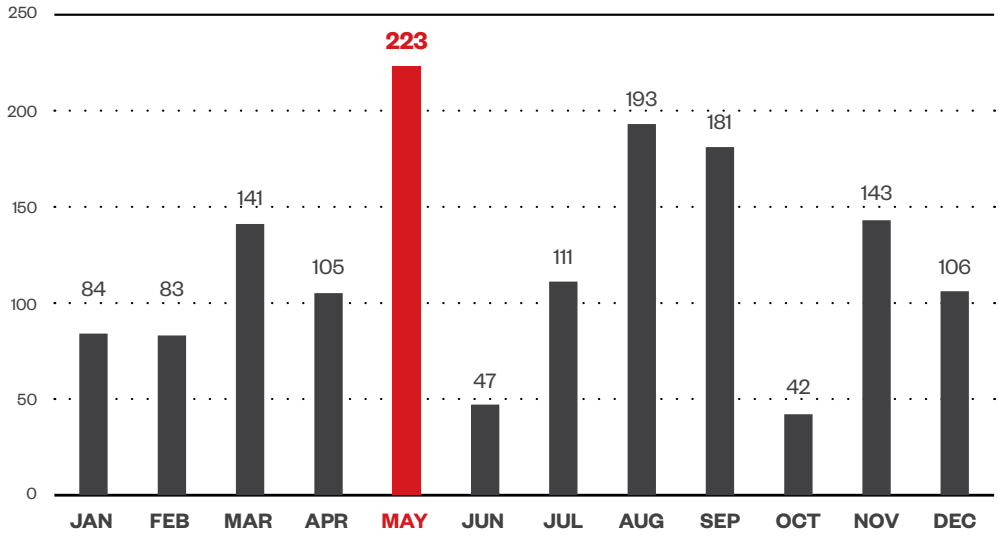
The first quarter of 2023 starts with relatively low zero-day advisories, with a significant increase by the end of the quarter in March. The second quarter fluctuates and peaks in May, while the third quarter stabilizes at a relatively high level of activity. The last quarter dips to the year's lowest number of zero-day advisories in October, picks back up again in November, but shows a slight downturn in the last month indicating a possible decrease in threat actor activity as the year ended.



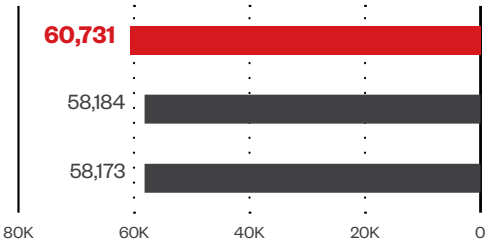
ZDI Industrial Control System and Zero-Day Vulnerabilities



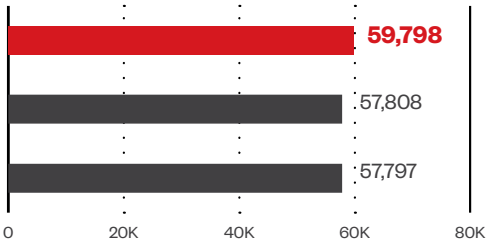
Non-ICS and N-Day Vulnerabilities



Riskiest CVEs by customer count



3 riskiest unpatched CVEs



CVE-2023-2488 (Windows SmartScreen Security Feature Bypass Vulnerability)

- CVSS base score: 4.4 medium

CVE-2023-21823 (Windows Graphics Component Remote Code Execution Vulnerability)

- CVSS base score: 7.8 high

CVE-2023-23376 (Windows Common File Log System Driver Elevation of Privilege Vulnerability)

- CVSS base score: 7.8 high

Risk Events

Top 2 Risk Events Detected

The top two risk events detected via our attack surface risk management (ASRM) involve risky cloud applications and accessing risky websites.

82,976,277,500

Risky Cloud App Access

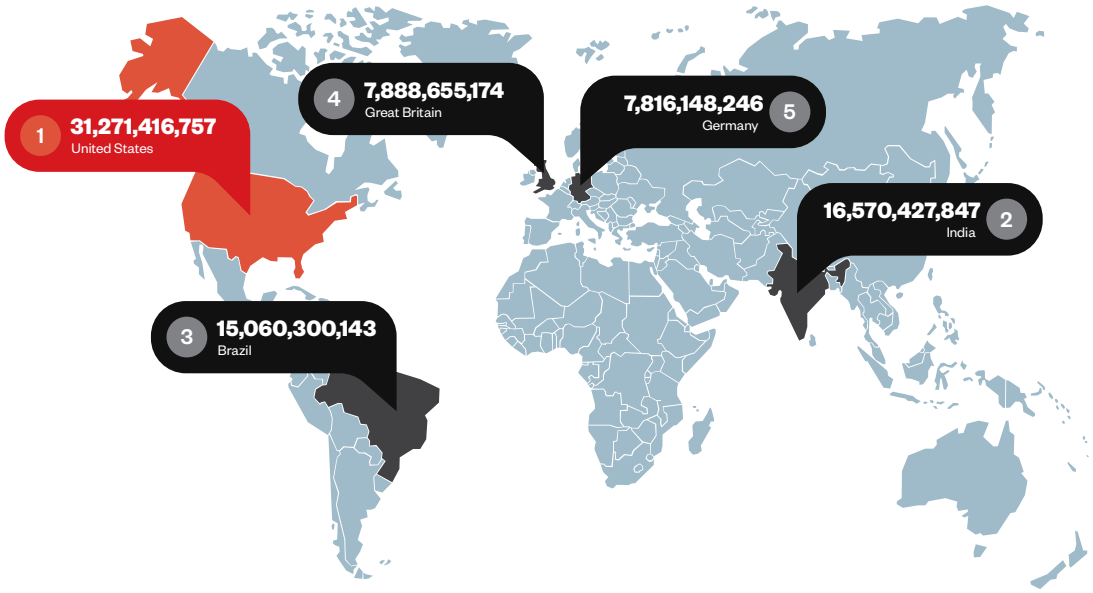
18,819,067,819

Risky Website Access Detected

- SOCs are recommended diligence in monitoring cloud applications accessed by their networks, especially as more organizations are integrating cloud environments in their operations.
- Security teams should also conduct training to equip end-users with the knowledge to identify and avoid accessing risky websites and links; human negligence remains the weakest link in cybersecurity.

Top Countries with Risk Events Detected

The United States of America recorded the most risk events at over 31.2 billion detections, almost doubling the number of the country with the second most risk events, India at 16.5 billion detections.




corero
JUNIPER NETWORKS
2023
DDOS THREAT
INTELLIGENCE
REPORT _

EXECUTIVE SUMMARY

We recommend that companies employ advanced, holistic detection and protection to combat the rising risk of carpet bomb attacks. We also recommend flexible protection that can adapt to the ever-changing DDoS landscape to help organizations maintain their business continuity and protect against future threats.

DDoS threats continue to grow in both volume and sophistication. Over the past year, Corero's customers have seen a significant increase in certain kinds of attacks.

- Carpet bomb attacks have increased by 300%, creating a triple threat. These attacks can evade detection, neutralize security techniques, and overload system capacity.
- Mirai-like DDoS attacks have also increased significantly, with over seven times as many attacks in 2022 than 2021.
- Although the IPv6 landscape remains somewhat murky, it's clear that we're seeing a major rise in the share of malicious DDoS traffic carried by this protocol, to the tune of 600%.
- While the UDP protocol has long been the major DDoS attack vector, our team has observed a 70% increase in TCP-based vectors. This growth of malicious TCP traffic presents new problems in detecting and mitigating threats.
- Although directed DNS traffic represents a smaller percentage of overall attacks, it is growing at a faster rate, doubling from 2020 to 2022.

75%
DDOS ATTACKS LAST LESS THAN 10 MINUTES

25%
INCREASE IN HIGH PACKET RATE DDOS ATTACKS

300%
INCREASE IN CARPET BOMB DDOS ATTACKS

60%
INCREASE IN DDOS ATTACKS LASTING OVER 60 MINUTES

27%
LIKELIHOOD OF A REPEAT ATTACK IN SAME WEEK

98%
DDOS ATTACKS LESS THAN 10 GBPS

SECTION 2:

THE GROWING DANGER OF 'CARPET BOMB' ATTACKS _

So-called 'carpet bomb' attacks distribute traffic across a large number of targets rather than a more easily identifiable single target. Also known as spread-spectrum or spray attacks, their approach challenges standard victim-oriented detection, mitigation, and alert techniques.

While carpet bomb DDoS attacks were observed in 2020 and 2021, this vector was still relatively uncommon. However, the Corero Threat Intelligence team had observed a significant increase of up to 300% during 2022. Carpet bomb attacks are difficult to defend against, stymying many of the traditional detect-and-redirect DDoS mitigation techniques. Victims face a triple threat because of the attack's ability to:

1. EVADE

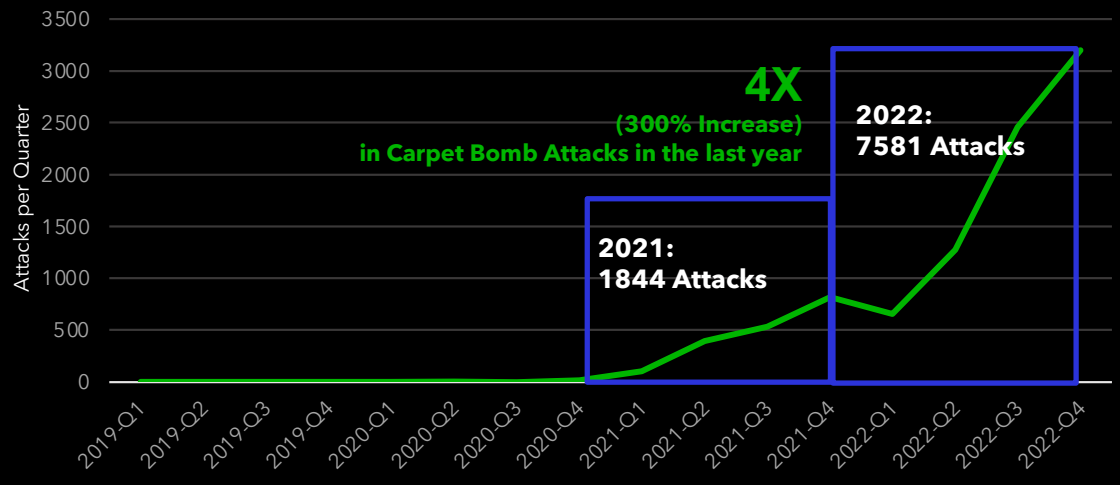
Avoiding detection and isolation by flying under the radar of per-destination IP traffic analysis techniques or thresholds.

2. NEUTRALIZE

Invalidating the practical use of 'black hole' or null routes techniques for the avoidance of link saturation or collateral damage.

3. OVERLOAD

Exceeding scrubbing lane capacity, straining cloud redirection budgets, or confusing alerting and reporting systems, due to the way they present as many simultaneous attacks targeting large numbers of victims.



SECTION 3:

2023 AND BEYOND: ADDITIONAL THREATS LANDSCAPE 2023

The online threat landscape continues to evolve quickly, with attackers launching more sophisticated and coordinated DDoS attacks every year.

We've observed four other noteworthy and ongoing DDoS trends from the past year:

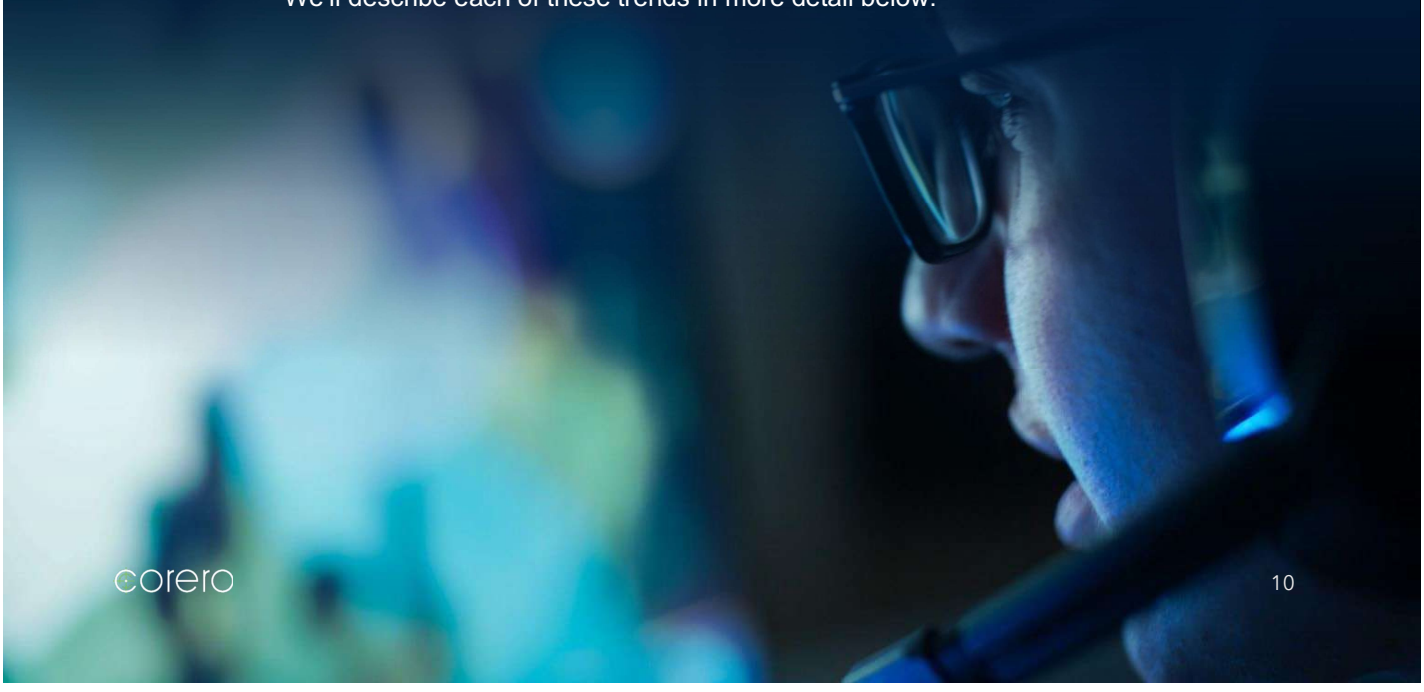
- More Mirai-like, botnet-originated DDoS attacks
- An increasing share of IPv6 DDoS attacks
- A shift toward TCP DDoS attack vectors
- A rise in DNS attacks: DDoS attacks targeting DNS ports or services

640%
INCREASE IN MIRAI-LIKE BOTNET ATTACKS

500%
INCREASE IN THE SHARE OF IPV6 BASED DDOS ATTACKS

70%
INCREASE IN THE SHARE OF TCP-BASED DDOS ATTACKS

We'll describe each of these trends in more detail below.



SUMMARY

2022 DDOS TRENDS

75%
DDOS ATTACKS LAST LESS THAN 10 MINUTES

25%
INCREASE IN HIGH PACKET RATE DDOS ATTACKS

300%
INCREASE IN CARPET BOMB DDOS ATTACKS

60%
INCREASE IN DDOS ATTACKS LASTING OVER 60 MINUTES

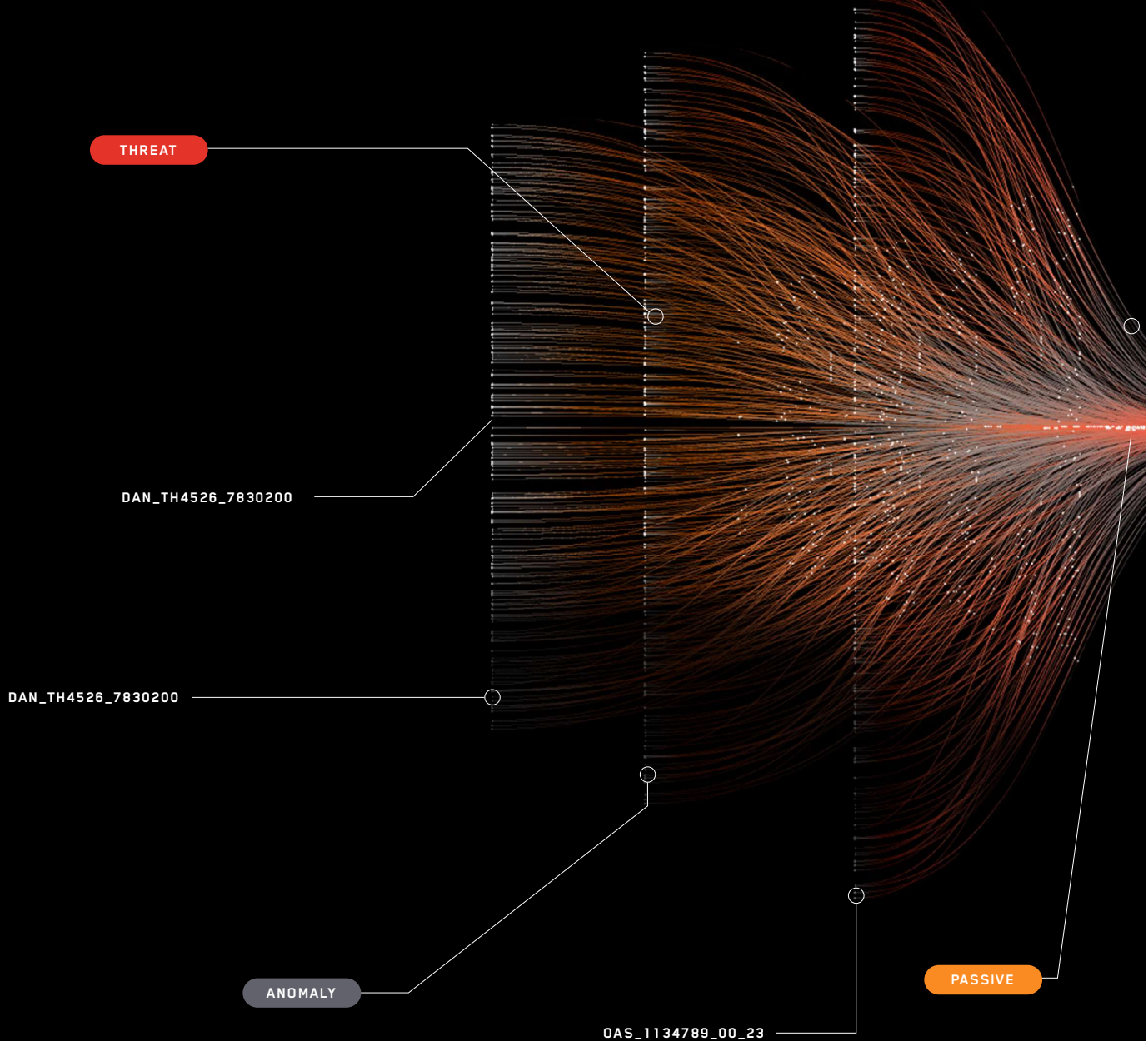
27%
LIKELIHOOD OF A REPEAT ATTACK IN SAME WEEK

98%
DDOS ATTACKS LESS THAN 10 GBPS

DARKTRACE

ANALYSIS OF THE SECOND HALF OF 2023

END OF YEAR THREAT REPORT



Darktrace/Email Trends

By learning the normal 'pattern of life' for every correspondent, Darktrace/Email™ is able to understand users and their unique communication patterns. Its Self-Learning AI develops an understanding of the person behind every email communication. This differs from the traditional security solutions, which rely heavily on previously seen malicious emails and known bad senders, meaning they are often prone to miss novel and increasingly sophisticated email threats.

Darktrace/Email can recognize the subtle deviations in expected email activity to determine whether any given email could represent a threat to customer networks. It is then able to make highly accurate decisions to mitigate and neutralize any email attack it faces.

Methodology: *The following email trends are derived from analysis of monitored Darktrace/Email model data for all customer deployments hosted in the cloud between September 1 and December 31, 2023. Around 90% of the global Darktrace customer base's email environments are cloud-based. The statistics presented here were obtained from dedicated Darktrace/Email models created in September 2023 to study email trends. The models were designed to alert for emails that were considered 100% anomalous for a customer's environment and contained "phishing indicators". For the purpose of this report, and indeed Darktrace's analysis of email environments, "phishing indicators" refers to emails that are confirmed as malicious, as opposed to merely unwanted spam emails. There was a total of 28 million spam emails held by Darktrace during this time.*

Darktrace's analysis of TTPs across customer email environments indicates that a significant number of email threats are capable of bypassing or manipulating traditional email security or authentication systems.

While Domain-based Message Authentication (DMARC) is often positioned as a way for organizations to 'solve' their email security problems, 65% of the phishing emails observed by Darktrace successfully bypassed its verification checks, indicating that malicious actors are increasingly improving their stealth and evasion tactics. Likewise, the fact that a significant portion of phishing emails were not detected by major email providers points to possible gaps or vulnerabilities in traditional security measures.*

Threat actors are evidently adapting and innovating their tactics through the use of novel social engineering techniques designed to manipulate recipients into giving up sensitive information like user credentials or bank information, or downloading malicious payloads.

Considering that over a quarter of the observed phishing emails were identified as containing a "significant" amount of text (200 words), threat actors are demonstrably having to innovate and bolster their efforts to craft sophisticated phishing campaigns, potentially leveraging Generative AI tools to automate social engineering activity.

Between September 1 and December 31, 2023, Darktrace/Email detected 10.4 million phishing emails across the customer fleet.

65%
of these emails successfully passed DMARC authentication

58%
of these emails passed through all existing security layers

45%
of these emails were identified as spear phishing attempts

3%
of these emails utilized newly created domains

38%
of these emails were observed utilizing novel social engineering techniques

28%
of these emails contained over 1,000 characters (or around 200 words)

Darktrace/Email detected at least 639,000 malicious QR codes within these emails

* All emails seen by Darktrace/Email have already passed through any existing gateway; emails are then checked by native spam filtering (Microsoft or Google Workspace). In 58% of cases, phishing emails detected by Darktrace/Email passed through this filtering, either because of gaps in detection or because customers have disabled it, trusting Darktrace/Email to handle all decisions.

agari by HelpSystems

PHISHLABS by HelpSystems

QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT

AUGUST 2022

ABOUT THE REPORT

In Q2, Agari and PhishLabs analyzed hundreds of thousands of phishing and social media attacks targeting enterprises, their employees, and brands. This report uses the data from those attacks to present key trends shaping the threat landscape.

Security leaders and practitioners can use this information to better understand these threats and to take proactive measures to reduce risk.

KEY TAKEAWAYS

Phishing is Steadily on the Rise
Phishing attacks are up nearly 6% in Q2 from Q1 2022

Social Media is an Accessible and Preferred Threat Channel
Social media attacks have increased more than 100% in a year

Response-Based Phishing Continues to Climb
Response-Based threats targeting corporate inboxes reached the highest volume since 2020

Emotet Leads Ransomware Payloads
Emotet has fully recovered, representing nearly 50% of all malware payload attacks in Q2

Hybrid Vishing Attack Volume Trending Up
Hybrid Vishing attacks have increased 625% in volume since Q1 2021

O365 Credentials Coveted by Criminals
Nearly 60% of credential theft phishing attacks targeted O365 credentials in Q2

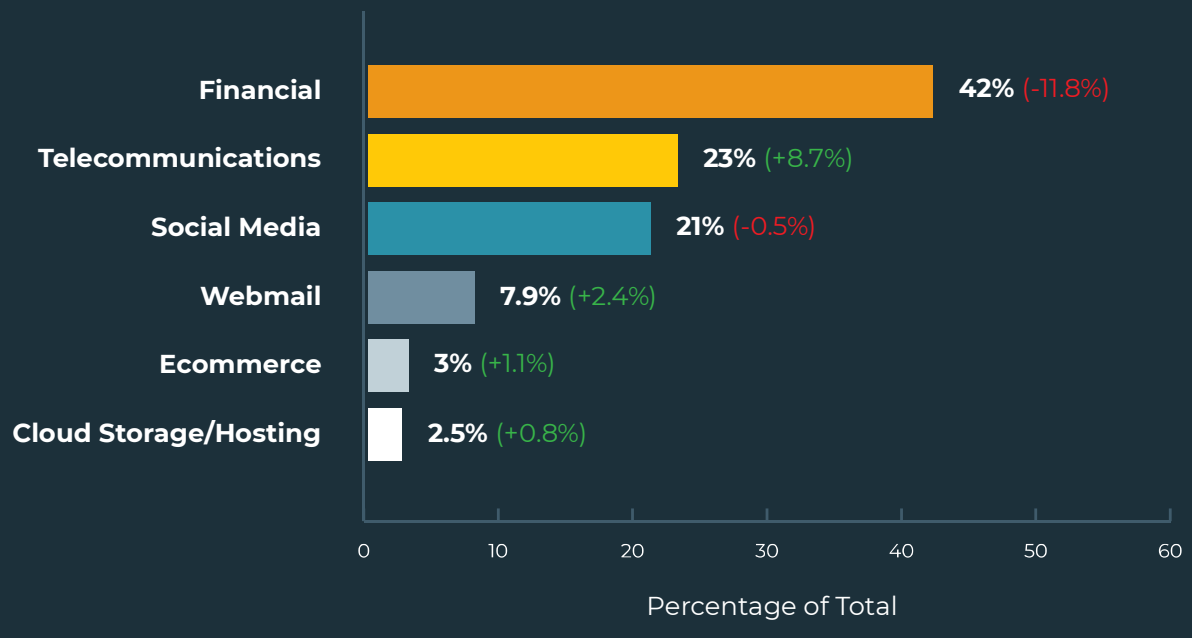
TOP TARGETED INDUSTRIES

Financial Institutions were targeted most by phishing sites in Q2, experiencing 42% of all attacks. While it is historically the top targeted industry, this is the second consecutive quarter incidents have declined. Year to date, attacks targeting the financial industry are down more than 19%.

Telecommunications was the second most targeted industry after experiencing a nearly 9% increase in share during Q2. This was the largest increase among top targeted industries. Telecom incidents contributed to 23% of observed phishing attacks.

Other prominent technology sectors combined to make up 34.4% of credential theft phishing incidents in Q2. Social Media was 21% of overall industry volume despite a slight decrease in attacks. Webmail (7.9%), Ecommerce (3%), and Cloud Storage/Hosting (2.5%) all experienced increases in Q2.

Financials continued to experience a majority of phishing attacks, accounting for 42% of all incidents.



In Q2, only 17% of phishing sites were staged using Paid Domain Registrations.

STAGING METHODS

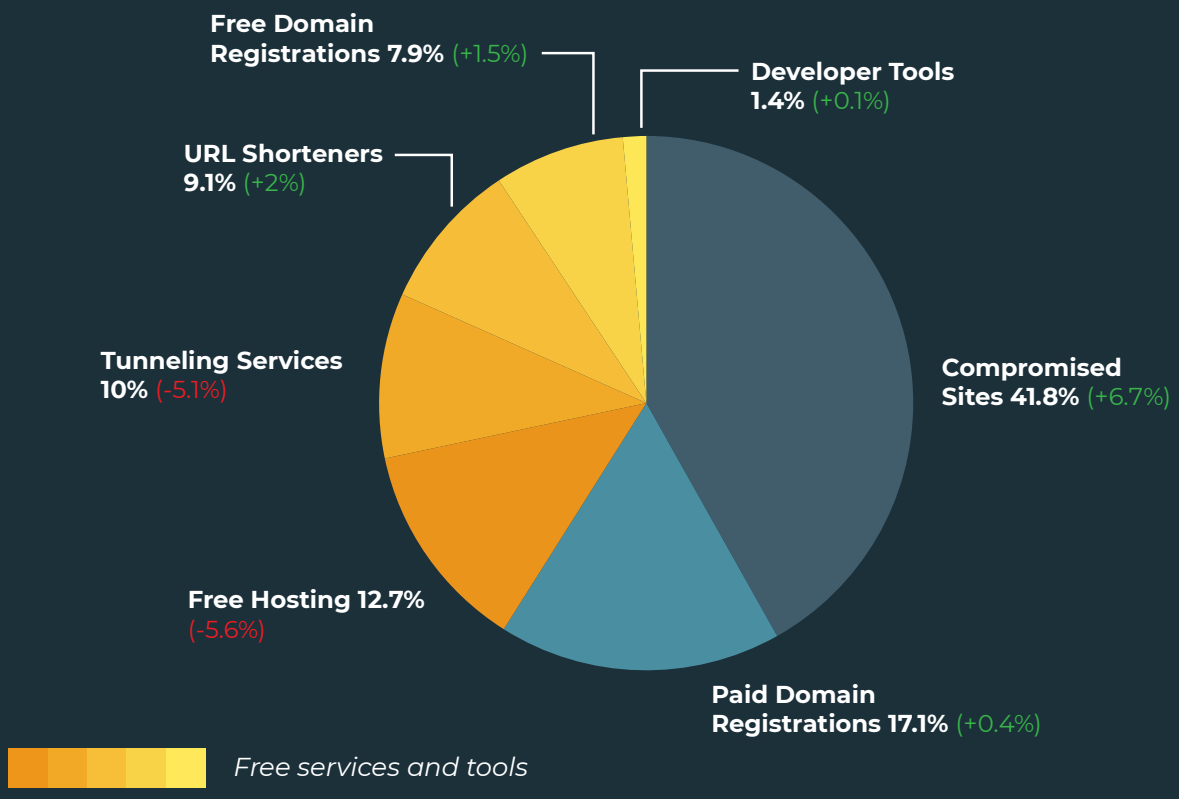
In Q2, 4 out of every 5 phishing sites were staged on infrastructure that required no investment by threat actors, including Free Services and Tools or Compromised Sites. However, abuse of Free Hosting and Tunneling Services fell during the quarter, suggesting those providers have taken measures that have made them less attractive to cybercriminals.

Compromising existing websites was the preferred method to stage phishing campaigns, contributing to 41.8% of the overall share. Compromised Sites also experienced the greatest growth in activity, increasing 6.7% over Q1.

The use of Free Services and Tools has declined steadily since the onset of 2022. In Q2, Free Services dropped nearly 7% in share from Q1, accounting for only 41% of all incidents.

Free Hosting represented most of the activity within the group, accounting for 12.7% of abuse. Free Hosting also experienced the largest decrease, declining 5.6%. Tunneling Services were the second most abused free service, representing 10% of all activity.

URL Shorteners (9.1%), Free Domain Registrations (7.9%), and Developer Tools (1.4%) all experienced nominal increases.

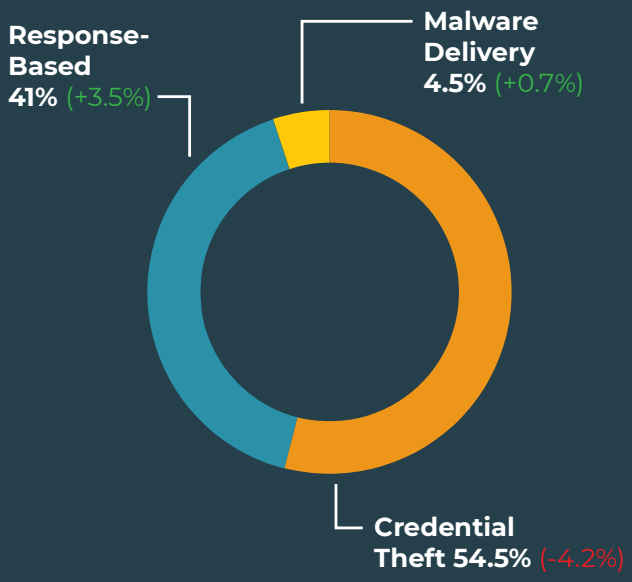


THREATS FOUND IN CORPORATE INBOXES

Credential Theft attacks reported in corporate inboxes represented nearly 55% of all email-based threats in Q2, despite experiencing a 4.2% decline in activity. Credential Theft incidents are repeatedly the top threat-type targeting organizations.

Response-Based attacks reported in corporate inboxes have climbed to the highest count and share in volume since 2020, representing 41% of email-based scams in Q2. Response-Based volume has increased steadily every quarter since Q1 2021, apart from a negligible decline in Q1 2022. Response-Based attacks consistently represent a significant portion of phishing volume, evidence that social engineering tactics continue to prove effective for criminals.

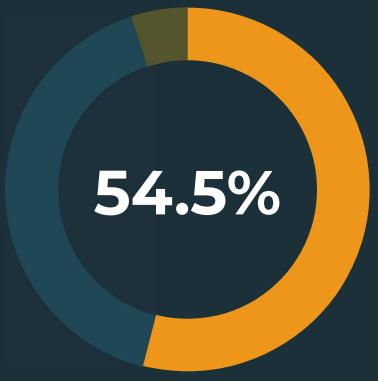
Malware Delivery increased 0.7% in Q2, contributing to 4.5% of share of attack volume.



CREDENTIAL THEFT

Credential Theft attacks targeting Office 365 accounts reached a six-quarter high in share and volume during Q2. More than 58% of all Credential Theft phishing links were delivered with the intent to steal O365 login credentials, up 17.7% compared to Q4 2021.

The increased focus on O365 account information is one example of the value bad actors place on credentials associated with network-wide collaboration and productivity applications. Malicious attachments such as Docuphish declined in Q2, representing 15% of Credential Theft attacks.



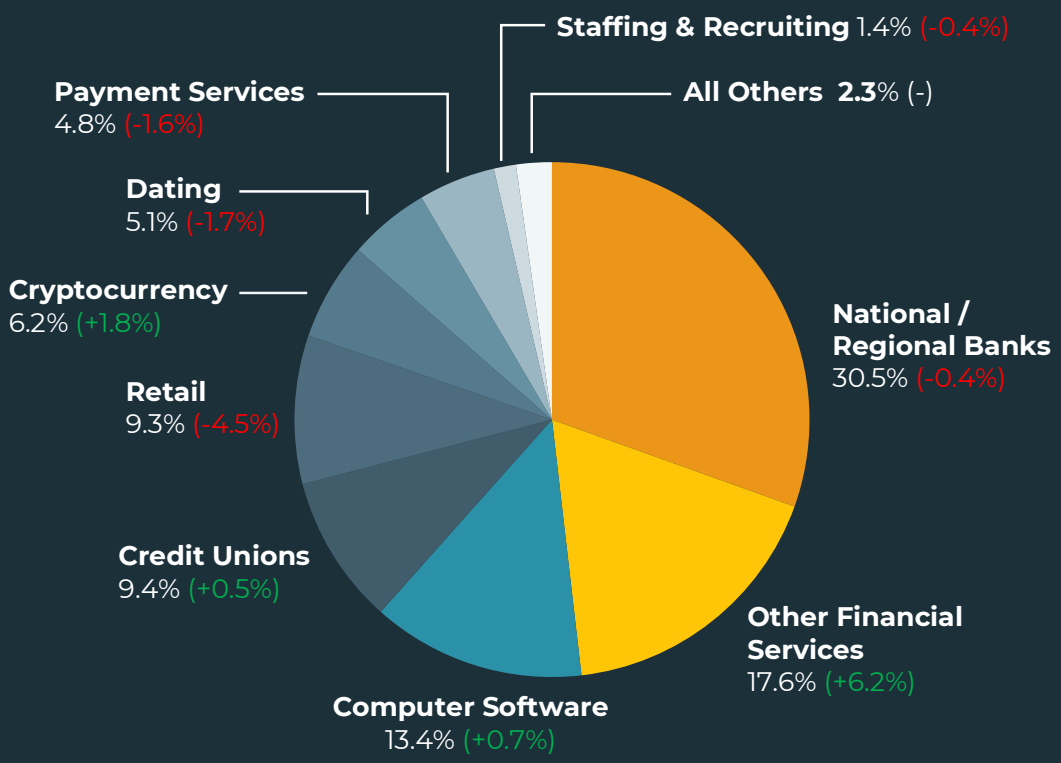
Phishing Link	85%	+5.2%
Attachment	15%	-5.2%

ATTACKS BY INDUSTRY

The Financial Industry as a whole continues to experience extensive abuse on Social Media. Banks, Other Financial Services (i.e. asset management and financial advisory firms), Credit Unions, Cryptocurrency, and Payment Services experienced more than 68% of share of attacks in Q2, fueled primarily by increased fraud and impersonation of a brand or executive.

While National/Regional Banks (30.5%) claimed most of the abuse in Q2, Other Financial Services (17.6%) experienced the most significant increase in attack volume, moving up multiple positions to represent the second most targeted industry. Computer Software (13.4%) and Credit Unions (9.4%) claimed the third and fourth spots, after experiencing increased attacks in Q2. Despite a slight decline in share, Retailers continued to be heavily targeted by impersonation attacks. In Q2, Retail experienced 9.3% of overall abuse.

Attacks targeting Cryptocurrency continue to grow as social platforms prove the ideal environment for cyber threats and impersonation scams. In Q2, attacks on Cryptocurrency increased 1.8% of share to represent 6.2% of attack volume.

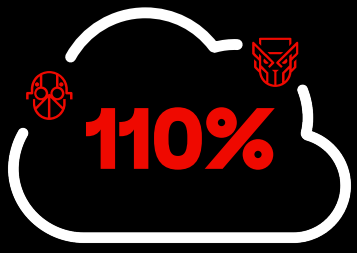



2024
GLOBAL THREAT REPORT
CROWDSTRIKE

Threat Landscape Overview

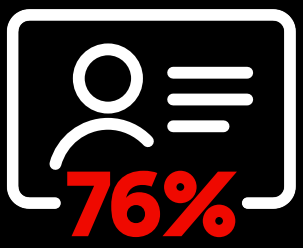
year over year = (YoY)

34 new adversaries tracked by CrowdStrike, raising the total to **232**



Cloud-conscious cases increased by **110% YoY**

Cloud environment intrusions increased by **75% YoY**



76% YoY increase in victims named on eCrime dedicated leak sites

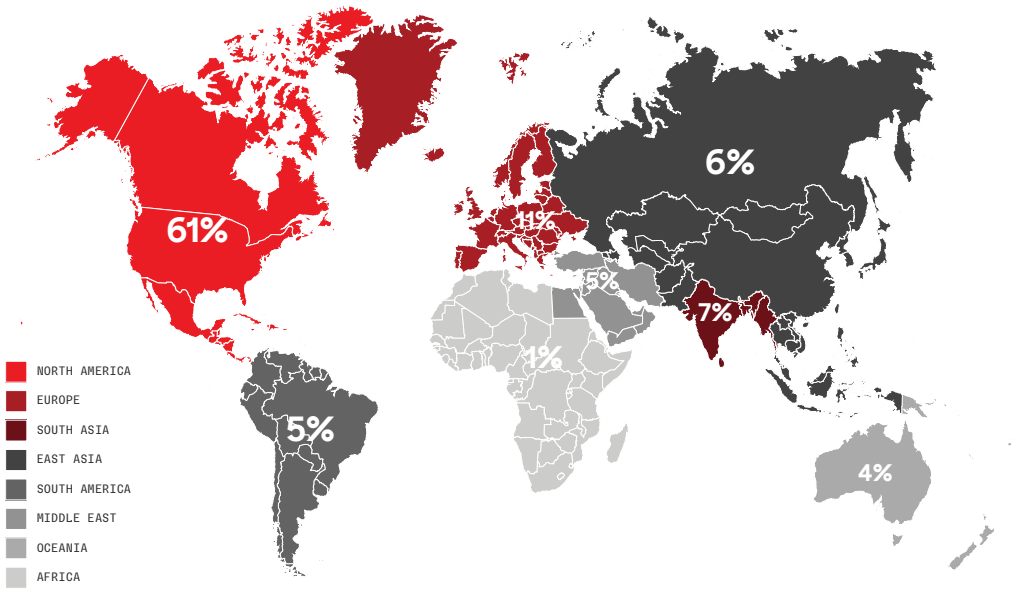
84% of adversary-attributed cloud-conscious intrusions were focused on eCrime

Today's cyber threats are particularly alarming due to the widespread use of hands-on or "interactive intrusion" techniques, which involve adversaries actively executing actions on a host to accomplish their objectives. Unlike malware attacks that depend on the deployment of malicious tooling and scripts, interactive intrusions leverage the creativity and problem-solving skills of human adversaries. These individuals can mimic expected user and administrator behavior, making it difficult for defenders to differentiate between legitimate user activity and a cyberattack.

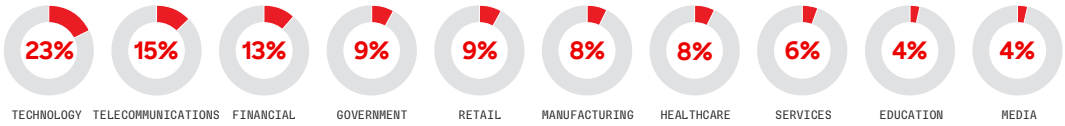
In 2023, CrowdStrike observed a 60% year-over-year increase in the number of interactive intrusion campaigns, with a 73% increase in the second half compared to 2022.

The technology sector was the most frequently targeted industry in which CrowdStrike CAO observed interactive intrusion activity in 2023, a continuing trend from 2022. The charts below reflect the relative frequency of intrusions in the top 10 industry verticals and in geographical regions.

Interactive Intrusions by Region



Interactive Intrusions by Industry

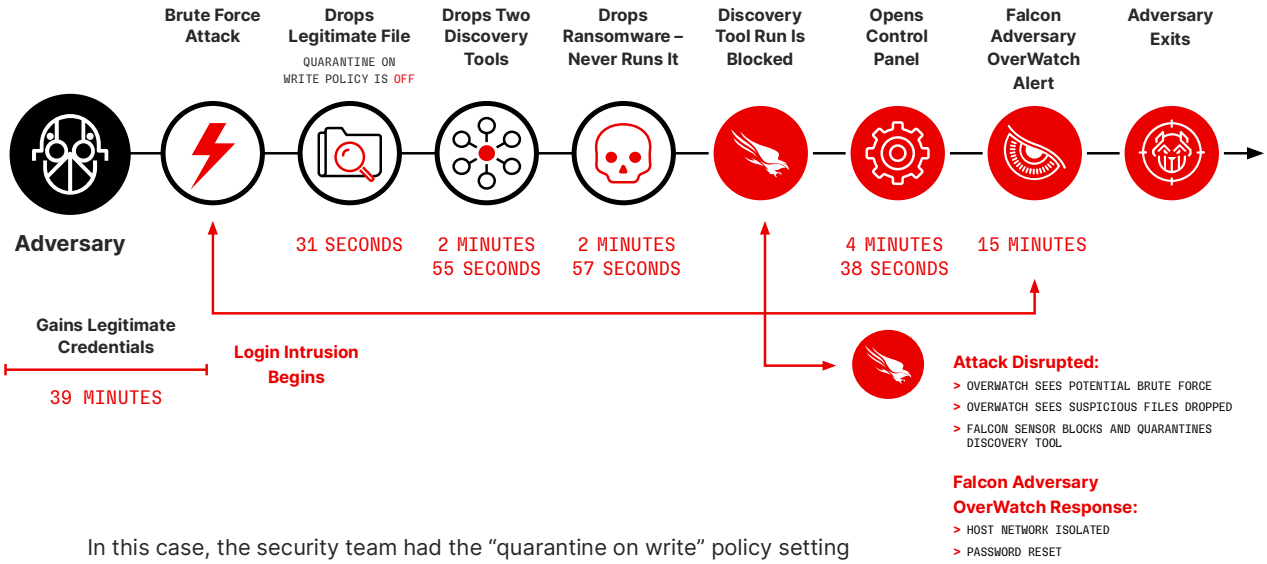


After gaining initial access to a network, adversaries seek to "break out" and move laterally from the compromised host to other hosts within the environment. The time it takes for them to do this — "breakout time" — is crucial because the initially compromised machines are rarely the ones adversaries need to achieve their goals. They must move laterally into the network, conduct reconnaissance, establish persistence and locate their targets. Responding within the breakout time window allows defenders to mitigate costs and other damages associated with intrusions.

This year, the average breakout time for interactive eCrime intrusion activity decreased from 84 minutes in 2022 to 62 minutes in 2023. The fastest observed breakout time was only 2 minutes and 7 seconds.

Anatomy of an eCrime Interactive Intrusion

To gain a better understanding of interactive intrusions, the following timeline illustrates the speed of a real-world hands-on attack:



In this case, the security team had the "quarantine on write" policy setting disabled, enabling the four files to be written to disk. The adversary executed a legitimate tool to obtain system information for reconnaissance and then dropped three more files, including ransomware, onto the system. They attempted to execute a network discovery and reconnaissance tool to map out lateral movement options, which was immediately blocked and quarantined by the Falcon sensor. This caused the adversary to open the control panel to understand which security tool was in use. When they identified the Falcon platform, they never attempted to execute the second discovery tool or the ransomware (which would have been prevented and quarantined) and moved to another victim. Within minutes, CrowdStrike CAO threat hunters notified the customer, took the machine offline and reset the user password.

Once an initial compromise occurs, it only takes seconds for adversaries to drop tools and/or malware on a victim's environment during an interactive intrusion. However, the saying "time is money" holds true for adversaries. More than 88% of the attack time was dedicated to breaking in and gaining initial access. By reducing or eliminating this time, adversaries free up resources to conduct more attacks.

To do this, they have continued to move beyond malware to faster, more effective means such as identity attacks (phishing, social engineering and access brokers) and the exploitation of vulnerabilities and trusted relationships. This trend is apparent over the last five years, as malware-free activity represented 75% of detections in 2023 — up from 71% in 2022.

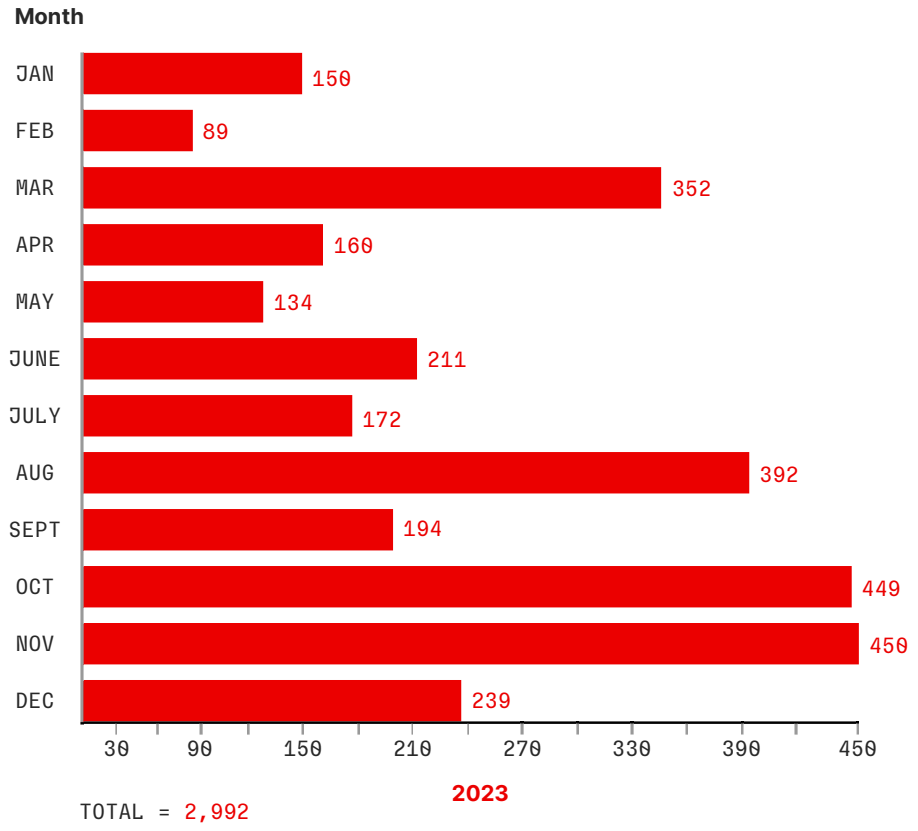
MALWARE-FREE ACTIVITY

»

75% 2023
71% 2022
62% 2021
51% 2020
40% 2019

This trend is partly related to the success of identity attacks, access brokers and the prolific abuse of valid credentials to facilitate access and persistence in victim environments. Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators. These adversaries continued to profit from providing initial access to a variety of eCrime threat actors in 2023, with the number of accesses advertised increasing by almost 20% compared to 2022.

Access Broker Advertisements by Month



Today's sophisticated cyberattacks only take minutes to succeed. Adversaries use techniques such as interactive hands-on-keyboard attacks and legitimate tools to attempt to hide from detection. To further accelerate attack tempo, adversaries can access credentials in multiple ways, including purchasing them from access brokers for a few hundred dollars. Organizations must prioritize protecting identities in 2024.

ADVERSARIES CONTINUE TO DEVELOP CLOUD-CONSCIOUSNESS

As predicted, cloud environment intrusions increased by 75% from 2022 to 2023 (Figure 2), with cloud-conscious cases increasing by 110% and cloud-agnostic cases increasing by 60%.

Cloud-conscious is a term referring to threat actors who are aware of the ability to compromise cloud workloads and use this knowledge to abuse features unique to the cloud for their own purposes.

eCrime adversaries are especially active in targeting cloud environments: 84% of cloud-conscious intrusions attributed to adversaries were conducted by likely eCrime actors, compared to 16% conducted by targeted intrusion actors. Traditional BGH adversaries, such as INDRIK SPIDER, became more cloud-conscious throughout the year.

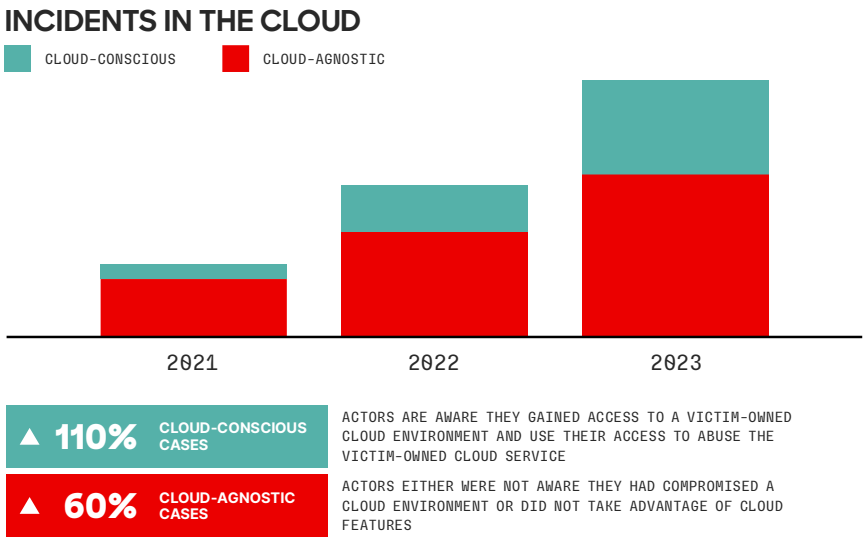


Figure 2. Increases in cloud cases

SCATTERED SPIDER predominantly drove cloud-conscious activity increases throughout 2023, accounting for 29% of total cases. Throughout 2023, SCATTERED SPIDER demonstrated progressive and sophisticated tradecraft within targeted cloud environments to maintain persistence, obtain credentials, move laterally and exfiltrate data.

Adversaries' preference for identity-based techniques is evident in their cloud-focused attacks. Next are several observations of cloud- and identity-focused activities categorized by the MITRE ATT&CK® enterprise tactics of Initial Access, Persistence, Privilege Escalation, Credential Access, Lateral Movement, Exfiltration and Impact.

AS PREDICTED, CLOUD ENVIRONMENT INTRUSIONS INCREASED BY 75% FROM 2022 TO 2023 (FIGURE 2), WITH CLOUD-CONSCIOUS CASES INCREASING BY 110% AND CLOUD-AGNOSTIC CASES INCREASING BY 60%.

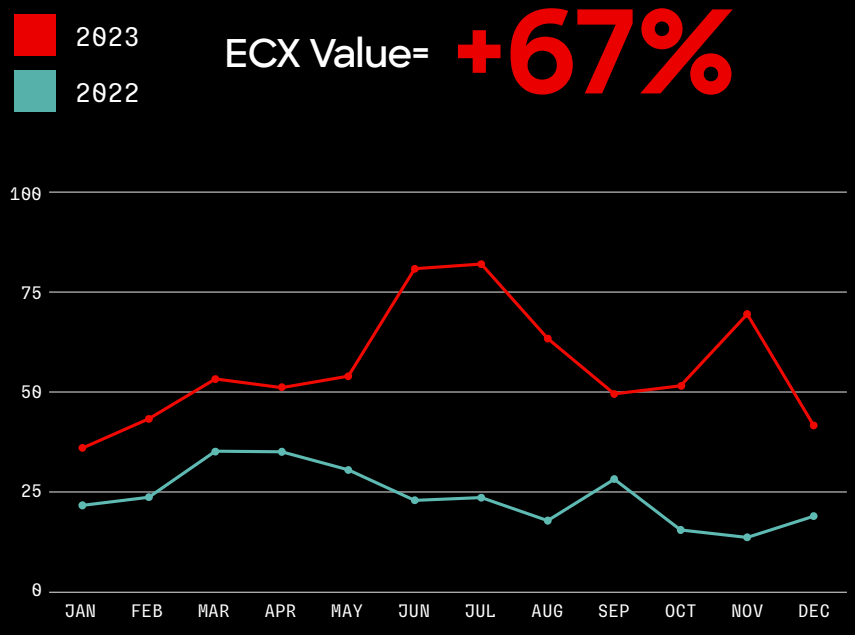
↑75%
IN CLOUD INTRUSIONS

eCrime Landscape

The CrowdStrike eCrime Index® (ECX) tracks activity — including the number of observed spam emails and the average cost of buying access to a corporate network — across multiple eCrime ecosystem segments and calculates the total number of observed ransomware victims.

Until May 2023, the ECX exhibited trends similar to those observed in 2022. However, from June 2023 onward, the ECX grew significantly, with major spikes between June and August. The most impactful contributors to these spikes included high BGH incident frequency and a sudden increase in observed DDoS attacks.

The ECX spiked again in November 2023, reflecting increases in spam email numbers and the rising average price for loaders and stealers.



New Vulnerabilities with 9/10 CVSS3 Score
+6%

BGH Incidents Involving Data Leaks
+76%

Average Loader Cost
+169%

Average Crypter Cost
+250%

Average Stealer Cost
+286%

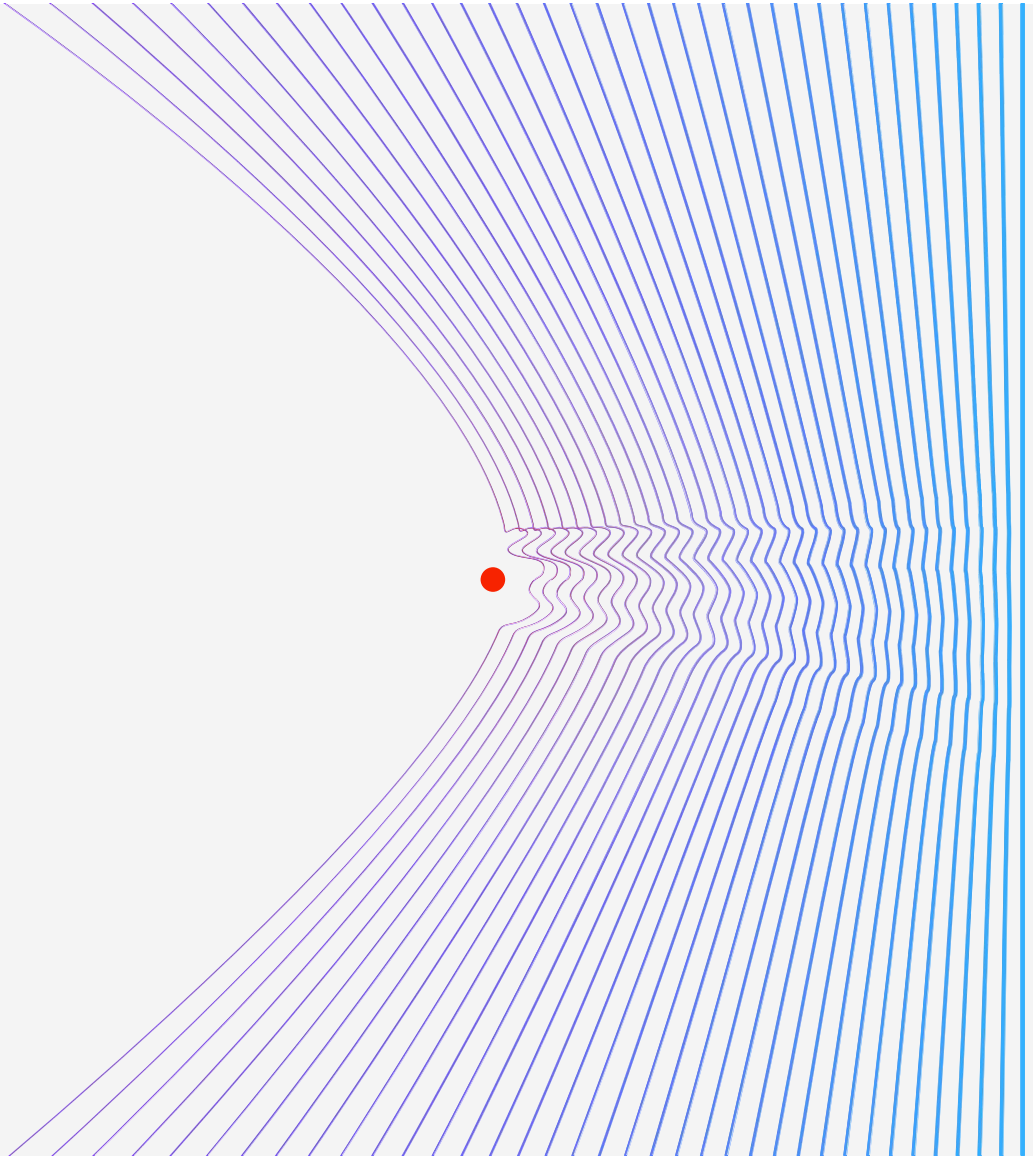
Average Ransom Demand
-27%

Identified Spam Emails
-15%

Figure 7. eCrime index value, 2022 vs. 2023, and key observable changes, 2023

IBM **Security**

Cost of a Data Breach Report 2023



IBM

01

Key findings

The key findings described here are based on IBM Security analysis of research data compiled by Ponemon Institute. Cost amounts in this report are measured in US dollars (USD).

USD 4.45M

Average total cost of a breach
The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million in the 2020 report.

51%

Percentage of organizations planning to increase security investments as a result of a breach
While data breach costs continued to rise, report participants were almost equally split on whether they plan to increase security investments because of a data breach. The top areas identified for additional investments included incident response (IR) planning and testing, employee training, and threat detection and response technologies.

USD 1.76M

The effect of extensive security AI and automation on the financial impact of a breach
Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches. Organizations that used these capabilities extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach. They also reported USD 1.76 million lower data breach costs compared to organizations that didn't use security AI and automation capabilities.

1 in 3

Number of breaches identified by an organization's own security teams or tools
Only one-third of companies discovered the data breach through their own security teams, highlighting a need for better threat detection. 67% of breaches were reported by a benign third party or by the attackers themselves. When attackers disclosed a breach, it cost organizations nearly USD 1 million more compared to internal detection.

USD 470,000

Additional cost experienced by organizations that didn't involve law enforcement in a ransomware attack
This year's research shows that excluding law enforcement from ransomware incidents led to higher costs. While 63% of respondents said they involved law enforcement, the 37% that didn't also paid 9.6% more and experienced a 33-day longer breach lifecycle.

53.3%

Since 2020, healthcare data breach costs have increased 53.3%
The highly regulated healthcare industry has seen a considerable rise in data breach costs since 2020. For the 13th year in a row, the healthcare industry reported the most expensive data breaches, at an average cost of USD 10.93 million.

82%

The percentage of breaches that involved data stored in the cloud—public, private or multiple environments
Cloud environments were frequent targets for cyberattackers in 2023. Attackers often gained access to multiple environments, with 39% of breaches spanning multiple environments and incurring a higher-than-average cost of USD 4.75 million.

USD 1.68M

Cost savings from high levels of DevSecOps adoption
Integrated security testing in the software development process (DevSecOps) showed sizable ROI in 2023. Organizations with high DevSecOps adoption saved USD 1.68 million compared to those with low or no adoption. Compared to other cost-mitigating factors, DevSecOps demonstrated the largest cost savings.

USD 1.49M

Cost savings achieved by organizations with high levels of IR planning and testing
In addition to being a priority investment for organizations, IR planning and testing emerged as a highly effective tactic for containing the cost of a data breach. Organizations with high levels of IR planning and testing saved USD 1.49 million compared to those with low levels.

USD 1.44M

Increase in data breach costs for organizations that had high levels of security system complexity
Organizations that reported low or no security system complexity experienced an average data breach cost of USD 3.84 million in 2023. Those with high levels of security system complexity reported an average cost of USD 5.28 million, representing an increase of 31.6%.

USD 1.02M

Average cost difference between breaches that took more than 200 days to find and resolve, and those that took less than 200 days
Time to identify and contain breaches—known as the breach lifecycle—continues to be integral to the overall financial impact. Breaches with identification and containment times under 200 days cost organizations USD 3.93 million. Those over 200 days cost USD 4.95 million—a difference of 23%.

Global highlights

The Cost of a Data Breach Report provides a global picture of the cost of data breaches, built using data from over 553 breaches in 16 different countries and taking into account hundreds of cost factors. This section examines critical metrics at the level of global average. We also explore the average per-record comparative costs between countries and industries.

USD 4.45M

Global average total cost of a data breach

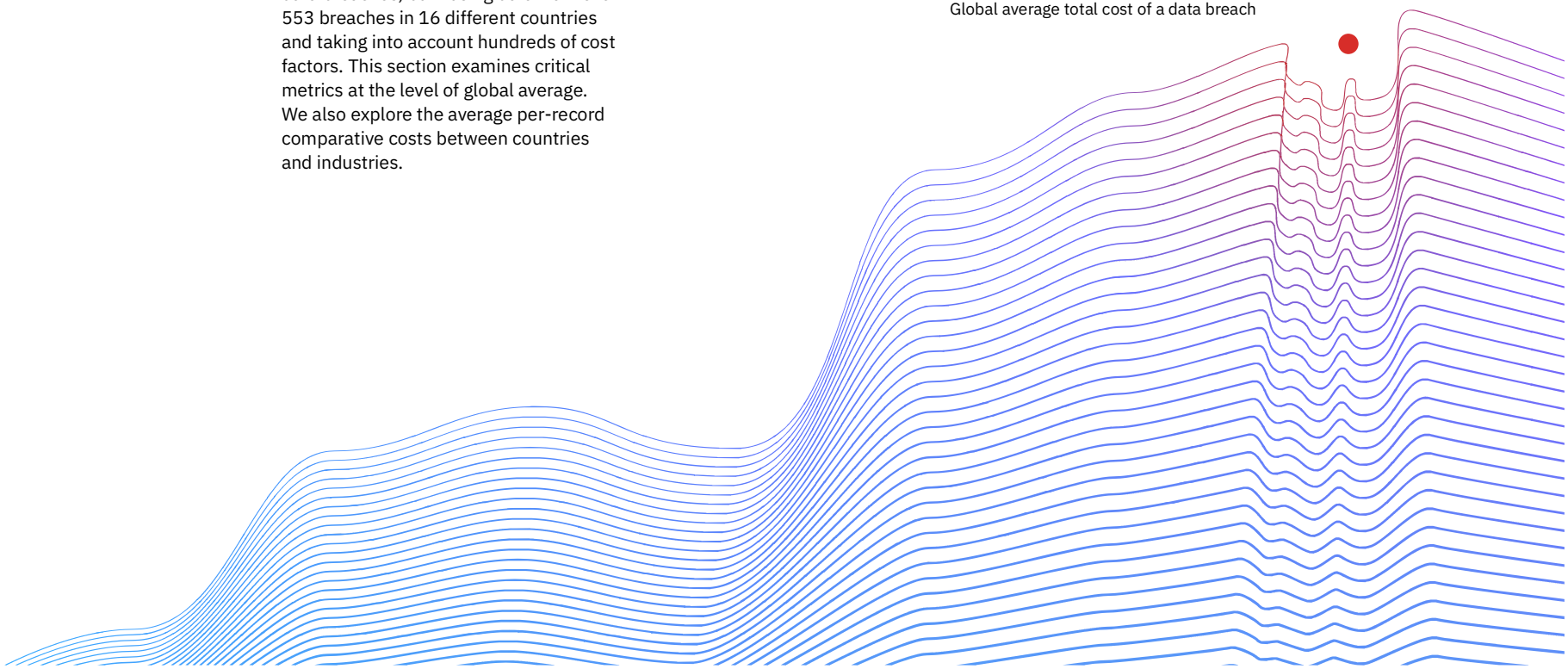


Figure 1. The cost of a data breach climbed to a new high.
Globally, the average cost of a data breach rose to USD 4.45 million, a USD 100,000 increase from 2022. This represents a 2.3% increase from the 2022 average cost of USD 4.35 million. Since 2020, when the average total cost of a data breach was USD 3.86 million, the average total cost has increased 15.3%.

Figure 2. Per-record cost of a data breach also reached a new high.
In 2023, the average cost per record involved in a data breach was USD 165, a small increase from the 2022 average of USD 164. This matches the relatively small growth from 2021 to 2022, where the cost rose by just USD 3. In the last seven years, the largest increase in average per-record costs was between 2020 and 2021, when the average rose from USD 146 to USD 161 or 10.3%. This study examined breaches sized between 2,200 and 102,000 records.[1]

Total cost of a data breach

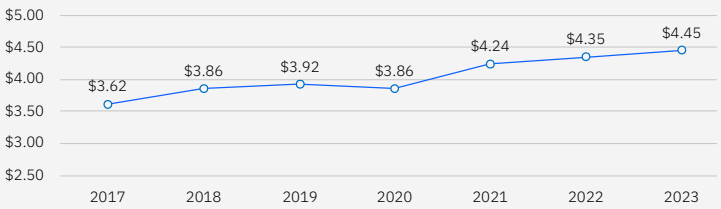


Figure 1. Measured in USD millions

Per-record cost of a data breach

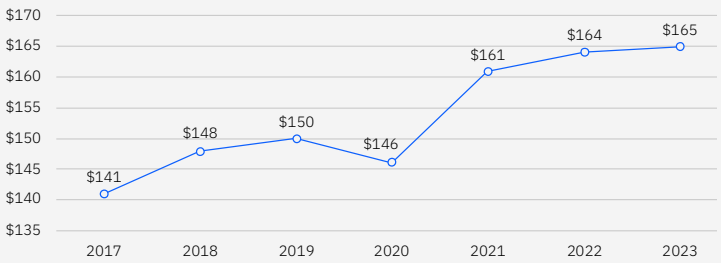


Figure 2. Measured in USD

Figure 3. For the 13th consecutive year, the United States held the title for the highest data breach costs.
The top five countries or regions with the highest average cost of a data breach saw considerable changes from 2022.

		2023	2022
1	↑	**United States** USD 9.48 million	**United States** USD 9.44 million
2	↑	**Middle East** USD 8.07 million	**Middle East** USD 7.46 million
3	↓	**Canada** USD 5.13 million	**Canada** USD 5.64 million
4	↓	**Germany** USD 4.67 million	**United Kingdom** USD 5.05 million
5	↓	**Japan** USD 4.52 million	**Germany** USD 4.85 million

Of this year's top five, Japan is the only country that didn't appear on the 2022 top five list, moving up from the number 6 most expensive spot last year. The top 5 list last year also included the United Kingdom (UK) at an average data breach cost of USD 5.05 million. This year, the UK saw a significant drop in average cost at USD 4.21 million—down 16.6% from last year—resulting in placement just outside of the top five.

The United States again had the highest average total cost of a data breach at USD 9.48 million, an increase of 0.4% from last year's USD 9.44 million. Like last year, the Middle East had the second-highest average total cost of a data breach at USD 8.07 million, up 8.2% from USD 7.46 million.

In Canada, the average total cost of a data breach decreased from USD 5.64 million to USD 5.13 million or 9%. The average cost also decreased in Germany, dropping from USD 4.85 million to USD 4.67 million or 3.7%. Japan saw the average drop slightly, from USD 4.57 million to USD 4.52 million or 1.1%.

Cost of a data breach by country or region

Figure 3. Measured in USD millions

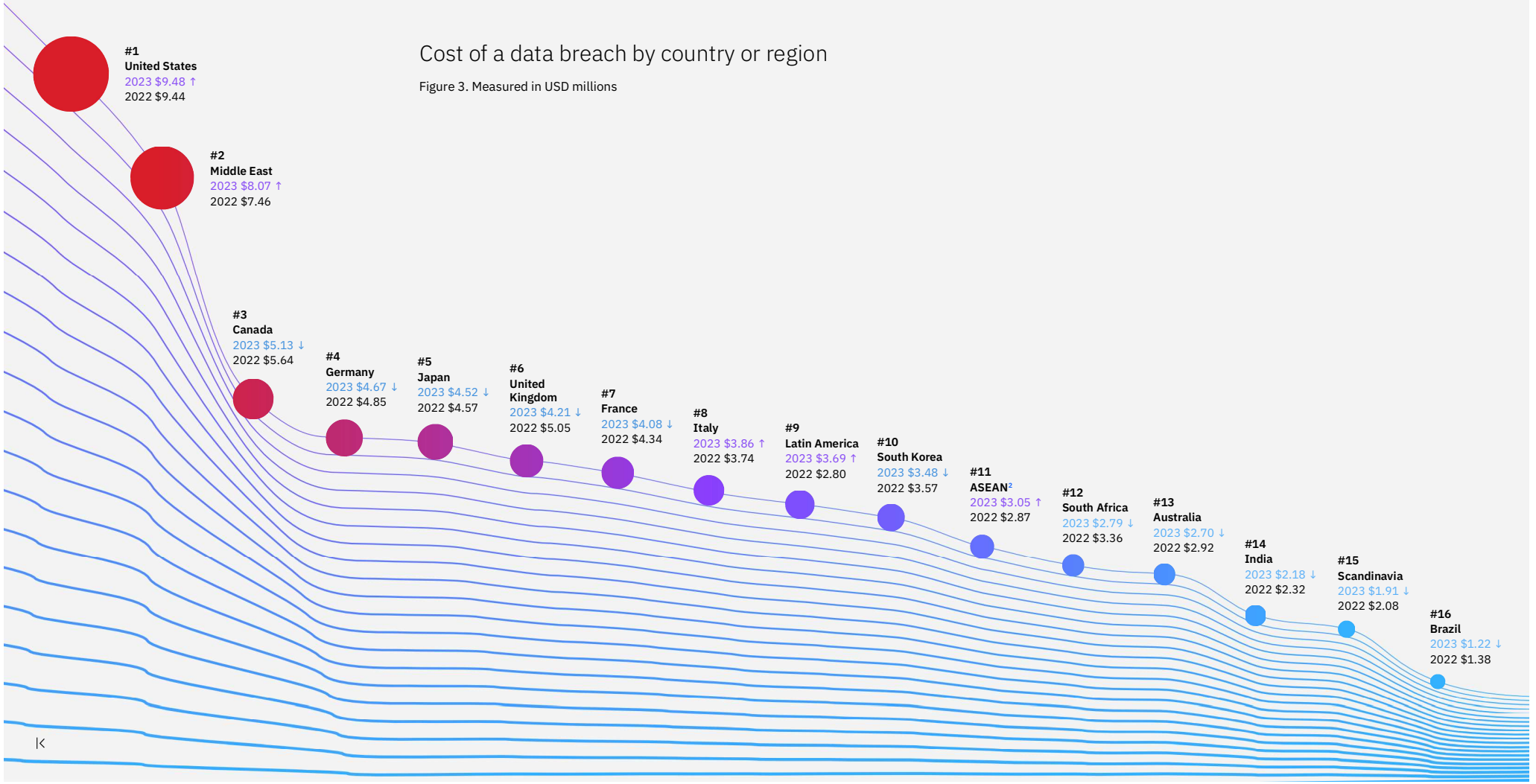


Figure 4. Across industries, healthcare reported the highest costs for the 13th year in a row.
Healthcare continues to experience the highest data breach costs of all industries, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. Over the past three years, the average cost of a data breach in healthcare has grown 53.3%, increasing more than USD 3 million compared to the average cost of USD 7.13 million in 2020. Healthcare faces high levels of industry regulation and is considered critical infrastructure by the US government. Since the start of the COVID-19 pandemic, the industry has seen notably higher average data breach costs.

The top five most costly industries underwent some changes from last year's rankings. Technology dropped out of the top five while the industrial sector was added, showing a 5.8% increase as it moved from the seventh-highest to the fifth. According to IBM threat intelligence, manufacturing is the industry most commonly targeted by cybercriminals.

	2023	2022
1 ↑	**Healthcare** USD 10.93 million	**Healthcare** USD 10.10 million
2 ↓	**Financial** USD 5.90 million	**Financial** USD 5.97 million
3 ↓	**Pharmaceuticals** USD 4.82 million	**Pharmaceuticals** USD 5.01 million
4 ↑	**Energy** USD 4.78 million	**Technology** USD 4.97 million
5 ↑	**Industrial** USD 4.73 million	**Energy** USD 4.72 million

Cost of a data breach by industry

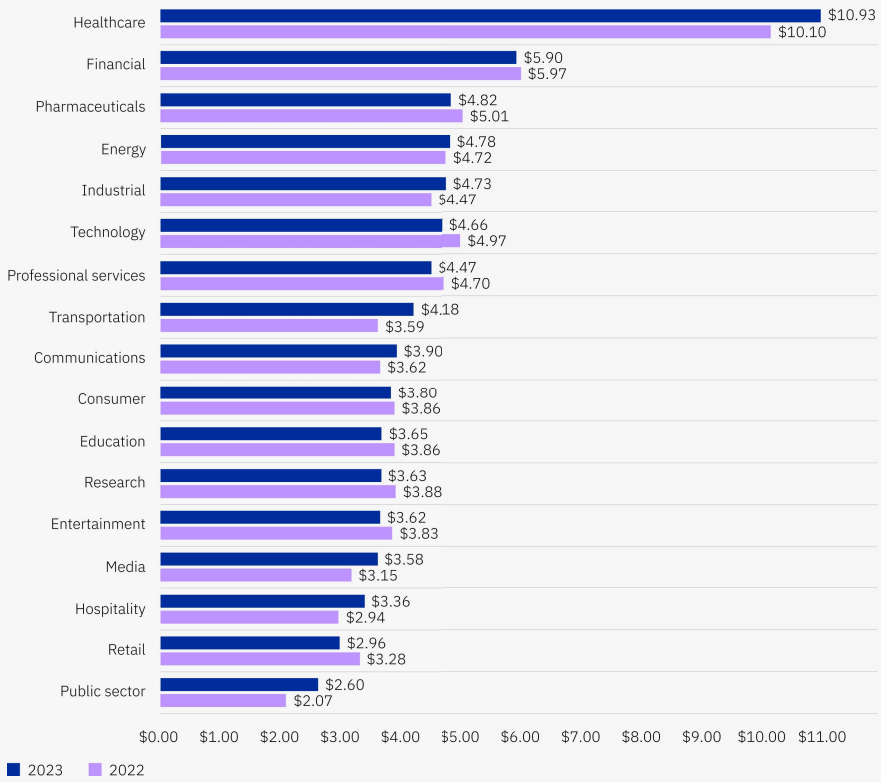


Figure 4. Measured in USD millions

Figure 5. Mean times to identify and contain breaches stayed roughly the same.
Compared to 2022, both the mean time to identify (MTTI) and the mean time to contain (MTTC) breaches saw only marginal changes. Mean time to identify refers to the time it takes an organization to uncover a security breach. Mean time to contain refers to the time required to resolve a security breach once it has been identified.

In 2022, it took organizations 207 days to identify a breach. In 2023, it took only 204 days. On the other hand, organizations required an average of 73 days to contain breaches in 2023, while they required just 70 days on average in 2022. The highest mean times to contain and identify breaches both occurred in 2021, at 212 and 75 days, respectively.

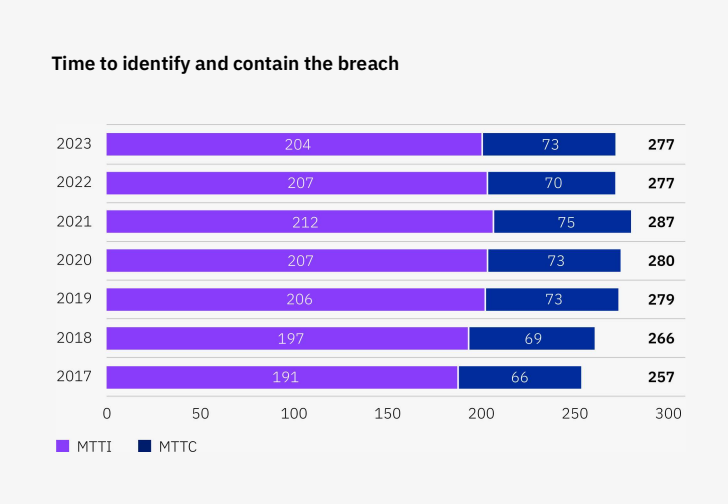


Figure 5. Measured in days

Figure 6. Lost business costs hit a five-year low.
Last year's report saw detection and escalation costs rise to become the costliest category of data breach expenses, indicating a shift toward longer and more-complex breach investigations. The trend continued this year as detection and escalation costs remained in the top spot and rose from USD 1.44 million to USD 1.58 million, demonstrating a change of USD 140,000 or 9.7%. Detection and escalation costs include activities that enable a company to reasonably detect a breach and can include forensic and investigative activities, assessment and audit services, crisis management, and communications to executives and boards.

The other key cost segments of a data breach—lost business cost, post-breach response and notification—also saw changes compared to 2022. Lost business costs dropped 8.5%, from USD 1.42 million in 2022 to USD 1.30 million in 2023. Lost business costs include activities such as business disruptions and revenue losses from system downtime, the cost of lost customers and acquiring new customers, and reputation losses and diminished goodwill.

Notably, the notification cost segment rose from USD 310,000 in 2022 to USD 370,000 in 2023, which represents a 19.4% increase. Post-breach response costs rose by just USD 20,000. Notification costs include activities that enable the company to notify data subjects, data protection regulators and other third parties.

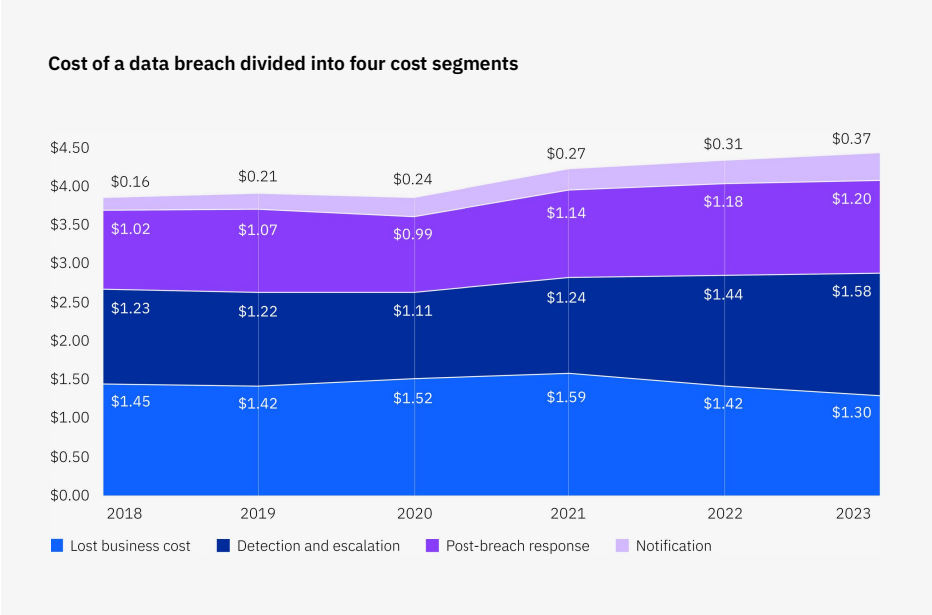


Figure 6. Measured in USD millions

Figure 7. Smaller organizations faced considerably higher data breach costs than last year.
In 2023, organizations with more than 5,000 employees saw the average cost of a data breach decrease compared to 2022. On the other hand, those with 5,000 or fewer employees saw considerable increases in the average cost of a data breach.

Organizations with fewer than 500 employees reported that the average impact of a data breach increased from USD 2.92 million to USD 3.31 million or 13.4%. Those with 500–1,000 employees saw an increase of 21.4%, from USD 2.71 million to USD 3.29 million. In the 1,001–5,000 employee range, the average cost of a data breach increased from USD 4.06 million to USD 4.87 million, rising nearly 20%.

In the 10,001–25,000 range, respondents reported an average cost of USD 5.46 million, a decrease of 1.8% from 2022's figure of USD 5.56 million. Organizations with more than 25,000 employees saw the average cost drop from USD 5.56 million in 2022 to USD 5.42 million in 2023, a decrease of USD 140,000 or 2.5%.

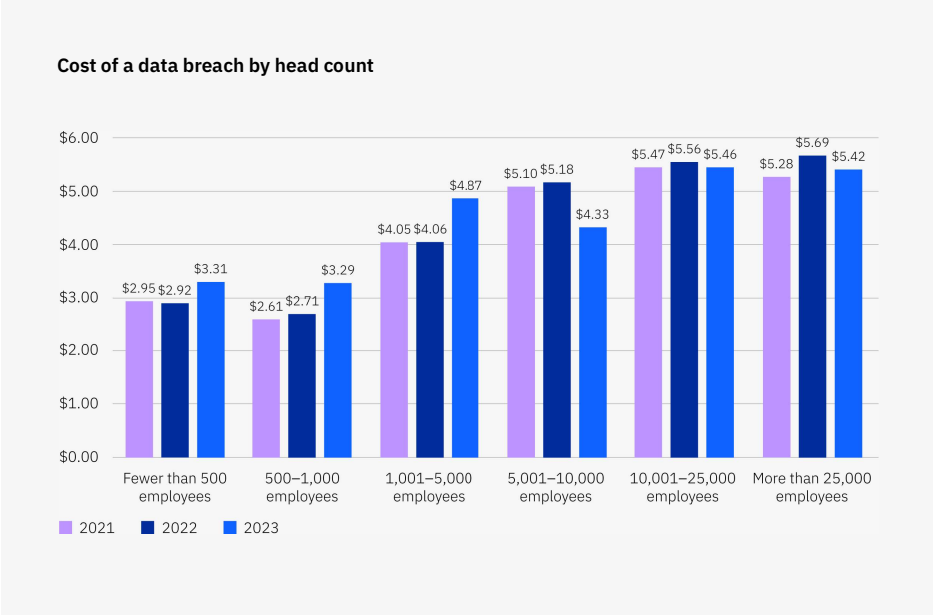


Figure 7. Measured in USD millions

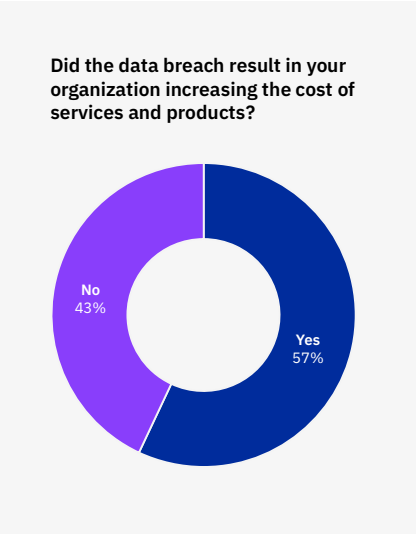


Figure 8. Share of total sample of breached organizations

Figure 8. Most organizations continue to increase the prices of services and products as a result of a data breach. The majority (57%) of respondents indicated that data breaches led to an increase in the pricing of their business offerings, passing on costs to consumers. This finding is similar to our 2022 report, where 60% of respondents said they increased prices.

Figures 9a and 9b. Customer PII was the costliest—and most common—record compromised.
Of all record types, customer and employee personal identifiable information (PII) was the costliest to have compromised. In 2023, customer PII such as names and Social Security numbers cost organizations USD 183 per record, with employee PII close behind at USD 181 per record. The least expensive record type to have compromised is anonymized customer data, which cost organizations USD 138 per record in 2023.

As was the case in 2022 and 2021, customer PII was the most commonly breached record type in 2023. 52% of all breaches involved some form of customer PII. This is an increase of five percentage points from 2022, when customer PII accounted for 47% of all data compromised. The second-most commonly compromised data type was employee PII at 40%. Compromised employee PII has seen sizable growth from 2021, when it only accounted for 26% of all records compromised.

Compromised intellectual property grew three percentage points since 2022, while anonymized (non-PII) data dropped seven percentage points from 2022—decreasing from 33% to 26%. Other corporate data, such as financial information and client lists, increased from 15% of data compromised in 2022 to 21% in 2023.

Type of data compromised

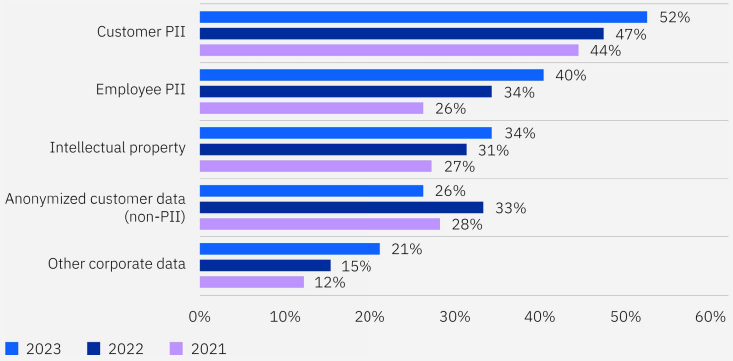


Figure 9a. More than one response permitted

Per-record cost of a data breach by type of record compromised

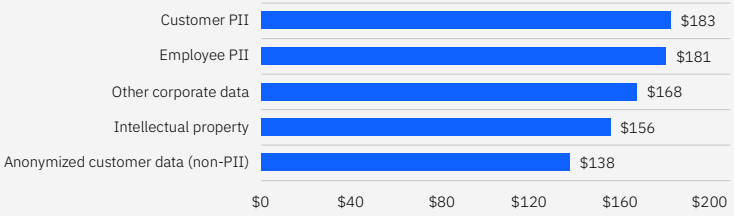
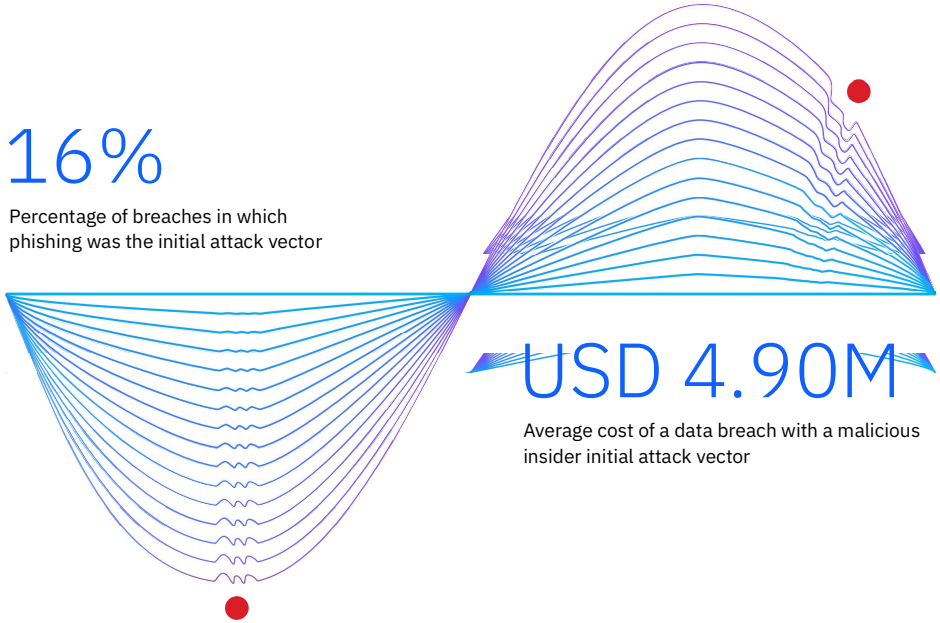


Figure 9b. Measured in USD

Initial attack vectors

This section examines the initial attack vector identified for data breaches in the study and its impact on the breach cost and timeline. It identifies the most common root causes for data breaches in the report and compares the average cost of breaches for each category as well as the average time to identify and contain those breaches. Phishing and stolen or compromised credentials were the two most prevalent attack vectors in this year's report, and both also ranked among the top four costliest incident types.



16%

Percentage of breaches in which phishing was the initial attack vector

USD 4.90M

Average cost of a data breach with a malicious insider initial attack vector

Figure 10. Phishing and stolen or compromised credentials were the two most common initial attack vectors. Phishing and stolen or compromised credentials were responsible for 16% and 15% of breaches, respectively, with phishing moving into the lead spot by a small margin over stolen credentials, which was the most common vector in the 2022 report. Cloud misconfiguration was identified as the initial vector for 11% of attacks, followed by business email compromise at 9%. This year, for the first time, the report examined both zero-day (unknown) vulnerabilities as well as known, unpatched vulnerabilities as the source of the data breach and found that more than 5% of the breaches studied originated from known vulnerabilities that had yet to be patched.

Although relatively rare at 6% of occurrences, attacks initiated by malicious insiders were the costliest, at an average of USD 4.90 million, which is 9.6% higher than the global average cost of USD 4.45 million per data breach. Phishing was the most prevalent attack vector and the second most expensive at USD 4.76 million. Breaches attributed to system error were the least costly, at an average of USD 3.96 million, and the least common, at 5% of occurrences.

Cost and frequency of a data breach by initial attack vector

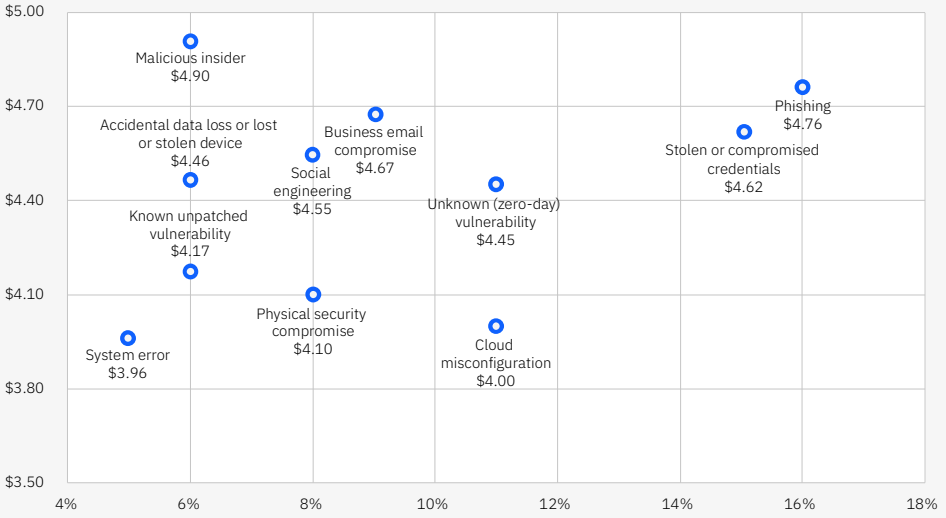


Figure 10. Measured in USD millions

Figure 11. Breaches that initiated with stolen or compromised credentials and malicious insiders took the longest to resolve.
This year, it took nearly 11 months (328 days) to identify and contain data breaches resulting from stolen or compromised credentials, on average, and about 10 months (308 days) to resolve breaches that were initiated by a malicious insider. Those two vectors, along with phishing and business email compromise, were also responsible for the costliest breaches.

As a point of comparison, the overall mean time to identify and contain a data breach was 277 days or just over nine months. That figure has remained relatively constant over the past few years of the report.

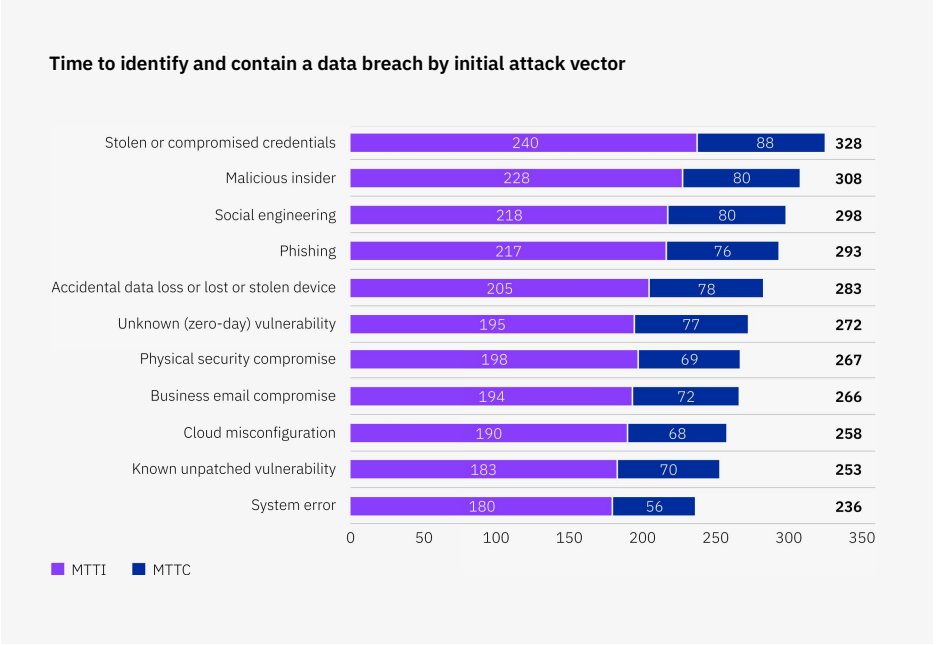
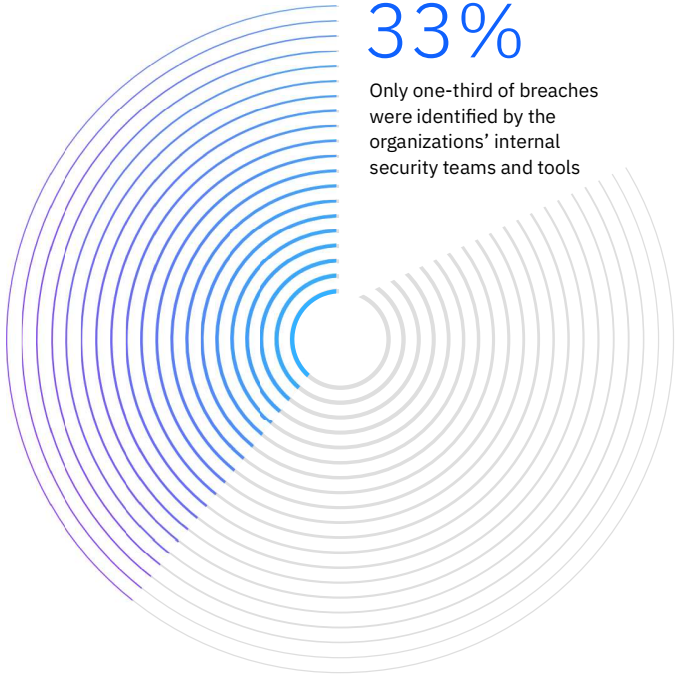


Figure 11. Measured in days

Identifying attacks

This section looks at how breaches were identified and the differences in cost and containment time based on the identification method, analyses that are reported for the first time this year. There are three categories that define how breaches are identified: by an organization's internal security teams and tools, including managed security service providers (MSSPs); by a benign third party, such as a security researcher or law enforcement; and by disclosure from the attacker, as in the case of ransomware.



33%

Only one-third of breaches were identified by the organizations' internal security teams and tools

Figure 12. Breaches were most commonly identified by a benign third party.
40% of breaches were identified by a benign third party or outsider, whereas 33% of breaches were identified by internal teams and tools. Over one-quarter or 27% of breaches were disclosed by the attacker as part of a ransomware attack.

Figure 13. Data breaches disclosed by the attacker, such as with ransomware, cost significantly more.
Attacks disclosed by attackers had an average cost of USD 5.23 million, which was a 19.5% or USD 930,000 difference over the average cost of breaches identified through internal security teams or tools of USD 4.30 million. Additionally, breaches disclosed by attackers cost 16.1% or USD 780,000 more than the USD 4.45 million average cost of a data breach for 2023. Breaches identified by an organization's own security teams and tools were significantly less expensive, costing nearly USD 1 million less than incidents disclosed by the attacker.

How was the breach identified?

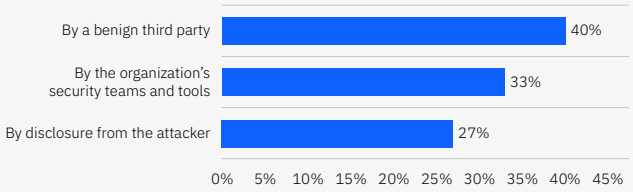


Figure 12. Only one response permitted

Cost of a data breach by how the breach was identified

Figure 13. Measured in USD millions

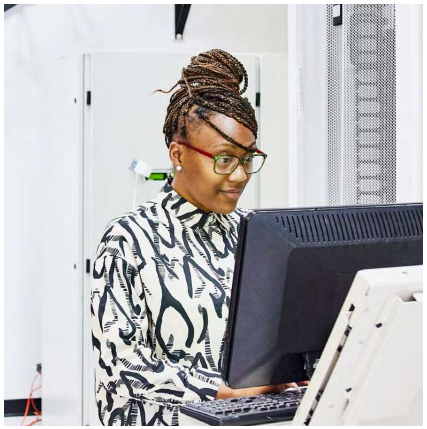


Figure 14. Data breaches disclosed by the attacker also took the longest time to identify and contain.
Respondents required a mean time of 320 days to identify and contain breaches disclosed by the attacker. This time frame was 80 additional days or 28.2% longer compared to breaches identified internally, which took a mean time of 241 days to identify and contain. The mean time to identify and contain a breach disclosed by the attacker took 47 days or 15.9% longer compared to breaches identified by a benign third party.

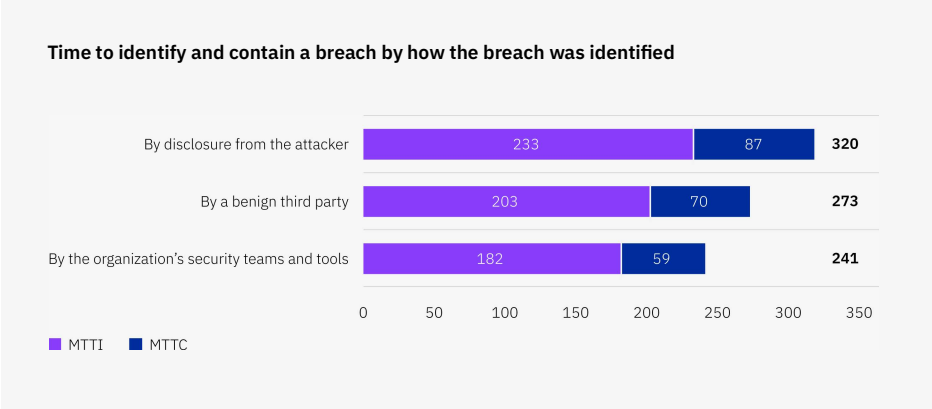


Figure 14. Measured in days

Data breach lifecycle

The data breach lifecycle is defined as the elapsed time between the initial detection of the breach and its containment. “Time to identify” describes the time, in days, it takes to discover an incident. “Time to contain” refers to the time, in days, it takes for an organization to resolve the situation and restore service after the breach has been detected. These two metrics help determine the effectiveness of an organization’s IR and containment processes.

277 days

Time to identify and contain a data breach

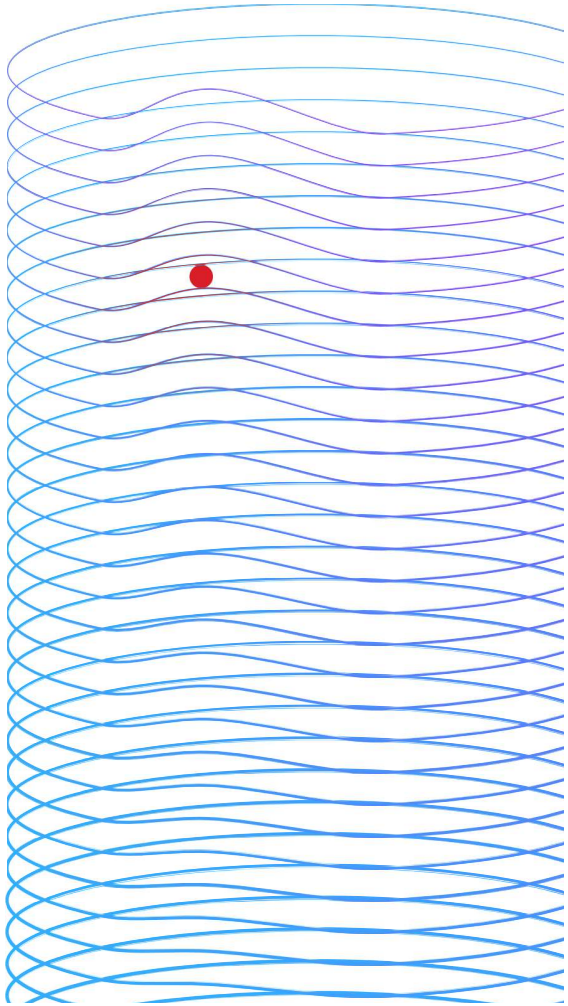


Figure 15. A shorter data breach lifecycle continues to be associated with lower data breach costs.
A shorter data breach lifecycle of fewer than 200 days was associated with an average cost of USD 3.93 million, while a longer lifecycle of more than 200 days was associated with an average cost of USD 4.95 million. This reflects a 23% difference and a cost savings of USD 1.02 million for the shorter lifecycle.

Looking back at previous years, the average cost of a data breach based on the 200-day lifecycle has been relatively consistent, although it changed incrementally.

For a data breach lifecycle of fewer than 200 days, the 2023 value of USD 3.93 million grew 5.1% from the previous year's average cost of USD 3.74 million. For a data breach lifecycle of more than 200 days, the 2023 value of USD 4.95 million grew 1.9% from the previous year's average cost of USD 4.86 million. The average cost savings of USD 1.02 million reported in 2023 reflects an 8.9% decrease from 2022's cost savings of USD 1.12 million.

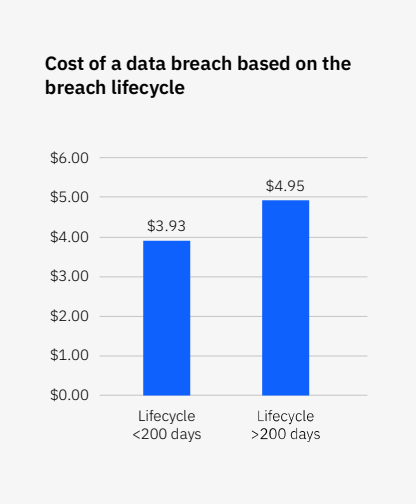


Figure 15. Measured in USD millions

Key cost factors

The types of security technologies and practices employed within an organization are among many factors that influence the mean cost of a data breach. This section quantifies 27 cost factors to help security and risk decision-makers understand the degree to which these factors amplify or mitigate costs. These factors aren't additive, so it's not consistent with the research methodology to add multiple cost factors together to calculate the potential cost of a breach.

This year, the Cost of a Data Breach Report considers several new factors, including supply chain breaches, ASM tools, data security and protection software, endpoint detection and response (EDR) tools, threat intelligence, proactive threat hunting, IR teams, and security orchestration, automation and response (SOAR) tools.

USD 5.36M

Average cost of a breach for organizations with high levels of security skills shortage

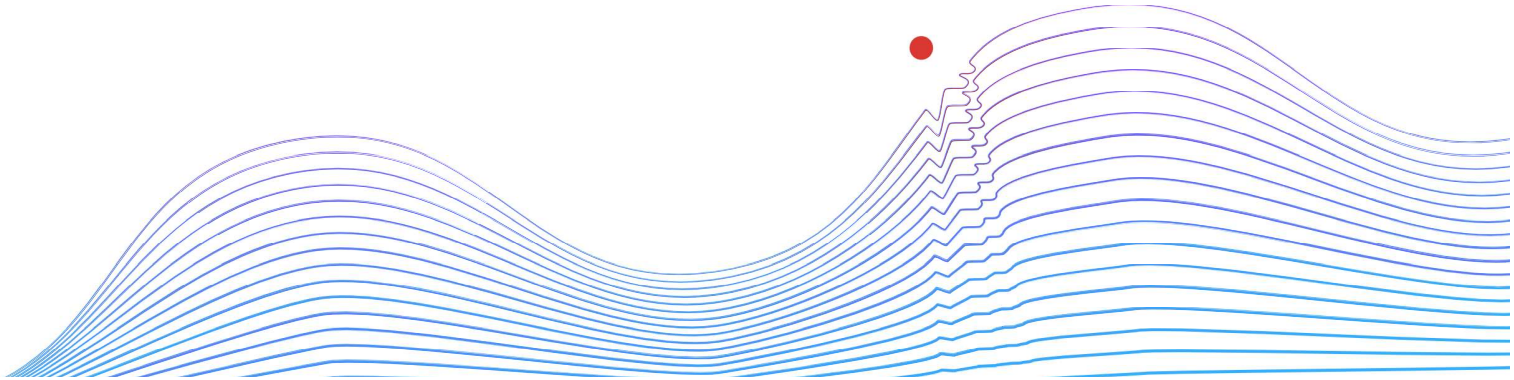


Figure 16. The impact of 27 factors on the mean cost of a data breach.
The chart demonstrates the average cost difference of breaches at organizations with these cost-influencing factors compared to the overall average data breach cost of USD 4.45 million. Cost mitigators describe those factors that are associated with a lower-than-average breach cost, while cost amplifiers are associated with a higher-than-average breach cost.

The three factors that rank most effective as cost mitigators—those associated with the biggest cost reduction—are the adoption of a DevSecOps approach, employee training, and IR planning and testing. For example, breaches at organizations with a DevSecOps approach in place had an average cost that was USD 249,000 less than the 2023 mean cost of a data breach of USD 4.45 million or approximately USD 4.20 million.

The biggest cost amplifiers were security system complexity, security skills shortage, and noncompliance with regulations. For example, breaches at organizations with security system complexity had an average cost of USD 241,000 more than the 2023 mean cost of a data breach of USD 4.45 million or approximately USD 4.69 million.

Impact of key factors on total cost of a data breach

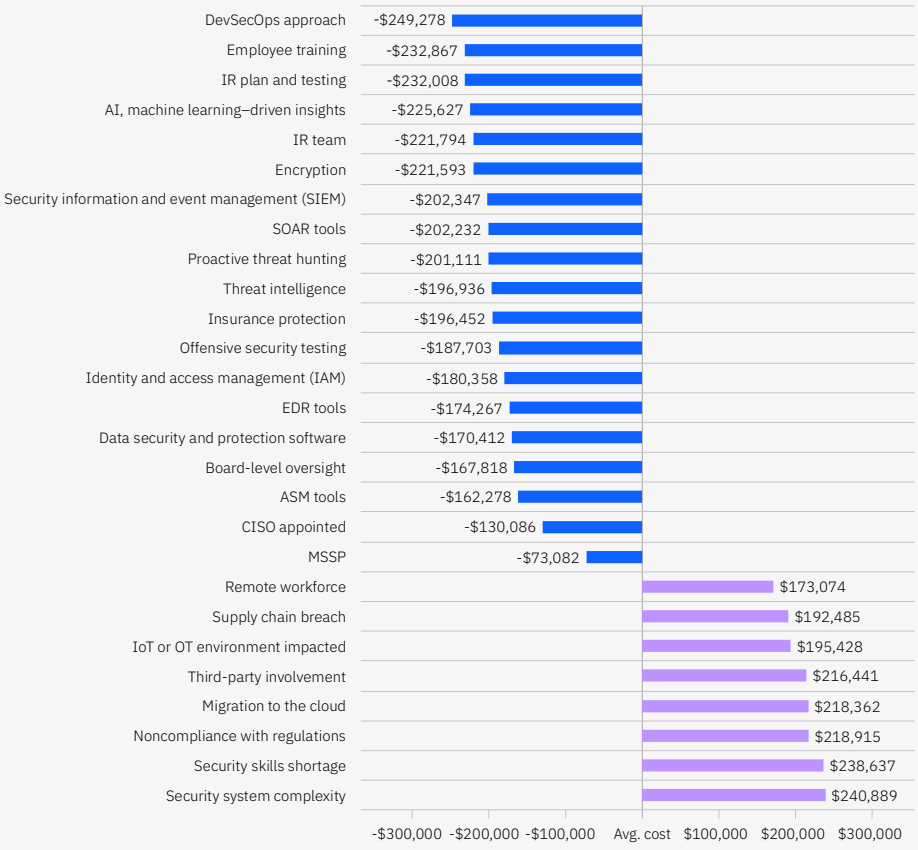


Figure 16. Measured in USD

Figure 17. The three most impactful cost amplifiers out of 27 factors.
This chart compares organizations with the highest levels of a top-ranking cost amplifier to those with the lowest level, which in some cases could mean no instance of that same factor. This comparison differs from the prior analysis (Figure 16) in which a high presence of these factors is compared to the mean. There was a difference of USD 1.58 million or 34.6% between high levels and low levels of secrity skills shortage. A difference of USD 1.44 million or 31.6% occurred between high levels and low levels of security system complexity. And there was a difference of USD 1.04 million or 23% between high levels and low levels of noncompliance with regulations.

Organizations with a high level of security skills shortage had a USD 5.36 million average cost, which was USD 910,000 higher than the average cost of a data breach, a difference of 18.6%. Those with a high level of security system complexity had a USD 5.28 million average cost, for a difference of USD 830,000 or 17.1% compared to the average cost of a data breach. Organizations with a high level of noncompliance with regulations showed an average cost of USD 5.05 million, which exceeded the average cost of a data breach by USD 560,000, a difference of 12.6%.

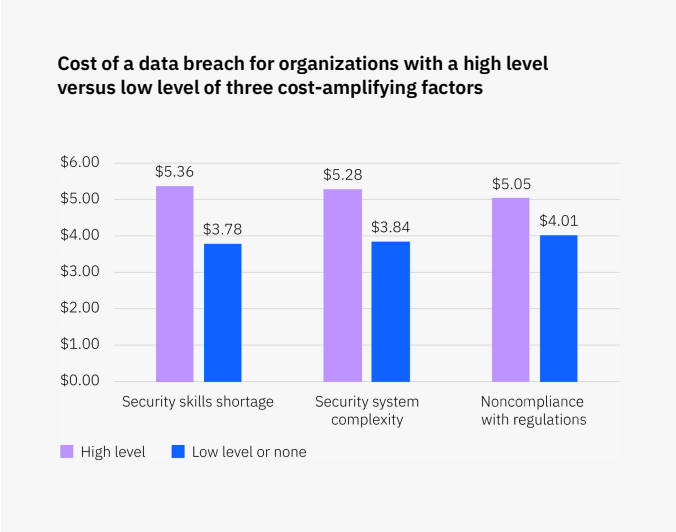


Figure 17. Measured in USD millions

Figure 18. The three most impactful cost mitigators out of 27 factors.
The chart compares organizations with the highest levels of a top-ranking cost mitigator to those with the lowest level, which in some cases could mean no instance of that same factor. The average cost of a breach showed a difference of USD 1.68 million or 38.4% between organizations with high levels and low levels of a DevSecOps approach. There was a difference of USD 1.49 million or 34.1% between high levels and little to no IR planning and testing. And last, there was a difference of USD 1.5 million or 33.9% between high levels and low levels of employee training.

Organizations with high levels of these cost mitigators present had a significantly lower than average cost of a data breach. High-level DevSecOps adopters had an average cost of USD 3.54 million—a difference of USD 910,000 or 22.8% compared to the overall average cost of a data breach. Organizations with a low usage of a DevSecOps approach had an average cost of USD 5.22 million, which was significantly higher by a difference of USD 770,000 or 15.9% compared to the average cost of a data breach.

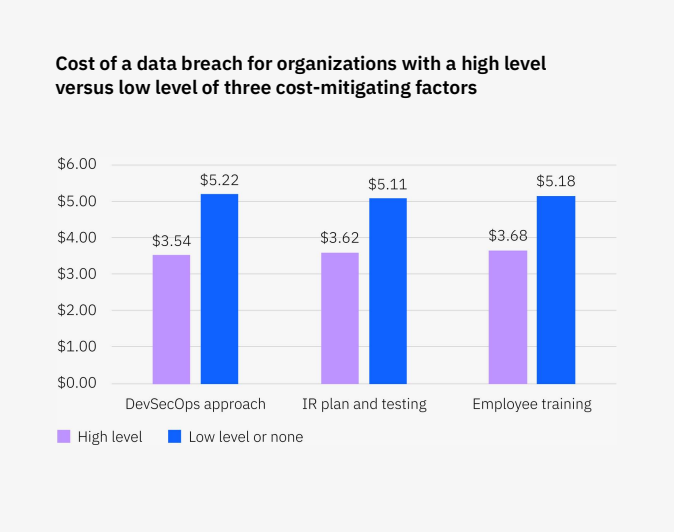


Figure 18. Measured in USD millions

Ransomware and destructive attacks

This year, ransomware and destructive attacks[3] accounted for 24% and 25% of malicious attacks, respectively.

As in the 2022 report, we looked at the lifecycle of these types of breaches and the impact of paying a ransom compared to not paying a ransom. This study doesn't include the cost of the ransom in calculating the total cost of the breach. In the 2023 report, for the first time, we examined the influence of involving law enforcement in the effort to contain a ransomware attack.

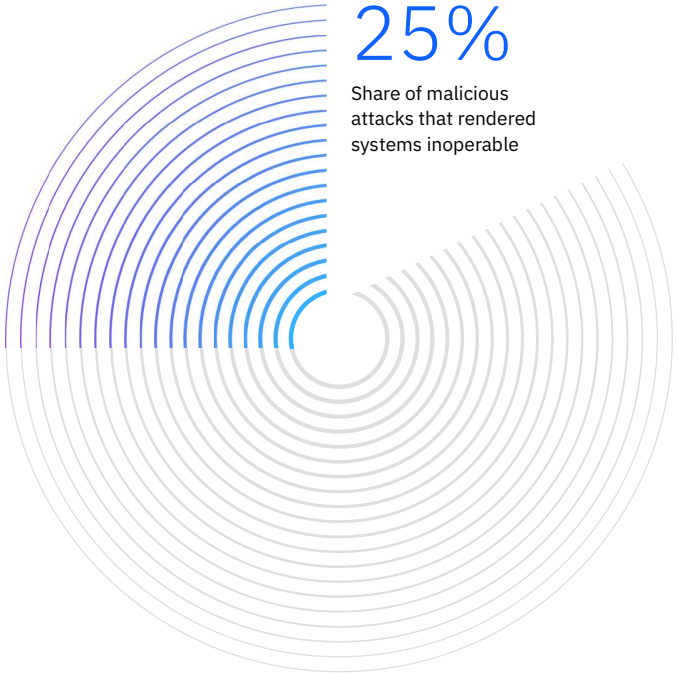


Figure 19. Nearly one-quarter of attacks involved ransomware.
Destructive attacks that left systems inoperable accounted for one out of every four attacks, and another 24% involved ransomware. Business partner and software supply chain attacks accounted for 15% and 12% of attacks, respectively.

Figure 20. Ransomware attack costs increased significantly.
At USD 5.13 million, the average cost of a ransomware attack in the 2023 report increased 13% from the average cost of USD 4.54 million in the 2022 report. At USD 5.24 million, the average cost of a destructive attack in the 2023 report also increased 2.3% from the average cost of USD 5.12 million in the 2022 report.

Share of total breaches by type of malicious attack

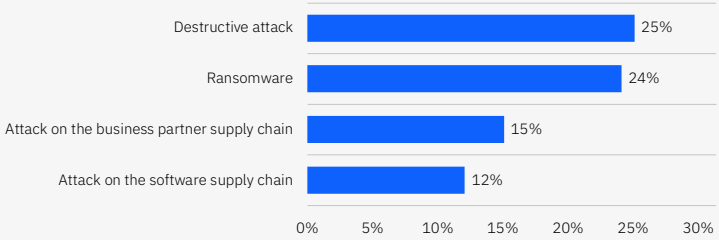


Figure 19. Percentages for each attack type shown are out of total breaches; bars will not sum to 100%

Cost of a ransomware or destructive attack

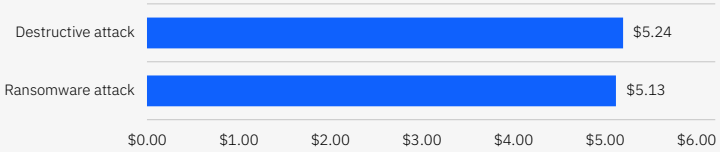


Figure 20. Measured in USD millions

Figures 21 and 22. Organizations that involved law enforcement saw significant time and cost savings.
37% of ransomware victims opted not to involve law enforcement to help contain a ransomware breach, but those that did experienced a less costly ransomware breach overall. The average cost of a ransomware breach was USD 5.11 million when law enforcement wasn't involved and USD 4.64 million when law enforcement was involved, for a difference of 9.6% or USD 470,000.

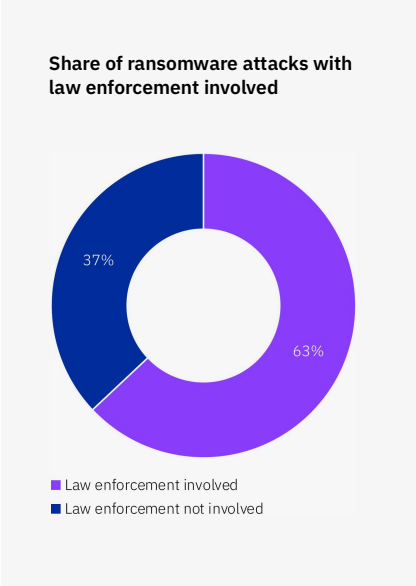


Figure 21. Share of all ransomware attacks

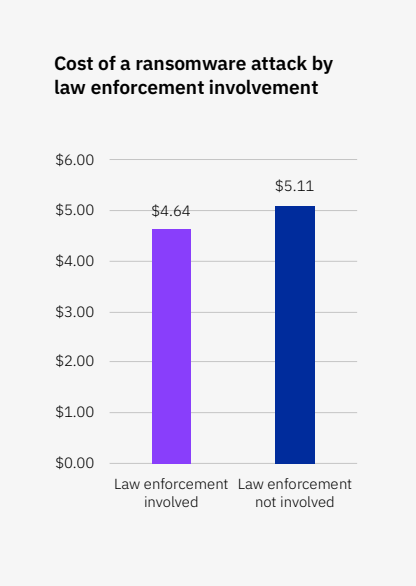


Figure 22. Measured in USD millions

Figure 23. Law enforcement helped shorten time to identify and contain ransomware breaches.
Total time to identify and contain a ransomware breach was 11.4% or 33 days shorter with law enforcement involvement, at 273 days in total compared to 306 days. The mean time to contain a ransomware breach was 63 days or 23.8% shorter with law enforcement involvement compared to 80 days without. It's clear that involving law enforcement can help reduce the cost and duration of a ransomware breach.

Time to identify and contain a ransomware attack with law enforcement involvement

Figure 23. Measured in days

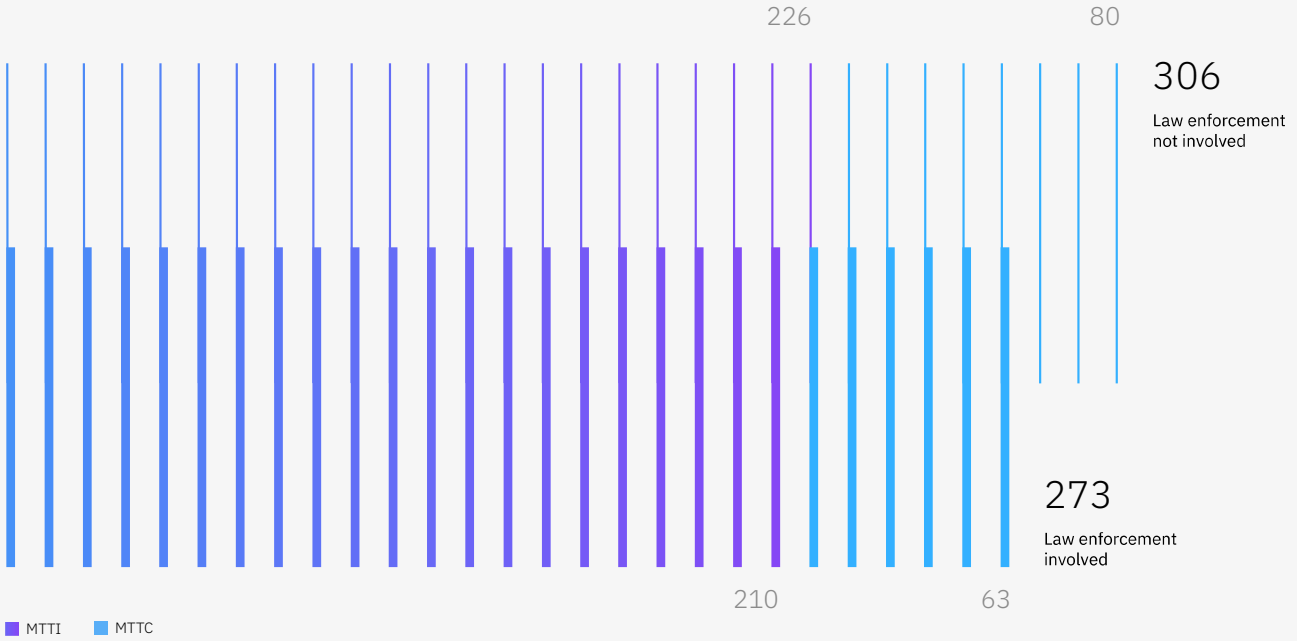


Figure 24. Automated response playbooks or workflows cut down the time to contain a ransomware breach.
Among organizations that experienced a ransomware attack, those that had automated response playbooks or workflows designed specifically for ransomware attacks were able to contain them in 68 days or 16% fewer days compared to the average of 80 days for organizations without automated response playbooks or workflows.

Figure 25. Paying the ransom led to minimal cost savings.
Organizations that paid the ransom during a ransomware attack achieved only a small difference in total cost, at USD 5.06 million compared to USD 5.17 million, a cost difference of USD 110,000 or 2.2%. However, this calculation doesn't include the cost of the ransom itself. Given the high cost of most ransomware demands, organizations that paid the ransom likely ended up spending more overall than those that didn't pay the ransom. In the 2022 report, the total cost savings were USD 630,000, with a total cost difference of 13.1%, again not including the cost of the ransom itself. The data shows that paying a ransom has become increasingly less advantageous overall, with an 82.5% decrease in savings from the 2022 to 2023 reports.

Impact of automated response playbooks or workflows for ransomware on time to contain a ransomware breach

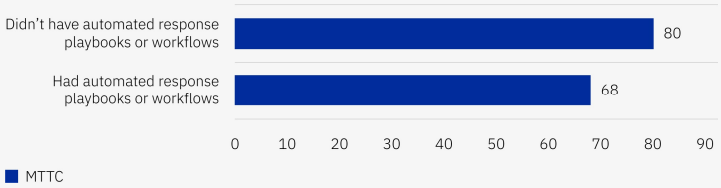


Figure 24. Measured in days

Cost of a ransomware attack based on whether the ransom was paid

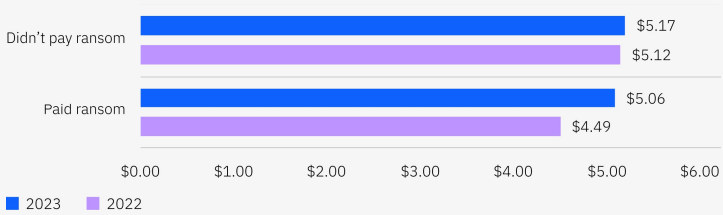


Figure 25. Measured in USD millions (cost of ransom not included)

Business partner supply chain attacks

A business partner supply chain compromise is a data breach that originates with an attack on a business partner. In this year's study, 15% of organizations identified a supply chain compromise as the source of a data breach.

Figures 26 and 27. A business partner supply chain compromise cost 11.8% more and took 12.8% longer to identify and contain than other breach types.
The cost of a data breach due to a business partner supply chain compromise averaged USD 4.76 million, which was USD 530,000 or 11.8% higher than the USD 4.23 million average cost of a data breach that was due to another cause.

Organizations took an average of 233 days to identify and 74 days to contain a business partner supply chain compromise, for a total lifecycle of 307 days. That average lifecycle was 37 days or 12.8% longer than the average lifecycle of 270 days for data breaches attributed to another cause.

Cost of a data breach due to a business partner supply chain compromise

Figure 26. Measured in USD millions

Time to identify and contain a data breach based on occurrence of a business partner supply chain compromise

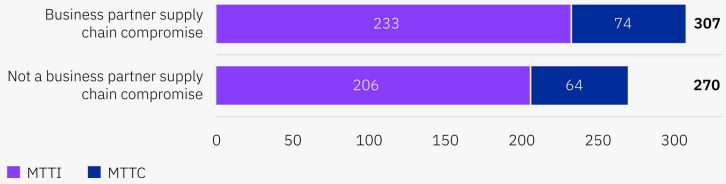
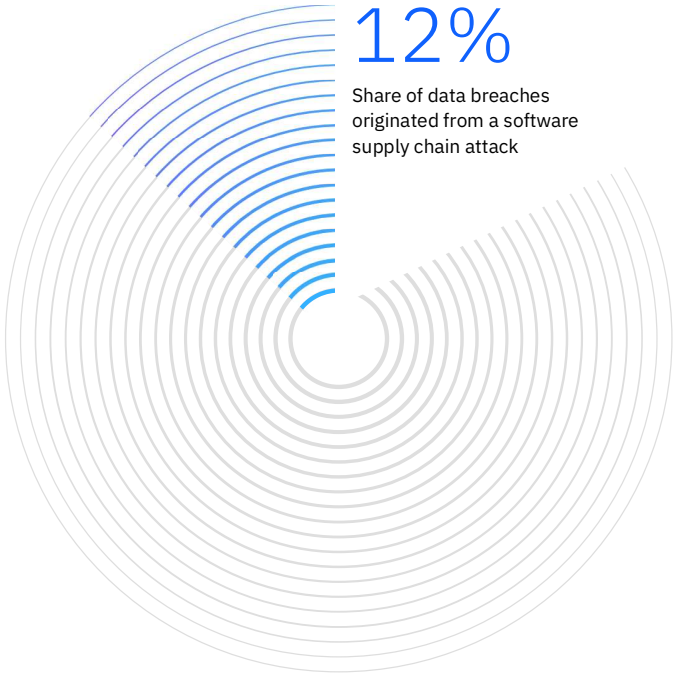


Figure 27. Measured in days

Software supply chain attacks

For the first time this year, the study also examined attacks that originated from a software supply chain attack in which an attacker infiltrates a software vendor's network and deploys malicious code to compromise the software before the vendor sends it to its customers. The compromised software then attacks the customer's data or system. In this year's study, 12% of organizations identified a software supply chain attack as the source of a data breach.



12%

Share of data breaches originated from a software supply chain attack

Figures 28 and 29. Software supply chain compromises cost 8.3% more and took 8.9% longer to identify and contain than other breach types.
The cost of a data breach due to a software supply chain compromise averaged USD 4.63 million, which was USD 370,000 or 8.3% higher than the USD 4.26 million average cost of a data breach that was due to another cause. A breach due to a software supply chain compromise had an 8.9% longer lifecycle, at 294 days compared to 269, than data breaches due to other causes.

Although a supply chain compromise originating from within the software supply chain is less costly than one originating from a business partner, both still cost more and take longer than the average data breach.

Cost of a data breach based on occurrence of a software supply chain compromise

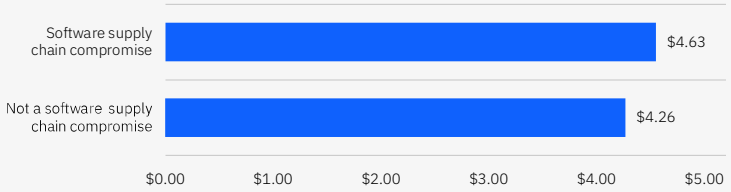


Figure 28. Measured in USD millions

Time to identify and contain a data breach based on occurrence of a software supply chain compromise

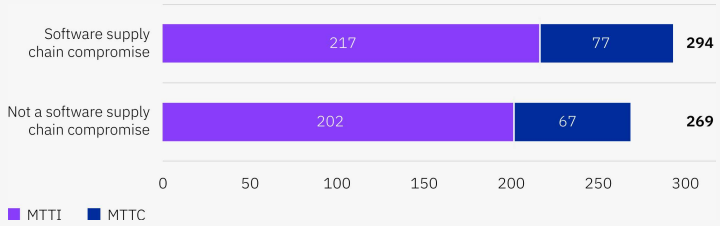


Figure 29. Measured in days

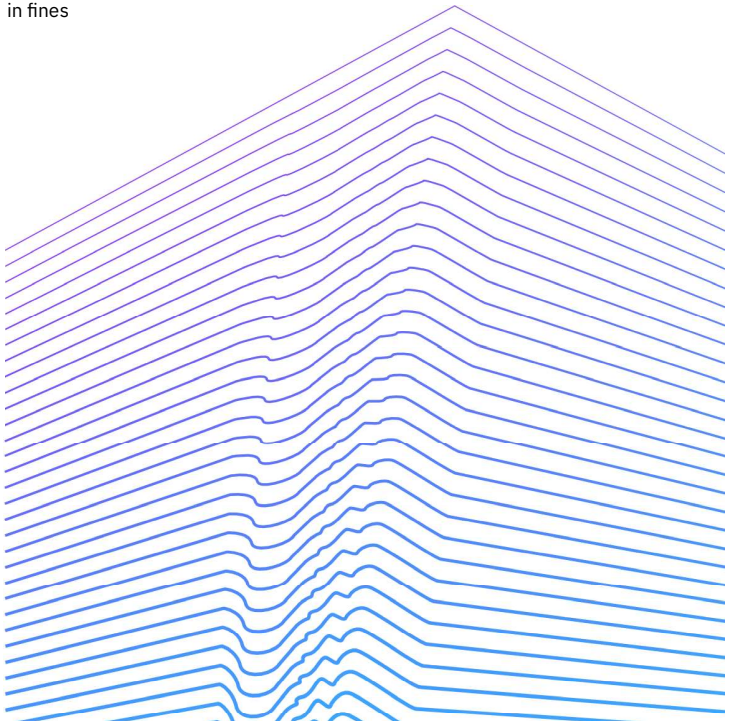
Regulatory environments

The research examined how the degree of data regulation affected the cost of a data breach. In environments with high levels of data regulation, 58% of costs continued to accrue after the first year. In low-regulation environments, 64% of the costs associated with a breach were more likely to be resolved within the first year.

The cost of a data breach tends to change in the time elapsed since the breach. There may be different costs associated with each stage of the breach as it's identified and contained and as the compromised data is recovered or repaired.

USD 250,000

20% of organizations that experienced a data breach paid this much or more in fines



Figures 30a and 30b. Peak costs were incurred more than two years after a data breach was identified in high-data regulation environments.
Organizations in low-regulation environments took on nearly two-thirds of their data breach costs in the first year, whereas organizations in high-regulation environments took on less than half of their data breach costs in the first year. Data breach costs in low-regulation environments peaked at 21% of total costs accrued in the time frame of 6–9 months. Data breach costs in high-regulation environments peaked at 21% of total costs accrued after the two-year mark. The bulk of data breach costs in a low-regulation environment spiked early on and tapered with time. In a high-regulation environment, costs oscillated and continued to rise two years after the breach was identified.

Distribution over time of data breach costs in low-data versus high-data regulation environments

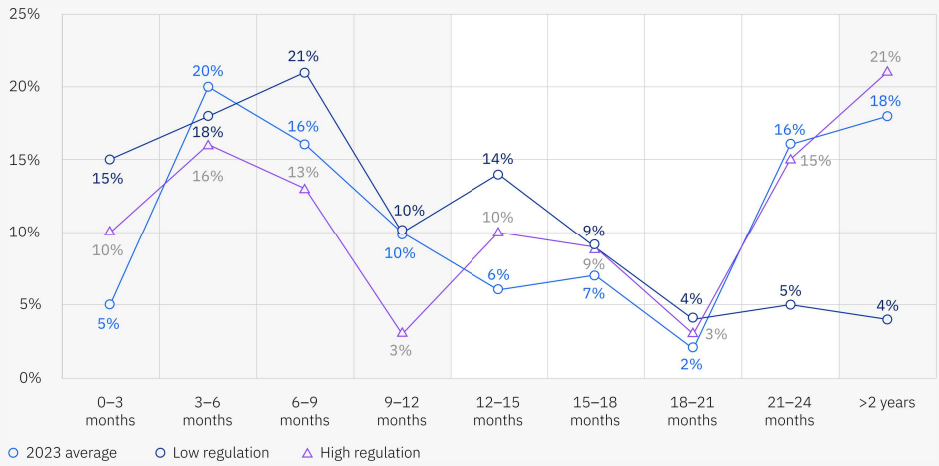


Figure 30a. Percentage of total costs accrued in three-month intervals

Distribution of data breach costs by year in low-data versus high-data regulation environments

Time elapsed since breach	Percentage of total cost		
	2023 average	Low regulation	High regulation
First year	51%	64%	42%
Second year	31%	32%	37%
Two-plus years	18%	4%	21%

Figure 30b. Percentage of total costs over the years

Figure 31. Data breach costs for critical infrastructure industries exceed USD 5 million.
Critical infrastructure organizations included those in the financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector industries. These organizations incurred data breach costs that were USD 1.26 million higher than the average cost of USD 3.78 million for organizations in other industries, a difference of 28.6%. This USD 5.04 million value also reflects a 4.6% increase of USD 4.82 million over the 2022 reported average cost of a data breach for critical infrastructure industries.

Cost of a data breach for critical infrastructure industries versus other industries

Figure 31. Measured in USD millions

Figures 32 and 33. Fewer than one-third of organizations incurred fines due to data breaches, and 80% of fines amounted to USD 250,000 or less.
Of the organizations studied, 31% incurred fines as a result of a data breach, and only 20% of those fines exceeded USD 250,000. A fine of USD 250,000 represented 5.6% of the average total cost of a data breach in the 2023 report.

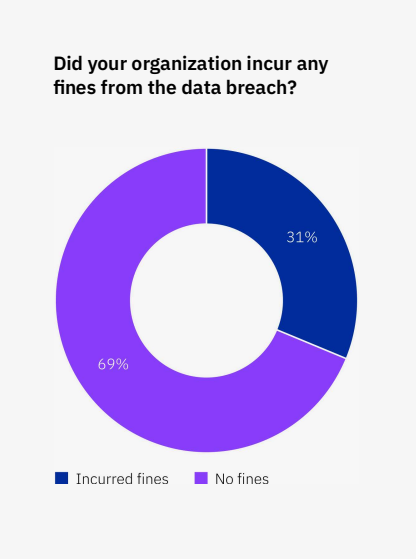


Figure 32. Share of all organizations

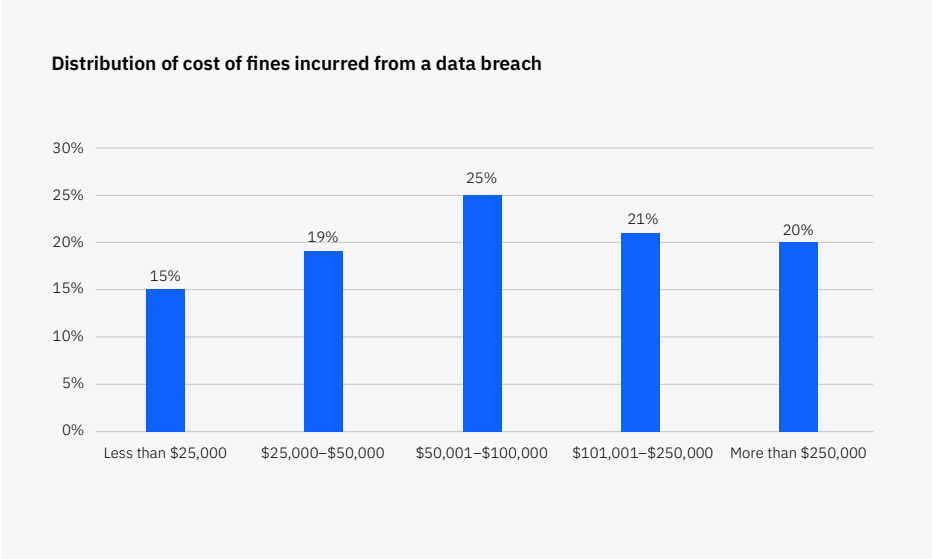
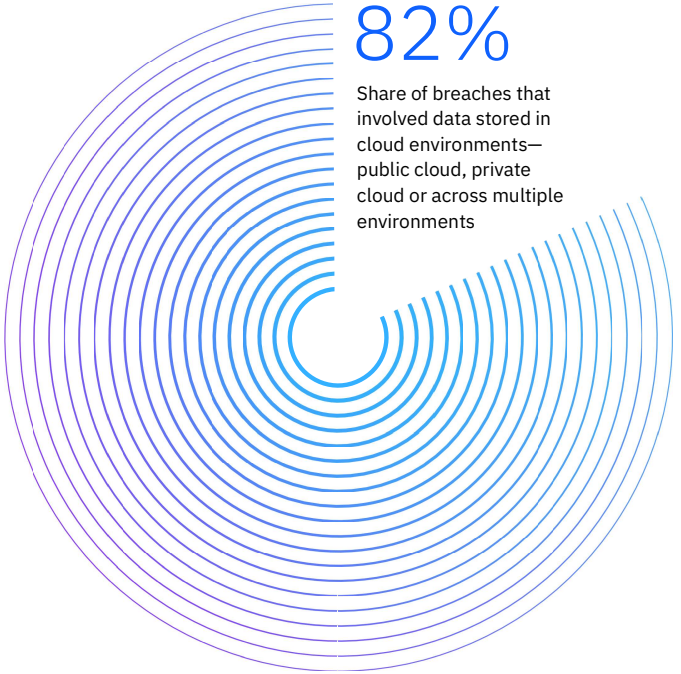


Figure 33. Among those that experienced fines, as measured in USD

Cloud breaches

The cost and duration of a breach varied depending on where the data was stored. Most commonly, the breaches studied included data that spanned multiple environments—including cloud and on premises—and breaches of this type also contributed to higher costs and longer time to identify and contain a data breach.



82%

Share of breaches that involved data stored in cloud environments—public cloud, private cloud or across multiple environments

Figure 34. Breaches most commonly impacted data stored across multiple environments.
The largest percentage of breaches, 39%, involved data stored across multiple environments, followed by 27% of breaches that involved data stored in the public cloud. The number of breaches occurring across multiple environments surpassed the combined 34% of breaches occurring only in private cloud or on-premises environments.

Figure 35. Data breaches in public clouds and multiple environments had higher costs.
In the 2023 report, the cost of data breaches across multiple environments reached USD 4.75 million, the highest cost of the environments analyzed, and 17.6% higher than the USD 3.98 million cost of data breaches in a private cloud environment, which was the lowest cost of the environments analyzed. The cost of data breaches across multiple environments also exceeded the average cost of a data breach of USD 4.45 million by a margin of 6.5%.

Where was the breached data stored?

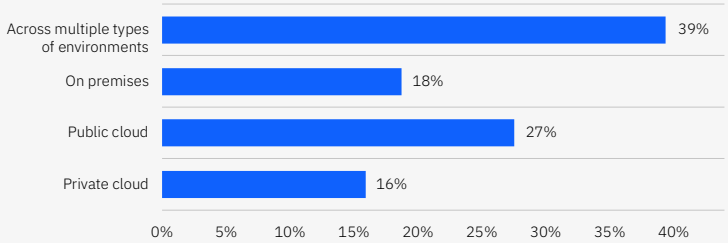


Figure 34. Share of all breaches

Cost of a data breach by storage location of breached data

Figure 35. Measured in USD millions

Figure 36. The use of public clouds and multiple environments also contributes to longer data breach lifecycles.
The longest time to identify and contain a breach involved data stored across multiple environments, taking 291 days. This interval exceeded the shortest time to identify and contain a breach—which was 235 days in a private cloud environment—by 56 days or 21.3%. It's also worth noting that the use of multiple environments is the only model that exceeds the 2023 reported average time to identify and contain a data breach of 277 days by a margin of 14 days or 4.9%.

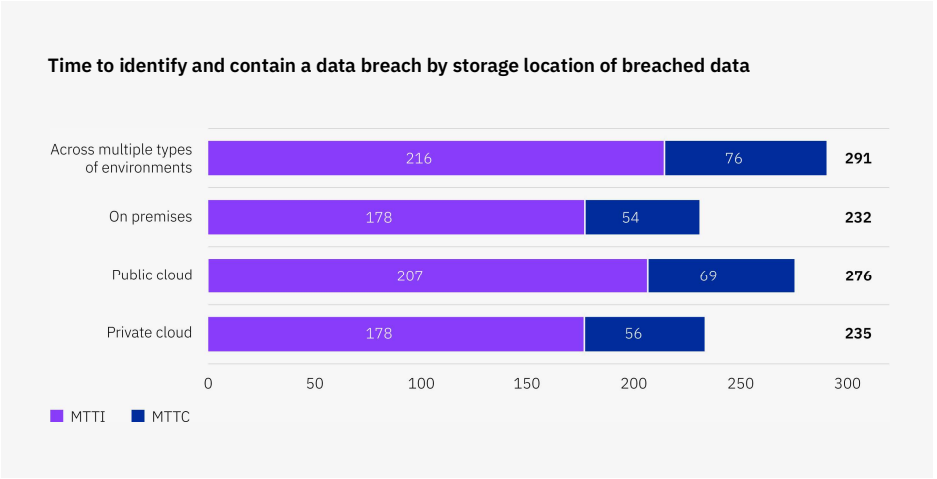
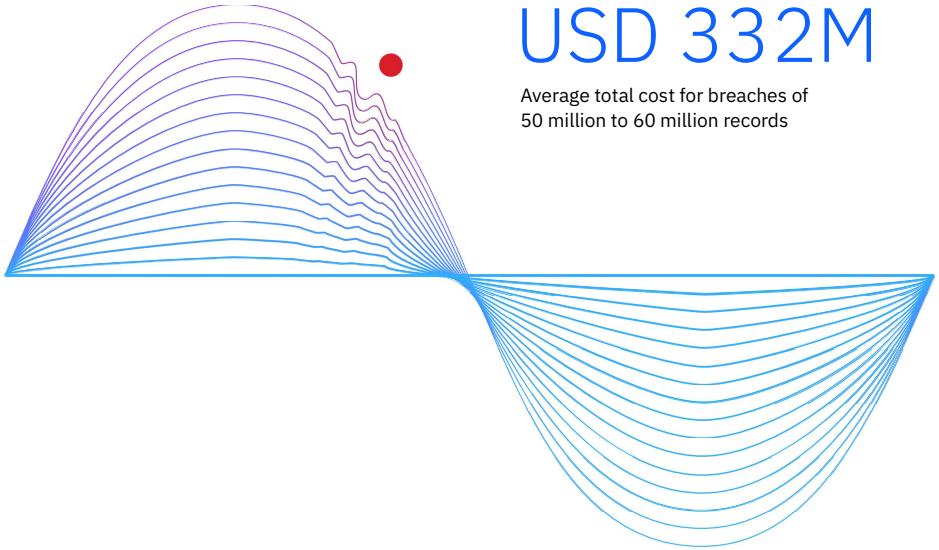


Figure 36. Measured in days

Mega breaches

Mega breaches, characterized by more than one million compromised records, are relatively rare. But they exert a powerful impact due to their outsized scope.

This year's study included 20 organizations that endured the loss or theft of between 1 million and 60 million records due to data breaches. The study deployed a distinct methodology to examine those mega breaches. They were considered separately from the study's other 553 breaches, each including no more than 101,200 lost or compromised records. For a full explanation of the research methodology, see the data breach FAQs at the end of this report.



USD 332M

Average total cost for breaches of 50 million to 60 million records

Figure 37. The cost of mega breaches fell in the 2023 report.
Across all breach size cohorts, the average cost of a mega breach fell to varying degrees. The highest percentage decrease occurred in the 1 million to 10 million cohort, with a 26.5% decrease from USD 49 million in the 2022 report to USD 36 million in the 2023 report. The smallest percentage decrease occurred in the 30 million to 40 million cohort, with a 3.8% decrease from USD 316 million in the 2022 report to USD 304 million in the 2023 report. In the 50 million to 60 million cohort, the 2022 reported cost of USD 387 million decreased by USD 55 million or 14.2% to equal USD 332 million in the 2023 report.

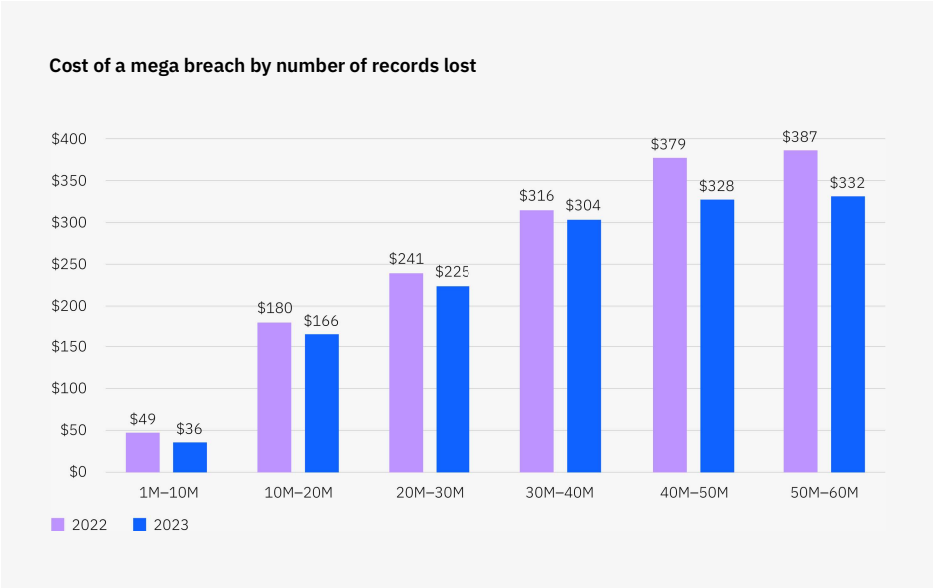


Figure 37. Measured in USD millions

Security investments

This section examines the security investment strategies that organizations adopted after experiencing a data breach. We'll explore how often organizations increased spending after a breach as well as how they chose to allocate funds.

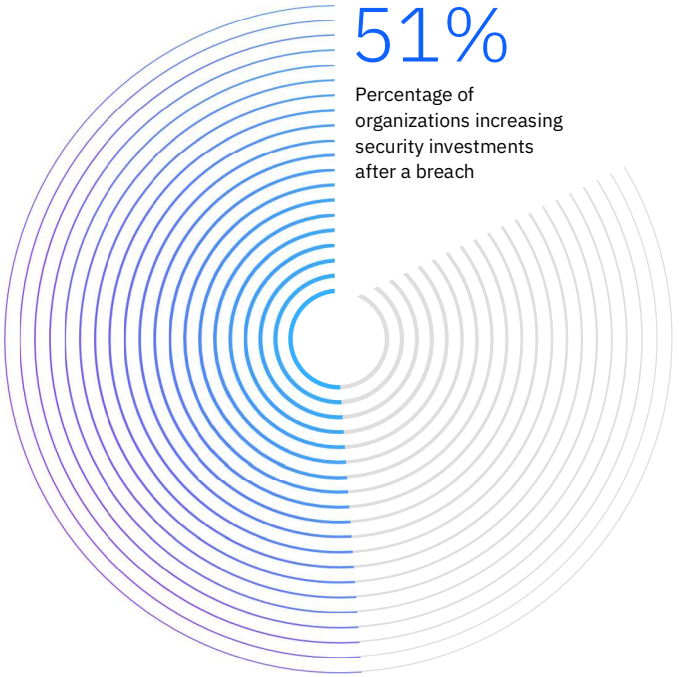


Figure 38. Respondents were split on increasing security investment after a breach.
Even as the global cost of a data breach increased, research participants reported divided perspectives on increasing security investments after an incident. 51% of respondents indicated they planned for additional security spending after the breach.

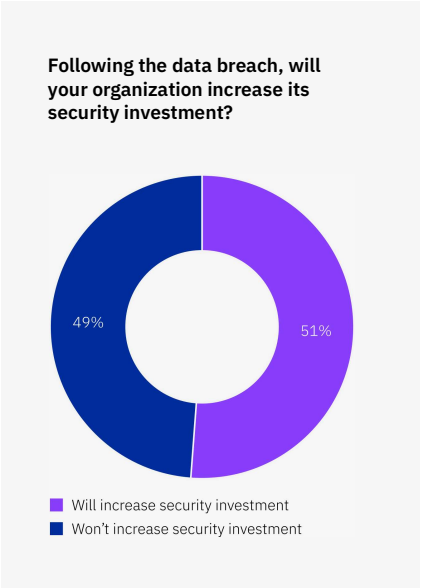


Figure 38. Percentage of all organizations

Figure 39. IR planning and testing and employee training saw significant post-breach investment.
Of the 51% that increased spending after a breach, organizations' most common investment was in IR planning and testing at 50%, followed closely by employee training at 46%. Threat detection and response technologies placed third at 38%, making them the top-ranked technology or tool investment considered in this section. Notably, these three investments map closely to top factors associated with lower data breach costs that are explored in this year's key cost factors section. At only 18% of respondents, insurance protection was the least common investment after a breach.

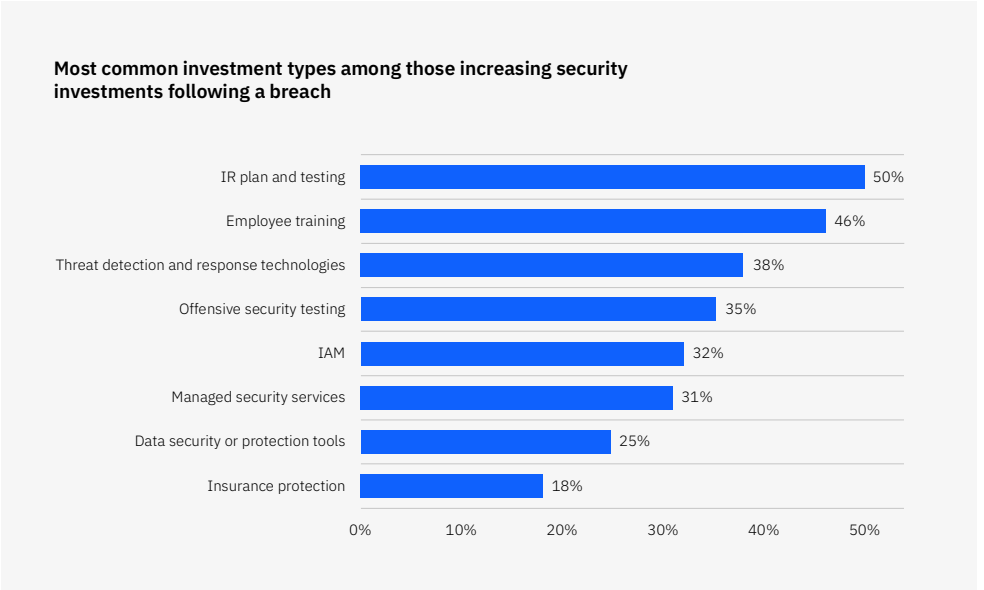


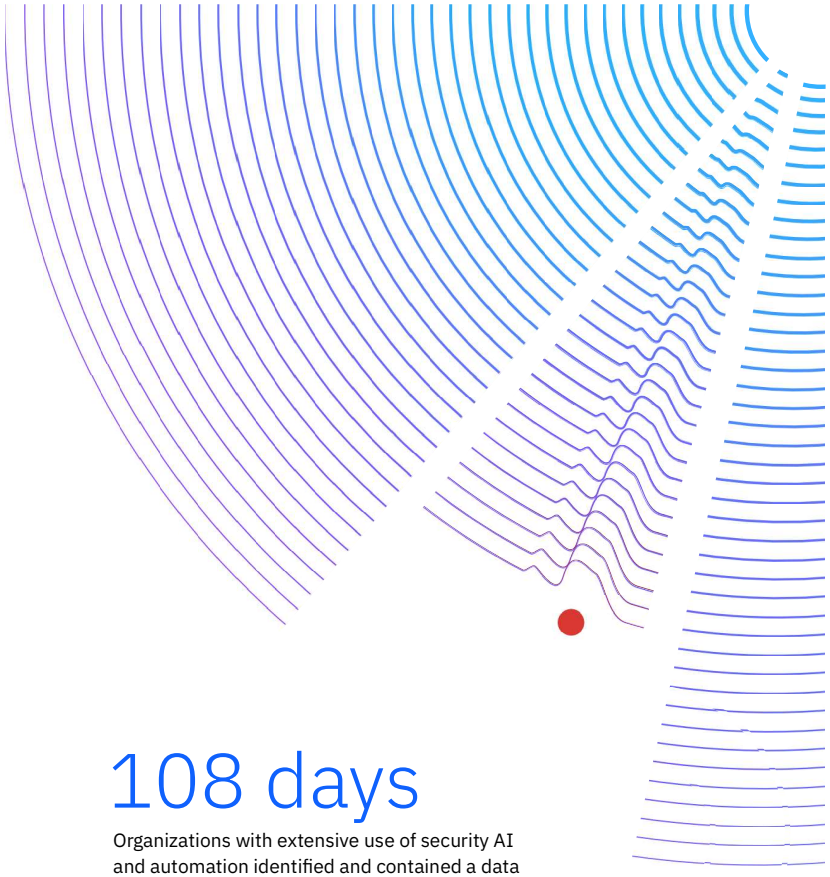
Figure 39. Share among organizations that are increasing investment; more than one response permitted

Security AI and automation

With security AI and automation use cases for the security industry advancing, this report examines the impact of these technologies on data breach costs and timelines. Examples include the use of AI, machine learning, automation and orchestration to augment or replace human intervention in detection and investigation of threats as well as the response and containment process. On the opposite end of the spectrum are processes driven by manual inputs, often across dozens of tools and complex, nonintegrated systems, without data shared between them.

Though this is the sixth year of investigating the impact of AI and automation on cybersecurity, this year we're introducing new criteria that considered AI's permeation throughout an organization's security processes as opposed to its level of deployment—ranging from not deployed to partially or fully deployed—in prior years' data.

- "Extensive use" refers to the integration of security AI and automation throughout operations, including several different tool sets and capabilities.
- "Limited use" refers to applying AI to just one or two use cases within security operations.
- "No use" refers to security processes that are driven solely by manual inputs.



108 days

Organizations with extensive use of security AI and automation identified and contained a data breach 108 days faster than organizations with no use.

Figure 40. A 61% majority of organizations employ some level of security AI and automation.
Only 28% of organizations extensively used security AI and automation tools in their cybersecurity processes, while 33% had limited use. That leaves nearly 4 in 10 relying solely on manual inputs in their security operations.

Figure 41. Extensive security AI and automation use delivered cost savings of nearly USD 1.8 million.
Organizations with extensive use of security AI and automation demonstrated the highest cost savings comparatively, with an average cost of a data breach at USD 3.60 million, which was USD 1.76 million less and a 39.3% difference compared to no use. Even organizations with limited use of security AI and automation measured an average cost of a data breach of USD 4.04 million, which was USD 1.32 million less or a 28.1% difference compared to no use. However, organizations with no use of security AI and automation experienced an average cost of a data breach of USD 5.36 million. This is 18.6% more than the 2023 average cost of a data breach of USD 4.45 million.

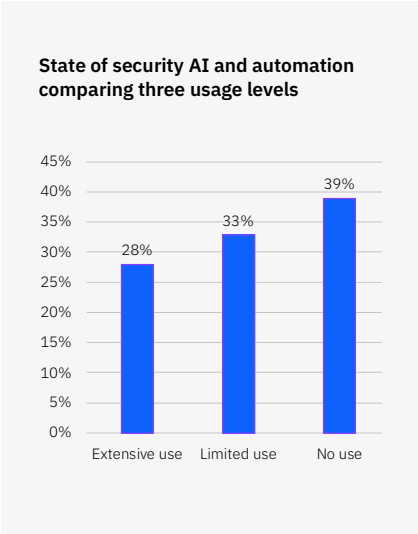


Figure 40. Percentage of organizations per usage level

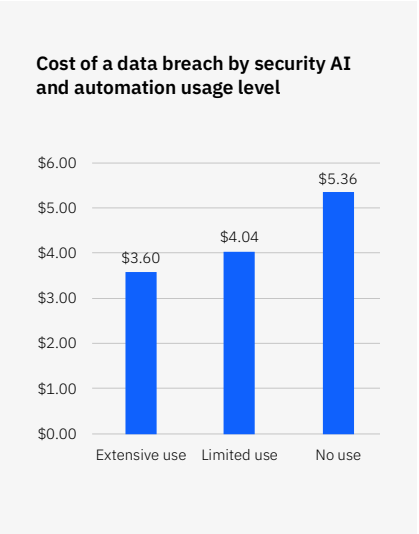


Figure 41. Measured in USD millions

Figure 42. Extensive security AI and automation reduced the time to identify and contain a breach by more than 100 days.
Respondents from organizations that extensively used security AI and automation were able to identify and contain a breach in 214 days, which was 108 days shorter than those with no use. This means identifying and containing a breach with extensive use of security AI and automation took just 66% of the time it took organizations with no use. Limited use also made a significant impact, with an average time to identify and contain a breach in 234 days, which was 88 days shorter than organizations with no use. It's clear that even a limited effort to integrate security AI and automation into security workflows can offer a significant acceleration in the time to identify and contain a breach as well as a sizable reduction in costs.

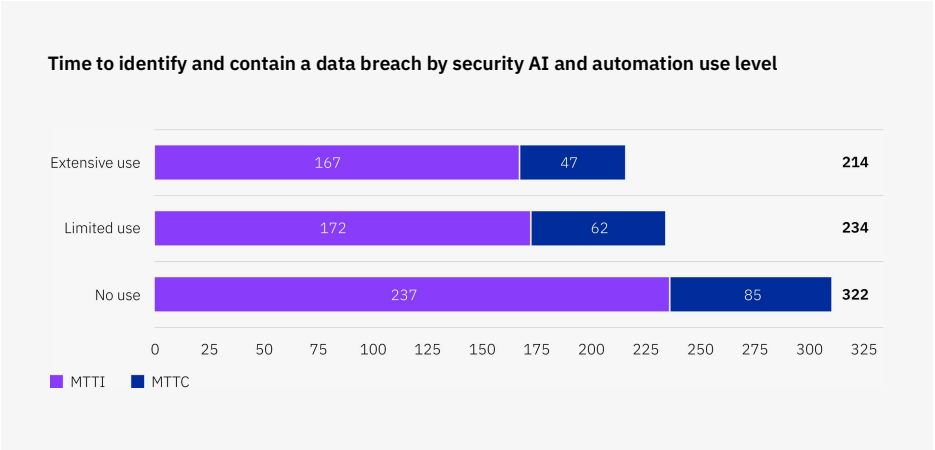
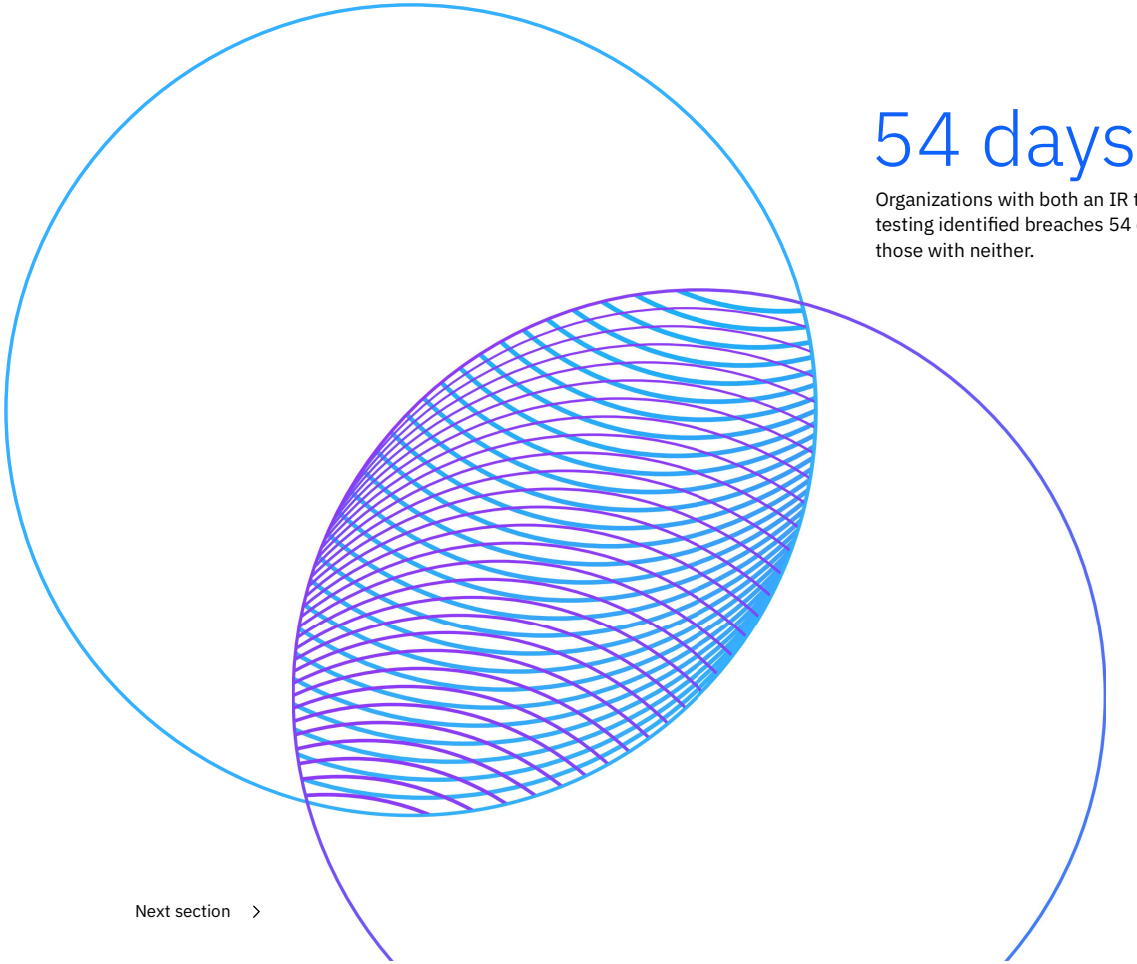


Figure 42. Measured in days

Incident response

IR strategies and tactics have been instrumental in reducing the impact of data breaches. The most effective IR strategy for reducing the duration of a data breach was to combine formation of an IR team with testing of the IR plan. However, some organizations pursued only one of those two strategies. As a standalone effort, IR plan testing was more effective than only forming an IR team in reducing the total time to identify and contain the breach.



54 days

Organizations with both an IR team and IR plan testing identified breaches 54 days faster than those with neither.

Figure 43. The combined IR strategy saved 54 days in identifying and containing a breach.
The dual strategy of forming an IR team and testing an IR plan demonstrated a shorter time, 252 days, to identify and contain a data breach compared to 306 days of employing neither approach, a difference of 54 days or 19.4%. Testing the IR plan without forming a team was nearly as effective, resulting in a difference of 48 days or 17%.

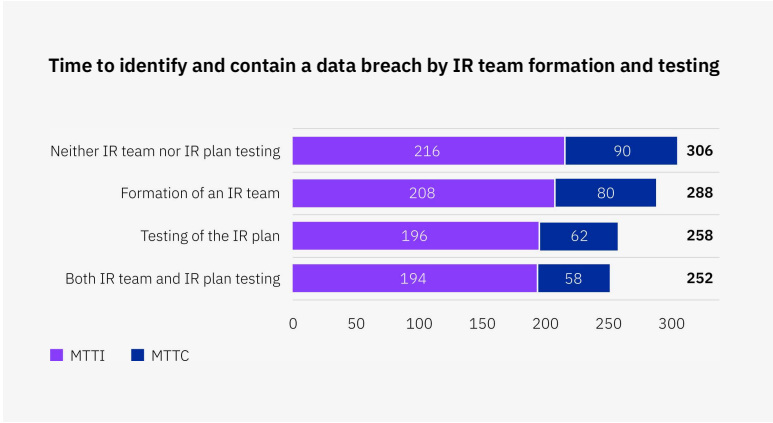
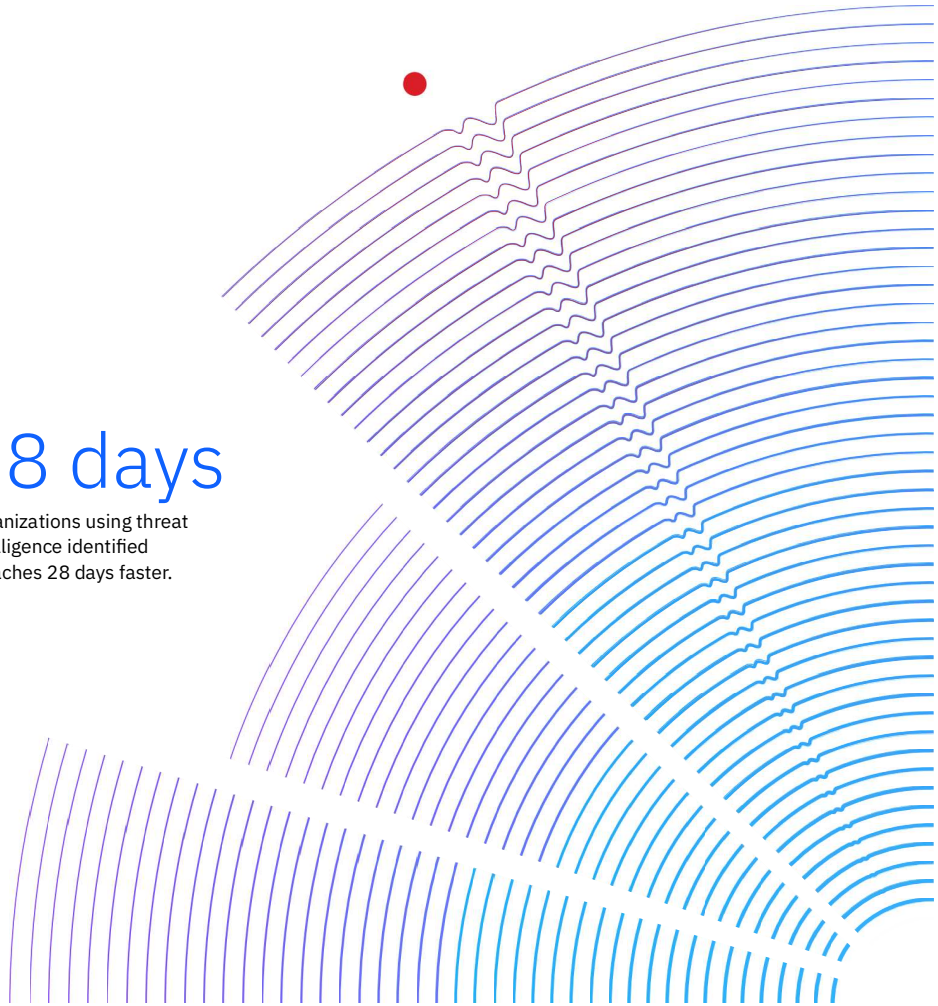


Figure 43. Measured in days

Threat intelligence

New to the report this year is the impact of threat intelligence services on the mean time to identify a breach. Threat intelligence services provide security leaders with information and insights about cyberthreats and vulnerabilities to help them improve their organization's security posture.



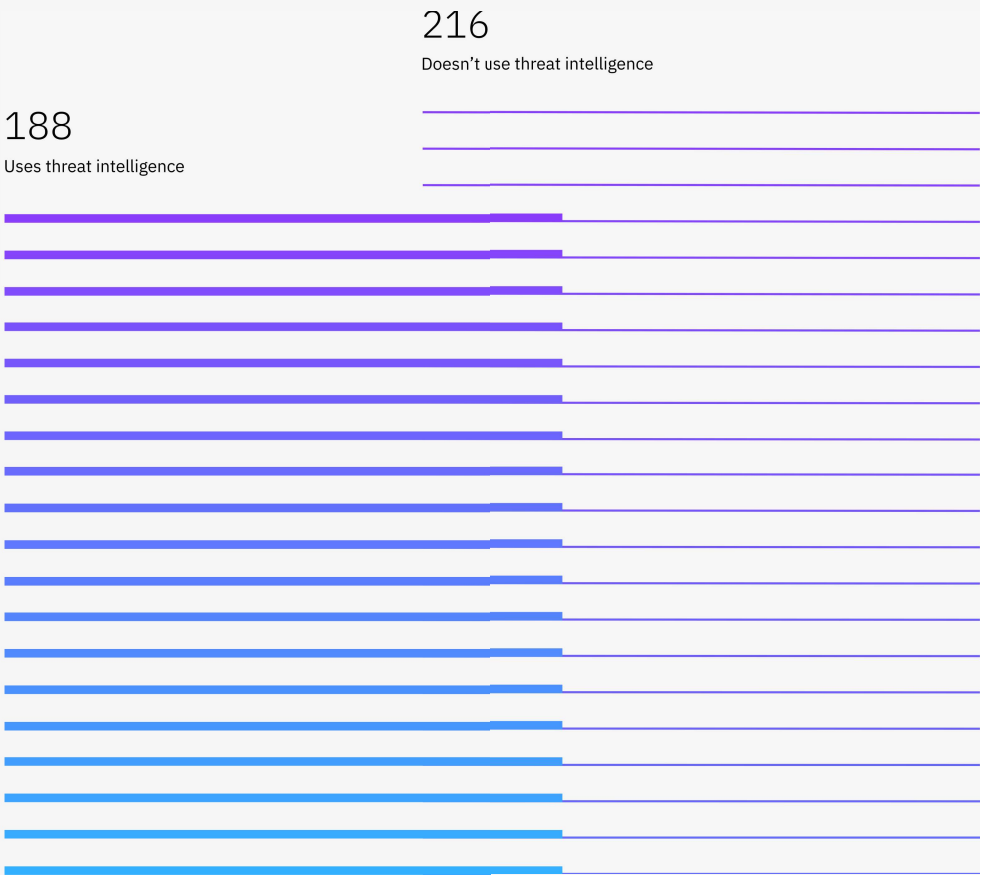
28 days

Organizations using threat intelligence identified breaches 28 days faster.

Figure 44. Threat intelligence reduced breach identification time.
This year's research showed that threat intelligence users uncovered breaches in 13.9% less time than those without a threat intelligence investment, a difference of 28 days. Compared to this year's global MTTI of 204 days, organizations employing threat intelligence services were able to identify breaches in 8.2% or 16 days less time. Respondents that did not use threat intelligence took 5.7% or 12 days longer than the global average to identify breaches.

Time to identify a data breach using threat intelligence

Figure 44. MTTI measured in days

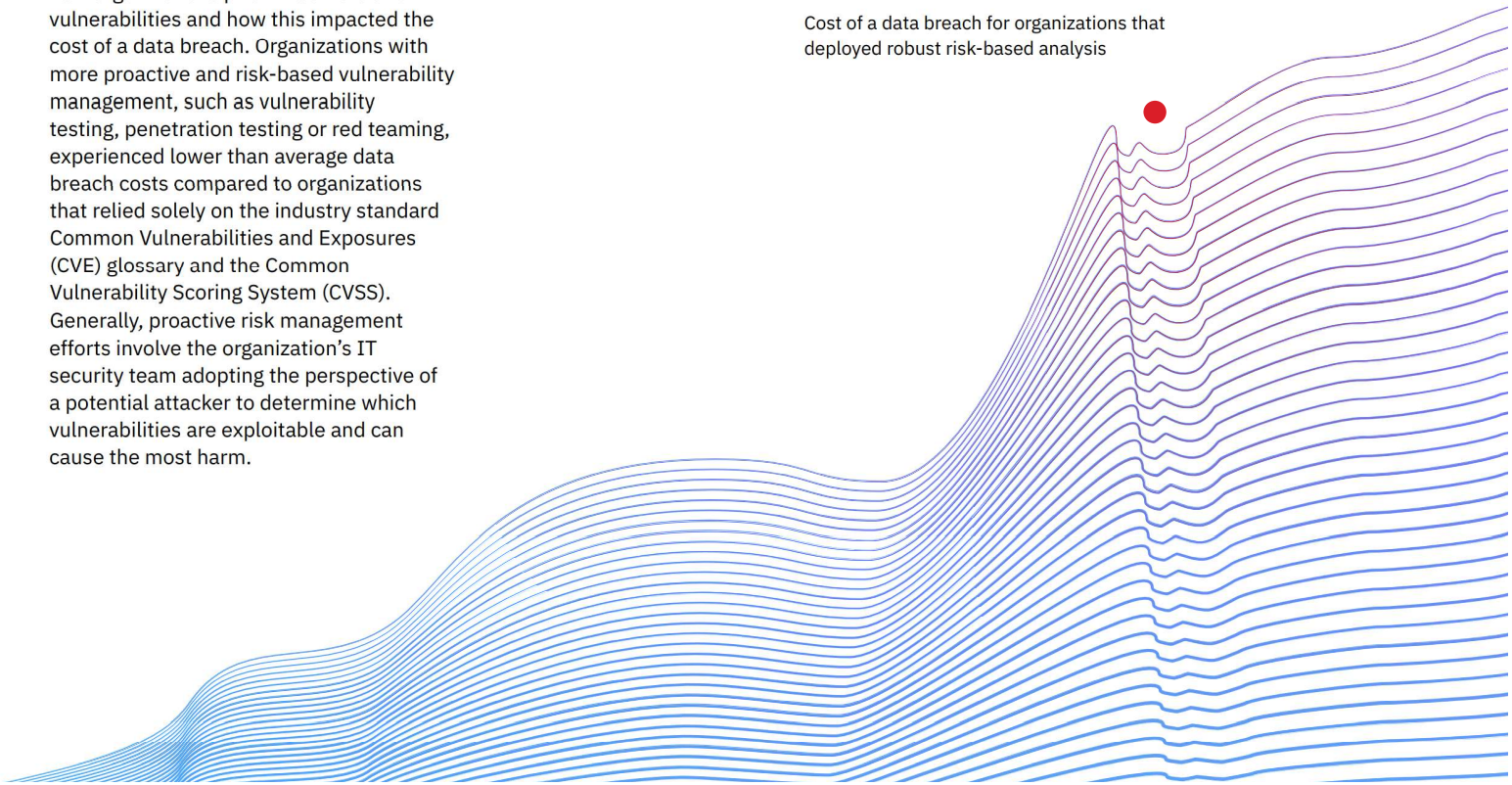


Vulnerability and risk management

New this year, the research examined how organizations prioritized risks and vulnerabilities and how this impacted the cost of a data breach. Organizations with more proactive and risk-based vulnerability management, such as vulnerability testing, penetration testing or red teaming, experienced lower than average data breach costs compared to organizations that relied solely on the industry standard Common Vulnerabilities and Exposures (CVE) glossary and the Common Vulnerability Scoring System (CVSS). Generally, proactive risk management efforts involve the organization's IT security team adopting the perspective of a potential attacker to determine which vulnerabilities are exploitable and can cause the most harm.

USD 3.98M

Cost of a data breach for organizations that deployed robust risk-based analysis



Figures 45 and 46. Organizations that prioritize activities beyond CVE score experienced less costly breaches.
More than one-third of organizations or 36% relied solely on CVE scoring to prioritize vulnerabilities, while the majority of organizations or 64% used more involved risk-based analysis. The 2023 research showed a significant difference in the cost of data breaches between these two groups. Organizations that deployed more intensive, risk-based analysis experienced an average cost of a data breach of USD 3.98 million, a difference of 18.3%, compared to USD 4.78 million for organizations that relied on CVE scores only.

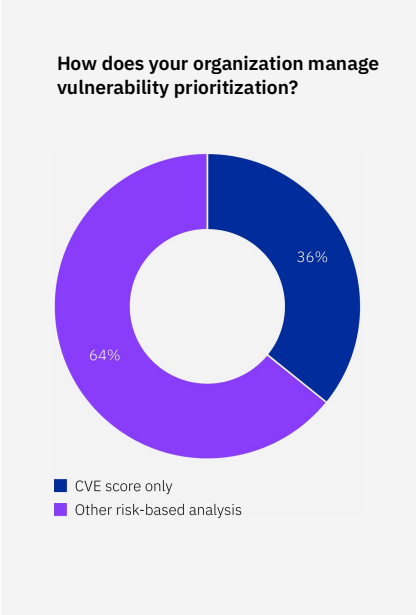


Figure 45. Percentage of all organizations

Figure 46. Measured in USD millions

Attack surface management

ASM is a set of processes that aids in the discovery, analysis, remediation and monitoring of an organization's potential attack surfaces or vulnerabilities. Organizations that deployed an ASM solution were able to identify and contain data breaches in 75% of the time of those without an ASM solution.

Figure 47. ASM helped accelerate total time to identify and contain a data breach by nearly 12 weeks.
Without an ASM solution, organizations took 260 days to identify a data breach and another 77 days to contain it, for a total of 337 days or about 11 months. Organizations with an ASM solution identified the breach in 193 days and contained it in 61 days. The 254-day total time to identify and contain a breach represented an acceleration of 83 days or about 12 weeks so the data breaches were identified and contained in 75% of the time taken by data breaches at organizations without ASM solutions.

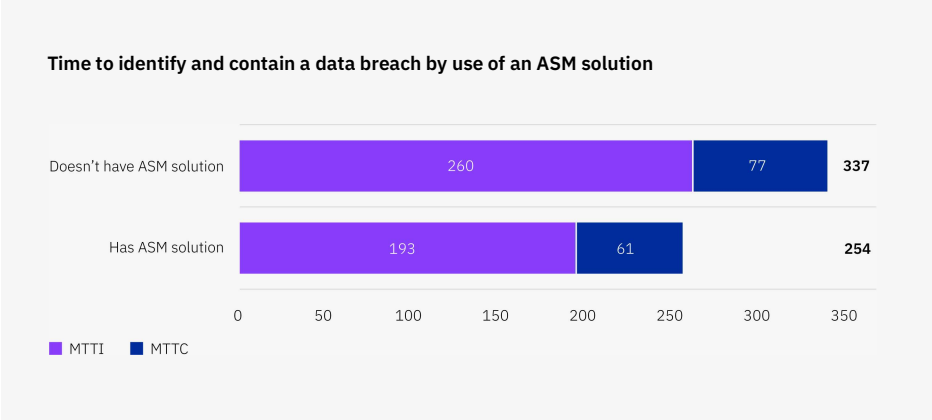


Figure 47. Measured in days

Managed security service providers

For the first time, our research explored the impact that partnering with an MSSP had on the time to identify and contain a breach. MSSPs offer organizations the ability to outsource security monitoring and management, often using high-availability security operations centers to provide around-the-clock services. MSSPs can help organizations enhance their security posture without increasing head count or investing in training for internal resources.

Figure 48. Organizations with MSSPs experienced a 21% shorter breach lifecycle.
In the 2023 report, organizations that had an MSSP were able to identify and contain breaches in 80% of the time of those without. Organizations that worked with an MSSP identified breaches 16 days faster or an 8.2% shorter identification time than the 2023 reported global average of 204 days. Those that didn't took 28 days longer or 12.8% longer. Containment times with no MSSP were five days longer or 6.6% longer than the 2023 reported global average of 73 days. Containment times with MSSP assistance were 10 days faster or 14.7% faster.

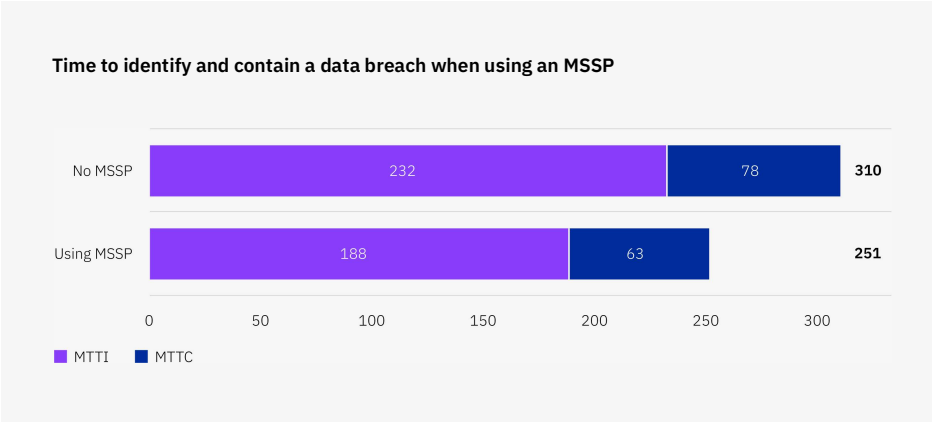
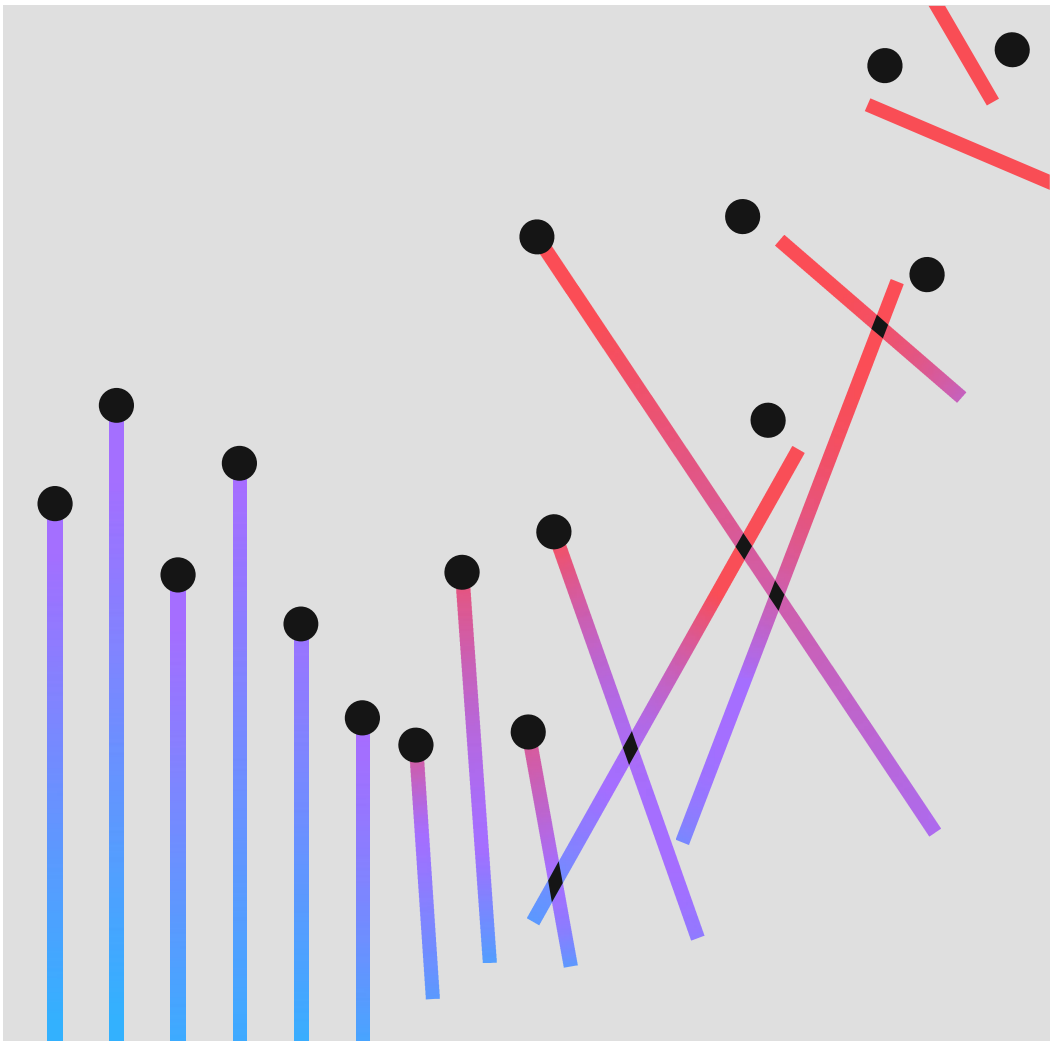


Figure 48. Measured in days

IBM **Security**

Cost of a Data Breach Report 2022



IBM

Significantly, for the first time, the research shows the following insights:

83%

of organizations studied have had more than one data breach.

60%

of organizations' breaches led to increases in prices passed on to customers.

79%

of critical infrastructure organizations didn't deploy a zero trust architecture.

19%

of breaches occurred because of a compromise at a business partner.

45%

of the breaches were cloud-based.

What's new in the 2022 report

With each year's edition, we aim to build upon past research to keep up with changing technology and events. We also try to form a more relevant picture of the risks and strategies for securing data and responding to a breach, from artificial intelligence (AI) to zero trust. Covering some of the technologies most companies focused on in the past year, the 2022 edition of this report has new analysis related to the value of the following:

- Extended detection and response (XDR)
- The use of risk quantification techniques
- Impacts of individual technologies that contribute to a zero trust security framework, such as identity and access management (IAM) and multifactor authentication (MFA)

Furthermore, the report takes a broader look at some leading contributors to higher data breach costs. For the first time, the report looks at the effects of supply chain compromises and the security skills gap.

The report examines areas of security vulnerability from the cloud to critical infrastructure. And we take a deeper dive than past years into the impacts of ransomware and destructive attacks. Also studied is the phenomenon of remote work that continues to be a reality for many organizations past the peak of the COVID pandemic.

As companies experience more breaches and costs continue to climb, this report can serve as a tool to help your teams better manage risk and limit potential losses.
The report is divided into the following five major sections:

- The executive summary with key findings and what's new in the 2022 edition
- In-depth analysis on the complete findings, including breach costs by geographic region and industry
- Security recommendations from IBM Security experts based on this report's results
- Demographics of organizations and industry definitions
- The study's methodology, including how costs were calculated

IBM Security and Ponemon Institute are pleased to present the results of the 2022 Cost of a Data Breach Report.

Key findings

The key findings described here are based on IBM Security analysis of research data compiled by Ponemon Institute.[1]

USD 4.35 million

Average total cost of a data breach

Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in the 2020 report.

83%

Percentage of organizations that have had more than one breach

Eighty-three percent of organizations studied have experienced more than one data breach, and just 17% said this was their first data breach. Sixty percent of organizations studied stated that they increased the price of their services or products because of the data breach.

USD 4.82 million

Average cost of a critical infrastructure data breach

The average cost of a data breach for critical infrastructure organizations studied was USD 4.82 million — USD 1 million more than the average cost for organizations in other industries. Critical infrastructure organizations included those in the financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector industries. Twenty-eight percent experienced a destructive or ransomware attack, while 17% experienced a breach because of a business partner being compromised.

USD 3.05 million

Average cost savings associated with fully deployed security AI and automation

Breaches at organizations with fully deployed security AI and automation cost USD 3.05 million less than breaches at organizations with no security AI and automation deployed. This 65.2% difference in average breach cost — between USD 3.15 million for fully deployed versus USD 6.20 million for not deployed — represented the largest cost savings in the study. Companies with fully deployed security AI and automation also experienced on average a 74-day shorter time to identify and contain the breach, known as the breach lifecycle, than those without security AI and automation — 249 days versus 323 days. The use of security AI and automation jumped by nearly one-fifth in two years, from 59% in 2020 to 70% in 2022.

1. Cost amounts in this report are measured in US dollars (USD).

USD 4.54 million

Average cost of a ransomware attack, not including the cost of the ransom itself

Eleven percent of breaches in the study were ransomware attacks, an increase from 2021, when 7.8% of breaches were ransomware, for a growth rate of 41%. The average cost of a ransomware attack went down slightly, from USD 4.62 million in 2021 to USD 4.54 million in 2022. This cost was slightly higher than the overall average total cost of a data breach, USD 4.35 million.

19%

Frequency of breaches caused by stolen or compromised credentials

Use of stolen or compromised credentials remains the most common cause of a data breach. Stolen or compromised credentials were the primary attack vector in 19% of breaches in the 2022 study and also the top attack vector in the 2021 study, having caused 20% of breaches. Breaches caused by stolen or compromised credentials had an average cost of USD 4.50 million. These breaches had the longest lifecycle — 243 days to identify the breach, and another 84 days to contain the breach. Phishing was the second most common cause of a breach at 16% and also the costliest, averaging USD 4.91 million in breach costs.

59%

Percentage of organizations that don't deploy zero trust

Just 41% of organizations in the study said they deploy a zero trust security architecture. The other 59% percent of organizations that don't deploy zero trust incur an average of USD 1 million in greater breach costs compared to those that do deploy. Among critical infrastructure organizations, an even higher percentage of 79% doesn't deploy zero trust. These organizations experienced on average USD 5.40 million in breach costs, more than USD 1 million higher than the global average.

USD 1 million

Average difference in cost where remote work was a factor in causing the breach versus when it wasn't a factor

When remote working was a factor in causing the breach, costs were an average of nearly USD 1 million greater than in breaches where remote working wasn't a factor — USD 4.99 million versus USD 4.02 million. Remote work-related breaches cost on average about USD 600,000 more compared to the global average.

45%

Share of breaches that occurred in the cloud

Forty-five percent of breaches in the study occurred in the cloud. Yet breaches that happened in a hybrid cloud environment cost an average of USD 3.80 million, compared to USD 4.24 million for breaches in private clouds and USD 5.02 million for breaches in public clouds. The cost difference was 27.6% between hybrid cloud breaches and public cloud breaches. Organizations with a hybrid cloud model also had shorter breach lifecycles than organizations that solely adopted a public or private cloud model.

USD 2.66 million

Average cost savings associated with an incident response (IR) team and regularly tested IR plan

Nearly three-quarters of organizations in the study said they had an IR plan, while 63% of those organizations said they regularly tested the plan. Having an IR team and an IR plan that was regularly tested led to significant cost savings. Businesses with an IR team that tested its IR plan saw an average of USD 2.66 million lower breach costs than organizations without an IR team and that don't test an IR plan. The difference of USD 3.26 million versus USD 5.92 million represents a 58% cost savings.

29 days

Savings in response time for those with extended detection and response (XDR) technologies

XDR technologies were implemented by 44% of organizations. Those organizations with XDR technologies saw considerable advantages in response times. Those organizations with XDR deployed shortened the breach lifecycle by about a month, on average, compared to organizations that didn't implement XDR. Specifically, organizations took 275 days to identify and contain a breach with XDR deployed versus 304 days without XDR deployed. This figure represents a 10% difference in response times.

12 years

Consecutive years the healthcare industry had the highest average cost of a breach

Healthcare breach costs hit a new record high. The average breach in healthcare increased by nearly USD 1 million to reach USD 10.10 million. Healthcare breach costs have been the most expensive industry for 12 years running, increasing by 41.6% since the 2020 report. Financial organizations had the second highest costs — averaging USD 5.97 million — followed by pharmaceuticals at USD 5.01 million, technology at USD 4.97 million and energy at USD 4.72 million.

USD 9.44 million

Average cost of a breach in the United States, the highest of any country

The top five countries and regions for the highest average cost of a data breach were the United States at USD 9.44 million, the Middle East at USD 7.46 million, Canada at USD 5.64 million, the United Kingdom at USD 5.05 million and Germany at USD 4.85 million. The United States has led the list for 12 years in a row. Meanwhile, the country with the fastest growth rate over last year was Brazil, a 27.8% increase from USD 1.08 million to USD 1.38 million.

USD 4.35 million

Global average total cost of a data breach

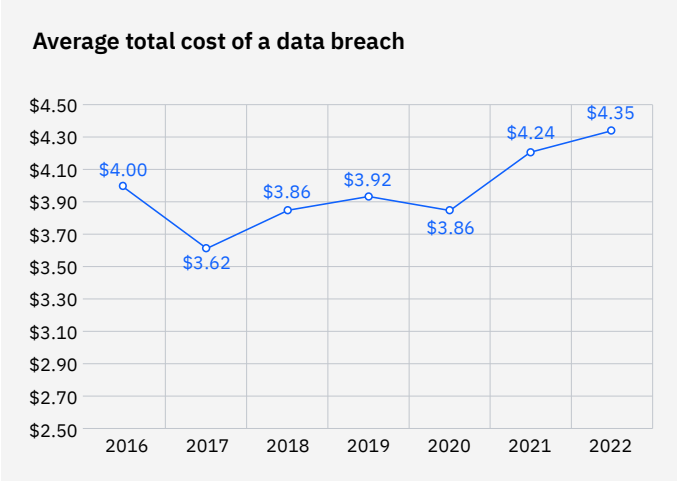


Figure 1: Measured in USD millions

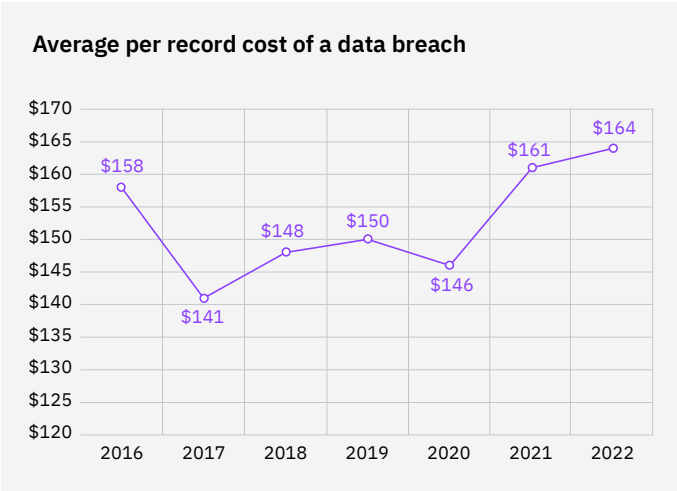


Figure 2: Measured in USD

Global highlights

The Cost of a Data Breach Report is a global report, comprising data from 17 countries and regions and 17 industries. In this section, we look at several key metrics at the level of global average, as well as comparative costs between countries and between industries.

Figure 1: The average cost of a data breach reached a record high in 2022.
The global average total cost of a data breach increased by USD 0.11 million to USD 4.35 million in 2022, the highest it's been in the history of this report. The increase from USD 4.24 million in the 2021 report to USD 4.35 million in the 2022 report represents a 2.6% increase. In the last two years, the average total cost has increased 12.7% from USD 3.86 million in the 2020 report.

Figure 2: The per record cost of a data breach hit a seven-year high.
The global per record cost of a data breach in 2022 was USD 164, a 1.9% increase from USD 161 in 2021. The increase from USD 146 in 2020 is an increase of 12.3%. This study examines breaches sized between 2,200 and 102,000 records. It's not consistent with this research to use the per record cost to calculate the cost of single or multiple breaches above 102,000 records. For more information, see the "Research methodology" section.

Average cost of a data breach by country or region

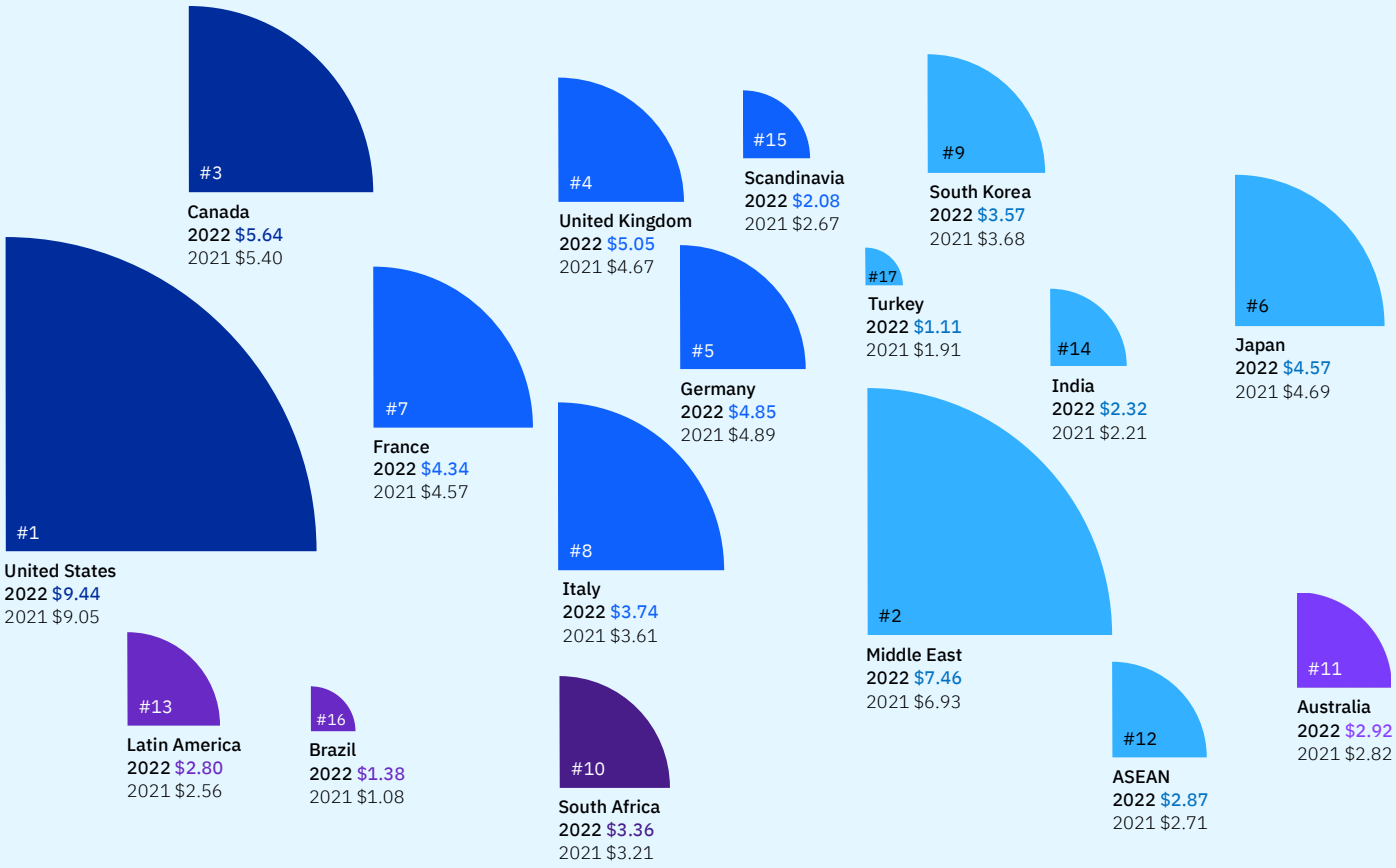


Figure 3: Measured in USD millions

Figure 3: The United States was the costliest country for average total cost of a data breach for the 12th year in a row. The top five countries or regions with the highest average cost of a data breach were:

1. The United States — USD 9.44 million
2. The Middle East — USD 7.46 million
3. Canada — USD 5.64 million
4. The United Kingdom — USD 5.05 million
5. Germany — USD 4.85 million

The United States had the highest average total cost of a data breach at USD 9.44 million, a 4.3% increase of USD 0.39 million, up from USD 9.05 million in 2021. Similar to last year, the Middle East region again had the second highest average total cost of a data breach, increasing from USD 6.93 million in 2021 to USD 7.46 million in 2022. This average cost was an increase of USD 0.53 million, or 7.6%. Canada was again the third highest cost country at USD 5.64 million, an increase of USD 0.24 million or 4.4%. The United Kingdom climbed to number four from eighth out of the 17 countries or regions, surpassing Germany, Japan and France in the ranking. The average total cost of a breach in the United Kingdom was USD 5.05 million, up from USD 4.67 million, an increase of USD 0.38 million, or 8.1%.

Out of the 17 countries or regions studied, six — Germany, Japan, France, South Korea, Scandinavia and Turkey — saw a decrease in the average total cost of a data breach. Brazil, 16th on the list at USD 1.38 million, saw the largest relative cost increase, up USD 0.3 million or 27.8%. Turkey, 17th on the list, saw the largest relative cost decrease, falling from USD 1.91 million to USD 1.11 million, a decrease of USD 0.8 million or 42%. Broad swings in currency valuations, such as occurred in Turkey, can play a role in cost variations from year to year.

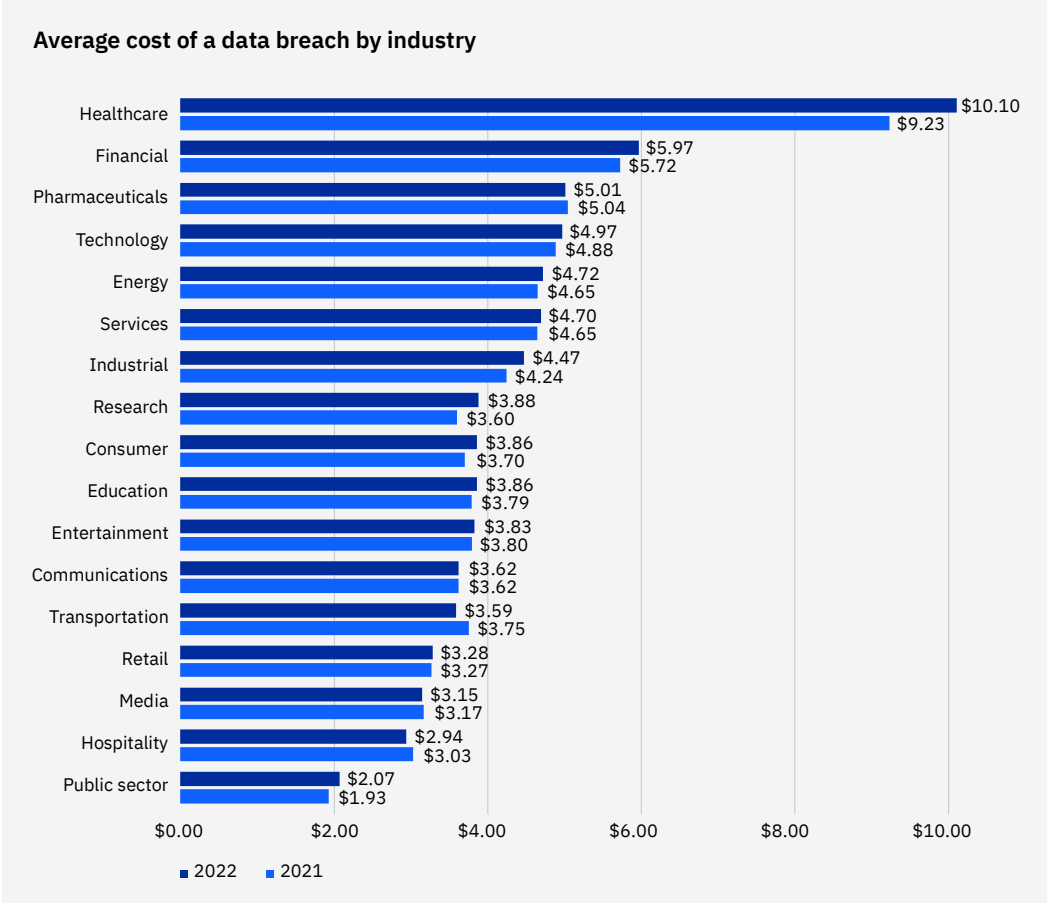


Figure 4: Measured in USD millions

Figure 4: Healthcare was highest cost industry for the 12th year in a row.
The average total cost of a breach in healthcare increased from USD 9.23 million in the 2021 report to USD 10.10 million in 2022, an increase of USD 0.87 million or 9.4%. Healthcare is one of the more highly regulated industries and is considered critical infrastructure by the US government.

Healthcare is one of the more highly regulated industries and is considered critical infrastructure by the US government.

The top five industries by cost were unchanged in the order of ranking from the 2021 report. Following healthcare were the financial, pharmaceuticals, technology and energy industries. The financial industry saw an increase from USD 5.72 million in 2021 to USD 5.97 million in 2022, an increase of USD 0.25 million or 4.4%. The industrial industry, comprised of chemical, engineering and manufacturing organizations, saw an increase from USD 4.24 million to USD 4.47 million in 2022, an increase of USD 0.23 million or 5.4%. The average total cost decreased slightly in four industries — pharmaceuticals, transportation, media and hospitality.

Figure 5: Detection and escalation costs surpassed lost business costs as the largest of four cost categories comprising the cost of a data breach, for the first time in six years. Broken down into four cost categories — lost business, detection and escalation, notification and post breach response — the largest share of data breach costs in 2022 was detection and escalation. Detection and escalation costs increased from USD 1.24 million in 2021 to USD 1.44 million in 2022, an increase of USD 0.2 million or 16.1%. Detection and escalation costs include activities that enable a company to reasonably detect a breach. These costs include forensic and investigative activities; assessment and audit services; crisis management; and communications to executives and boards.

For the first time in at least six years, lost business, at USD 1.42 million in 2022, wasn't the largest share of data breach costs. Lost business costs decreased from USD 1.59 million in 2021, a decrease of 10.7%. Lost business costs include activities that attempt to minimize the loss of customers, business disruption and revenue losses. These costs include business disruption and revenue losses from system downtime; cost of lost customers and acquiring new customers; and reputation losses and diminished goodwill.

Notification costs and post breach response costs remained relatively unchanged from 2021 to 2022. See "How we calculate the cost of a data breach" in the "Research methodology" section for definitions of each of the four cost categories.

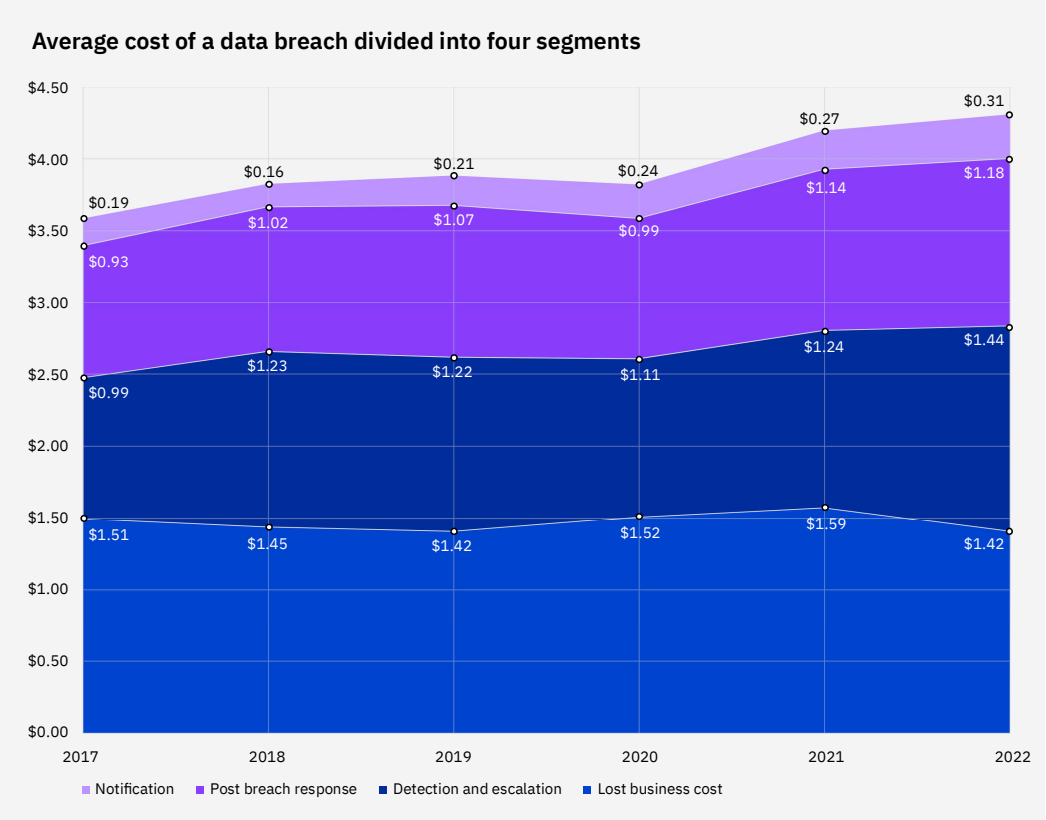


Figure 5: Measured in USD millions

Was this your first data breach?

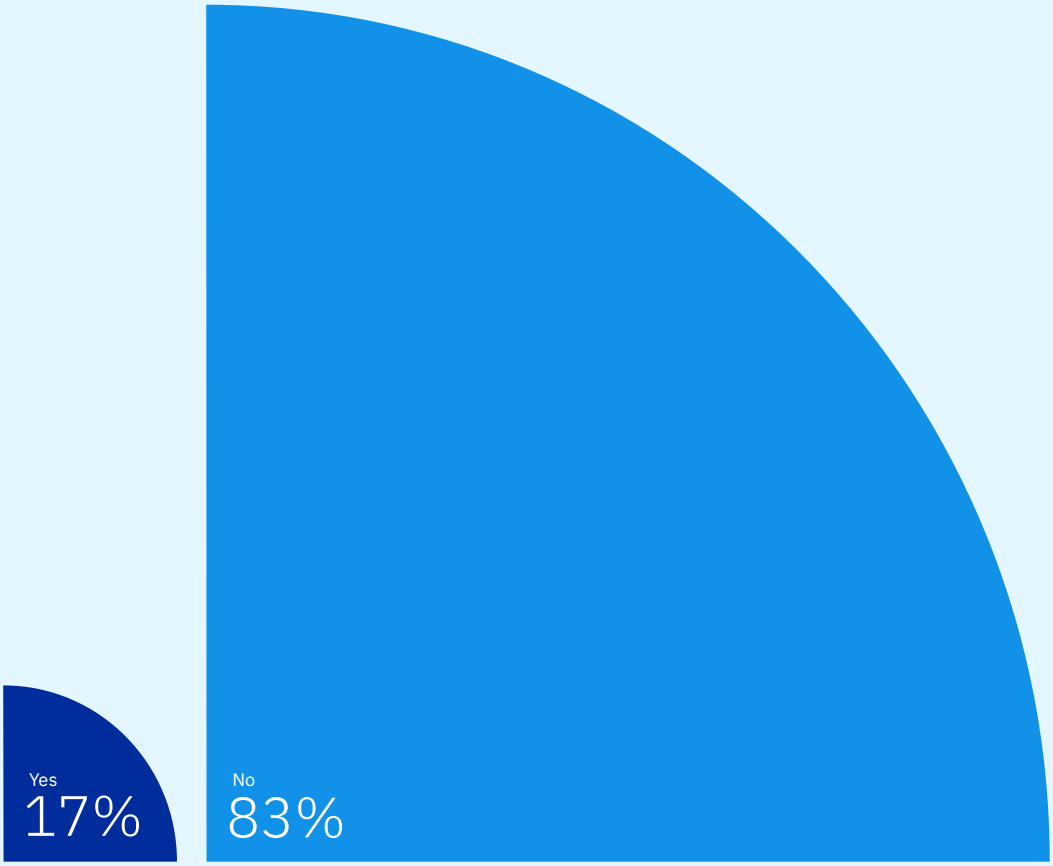


Figure 6

Figure 6: Most organizations in the study have experienced more than one data breach.
Of the 550 organizations in the study, just 17% said this was their first data breach. Eighty-three percent said this wasn't their first data breach. With security teams handling more incidents every year and considering the impact of remote work on security, it's likely the recurrence of breaches is climbing.

Figure 7: A majority of organizations in the study said they increased the price of their products and services as a result of the data breach.
In response to the question, 60% said they increased prices, and 40% said they didn't increase prices.

Did the data breach result in your organization increasing the price of products and services?

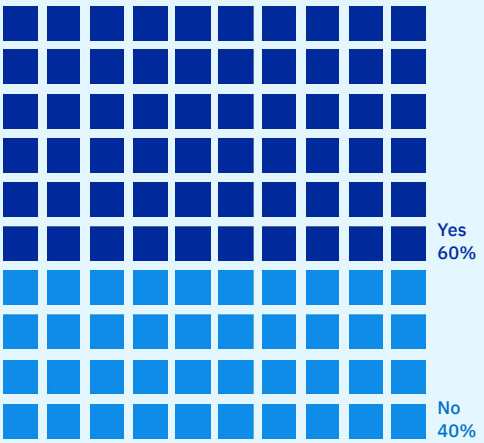


Figure 7

277 days

Average time to identify and contain a data breach

Data breach lifecycle

The time elapsed between the first detection of the breach and its containment is referred to as the data breach lifecycle. The time to identify a breach describes the time it takes to detect that an incident has occurred. The time to contain a breach refers to the time it takes for an organization to resolve a situation when it's been detected and ultimately restore service. These metrics can be used to determine the effectiveness of an organization's incident response and containment processes.

Figure 8: The mean or average time to identify and contain a data breach fell from 287 days in 2021 to 277 days in 2022, a decrease of 10 days or 3.5%.
In 2022 it took an average of 207 days to identify the breach and 70 days to contain the breach. In 2021 it took an average of 212 days to identify the breach and 75 days to contain the breach. The 277-day average in 2022 means that if a breach occurred on January 1, it would take until October 4 of that year to identify and contain the breach. The 277-day average is consistent with the average over the past seven years, with a maximum difference of 11% between the lowest total, 257 days in 2017, and the highest total, 287 days in 2021.

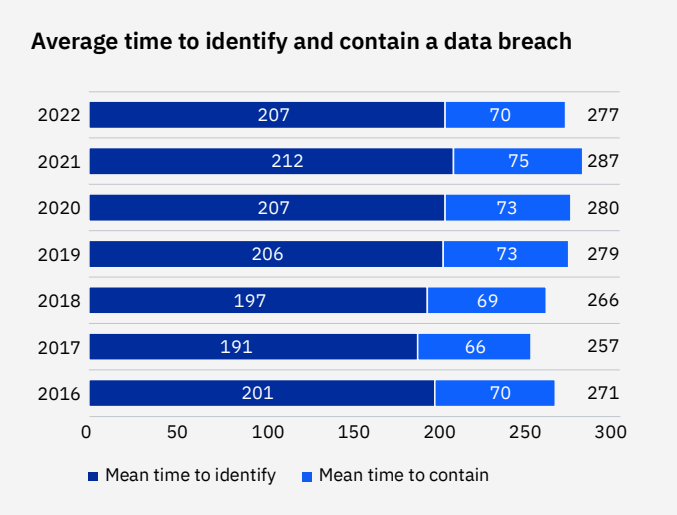


Figure 8: Measured in days

Figure 9: A shorter data breach lifecycle continues to be associated with lower data breach costs.
A data breach lifecycle of less than 200 days was associated with an average cost of USD 3.74 million in 2022, compared to USD 4.86 million for breaches with a lifecycle of greater than 200 days. This difference represents an average cost savings of USD 1.12 million, or 26.5%, for breaches with the shorter than 200-day lifecycle.

The cost gap between a lifecycle longer than 200 days and a lifecycle shorter than 200 days was smaller in 2022 than in 2021, when it was USD 1.26 million. The cost gap in 2022 — USD 1.12 million — is the same size as the cost gap in 2020. The cost gap has grown slightly over the past seven years, while the average cost of a data breach has also grown incrementally. The 2021 cost gap of USD 1.26 million was the largest of the past seven years.

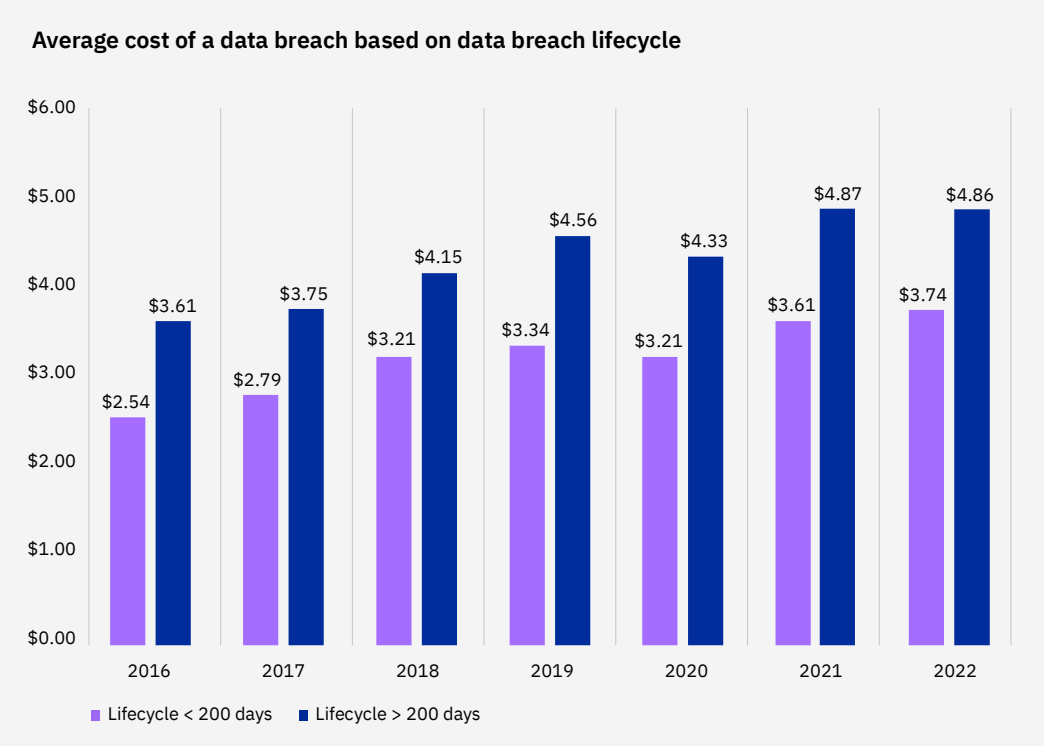


Figure 9: Measured in USD millions. Sum of days to identify and days to contain equals the breach lifecycle.

Figures 10a and 10b: Data breaches in high data protection regulatory environments, such as the healthcare, financial, energy, pharmaceuticals and education industries, tended to see costs accrue in later years following the breach.
The difference between low and high regulatory environments showed up in a pronounced way two years or more after the data breach — the "longtail" costs. In highly regulated industries, an average of 24% of data breach costs were accrued more than two years after the breach occurred. This result compares to an average of 8% of costs accrued more than two years after a breach in low regulatory environments.

In low regulatory environments, data breach costs tended to accrue in the first three to six months — where an average of 24% of data breach costs accrued. In the overall average for 2022, 52% of costs were incurred in the first 12 months, 29% in the second year after the breach and 19% more than two years after the breach. For highly regulated industries, 45% of costs accrued in the first year, 31% in the second year and 24% more than two years after the breach.

In the analysis of industries in the high regulation categories, we concluded that regulatory and legal costs may have contributed to higher costs in the years following a breach.

Note: This analysis was comprised of a subset of 218 companies with historical data from previous breaches.

Time elapsed	Percentage of total cost		
	2022 average	Low	High
1st year	52%	66%	45%
2nd year	29%	26%	31%
2+ years	19%	8%	24%

Figure 10a

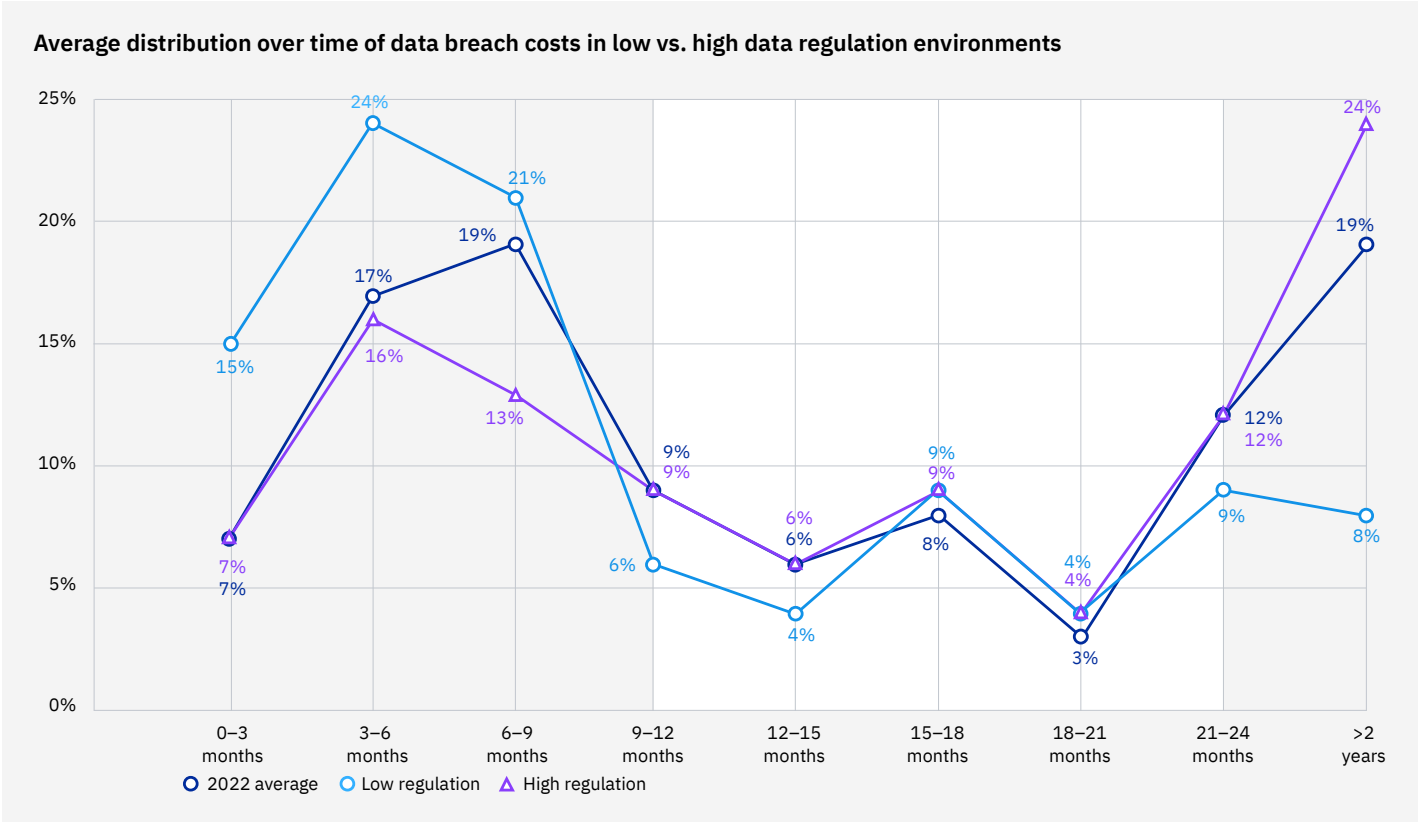


Figure 10b: Percentage of total costs accrued in three-month intervals

USD 4.91 million

Average cost of data breach with a phishing initial attack vector

Initial attack vectors

This section looks at the prevalence and cost of initial attack vectors of data breaches. The breaches in the study are divided into 10 initial attack vectors, ranging from accidental data loss and cloud misconfiguration to phishing, insider threats and stolen or compromised credentials. This section also compares the average time it takes to identify and contain breaches based on their initial attack vector.

Figure 11: The most common initial attack vector in 2022 was stolen or compromised credentials, responsible for 19% of breaches in the study, at an average cost of USD 4.50 million. In 2022, the most common initial attack vectors were compromised credentials at 19% of breaches, phishing at 16% of breaches, cloud misconfiguration at 15% of breaches and vulnerability in third-party software at 13% of breaches. The 2021 report saw the same order of the top four initial attack vectors.

The costliest initial attack vector in 2022 on average was phishing at USD 4.91 million. Following phishing was business email compromise at USD 4.89 million and 6% of breaches, vulnerability in third-party software at USD 4.55 million and compromised credentials at USD 4.50 million.

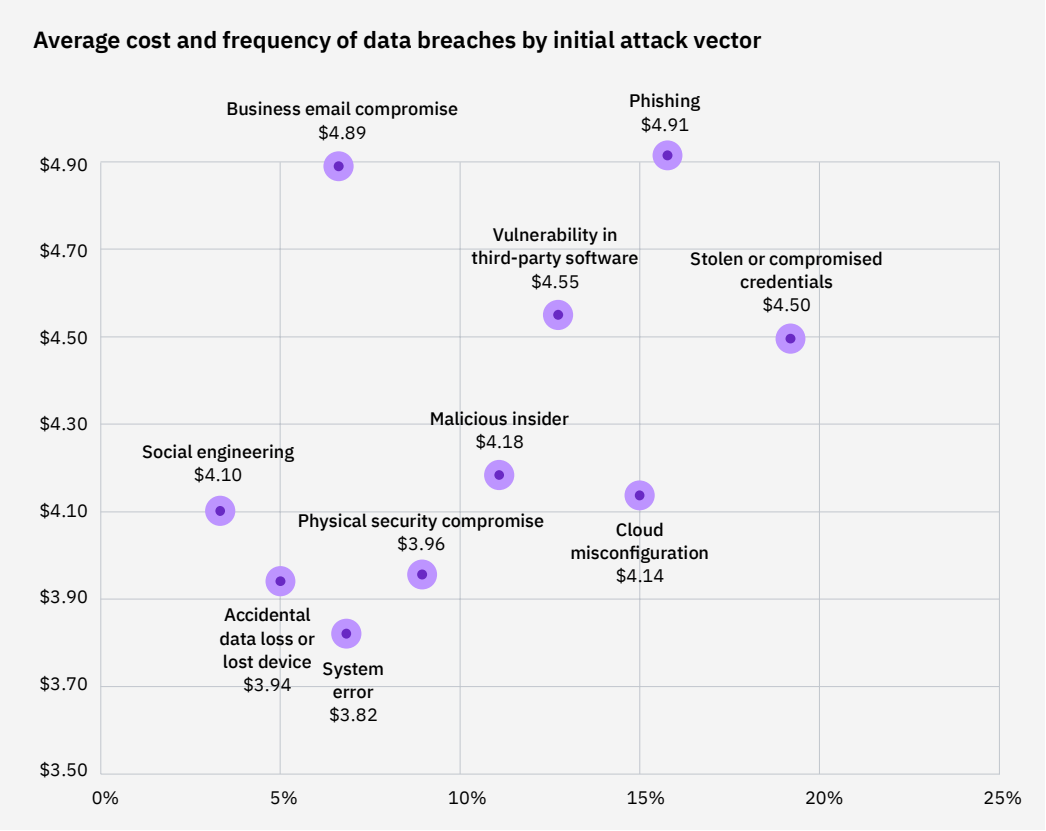


Figure 11: Measured in USD millions

Figure 12: Attack vectors with longer mean times to identify and contain, such as phishing or business email compromise, were also among the most expensive types of breaches. Stolen or compromised credentials were the initial attack vector with the longest mean time to identify and contain the breach, at 327 days. That time is 16.6% greater than the overall mean time to identify and contain a data breach. Compromised credentials were also the most common — 19% — initial attack vector leading to data breaches in the study.

Breaches caused by business email compromise had the second highest mean time to identify and contain, at 308 days. Business email compromise was also the second costliest initial attack vector, with breaches costing an average of USD 4.89 million. Breaches caused by phishing had the third highest mean time to identify and contain, at 295 days, and had the highest average cost by initial attack vector, at USD 4.91 million. Vulnerability in third-party software had the fourth highest mean time to identify and contain a breach, with an average that was above the overall average — 284 days versus 277 days.

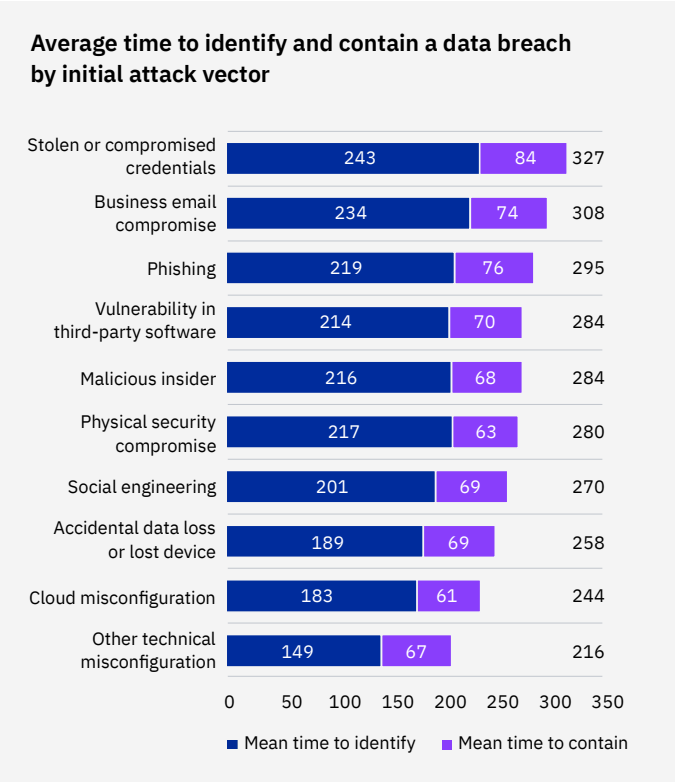


Figure 12: Measured in days

USD 5.57 million

Average cost of a breach for organizations with high levels of compliance failures

Key cost factors

This section looks at a multitude of factors that influence the cost of a data breach, including various types of security technologies and practices. A special analysis of 28 cost factors examines their impact on the mean cost of a data breach. We look at how these 28 factors were associated with either lower-than-average breach costs stemming from a cost mitigating influence, or a higher-than-average cost of a breach resulting from a cost amplifying influence.

The following cost factors are new to the report this year: IAM; XDR technologies; MFA; and crisis management teams.

These cost factors aren't additive, so it's not consistent with this research to add multiple cost factors together to calculate the cost of a breach.

Figure 13 shows the impact of 28 factors on the average cost of a data breach.
The chart shows the average cost difference of breaches at organizations with these cost-influencing factors compared to the mean cost of a data breach of USD 4.35 million. The chart is divided into those factors that are associated with a lower-than-average breach cost, which are cost mitigators, and those factors that are associated with a higher-than-average breach cost, or cost amplifiers.

AI platforms, a DevSecOps approach and use of an incident response (IR) team were the three factors associated with the highest cost decrease compared to the mean cost of a breach. For example, breaches at organizations with AI platforms had an average cost that was USD 300,075 less than the mean cost of a data breach of USD 4.35 million — which is approximately USD 4.05 million.

On the other hand, security system complexity, occurrence of cloud migration when the organization is in the process of migrating to the cloud and compliance failures were the three factors associated with the highest net increase in the average cost. For example, breaches at organizations with security system complexity had an average cost of USD 290,655 more than the mean cost of a data breach of USD 4.35 million — which is approximately USD 4.64 million.

For the first time, this year's report measured the impact of the following four new cost factors: IAM; XDR technologies; MFA; and crisis management teams. Each of these factors was associated with lower-than-average breach costs, led by IAM.

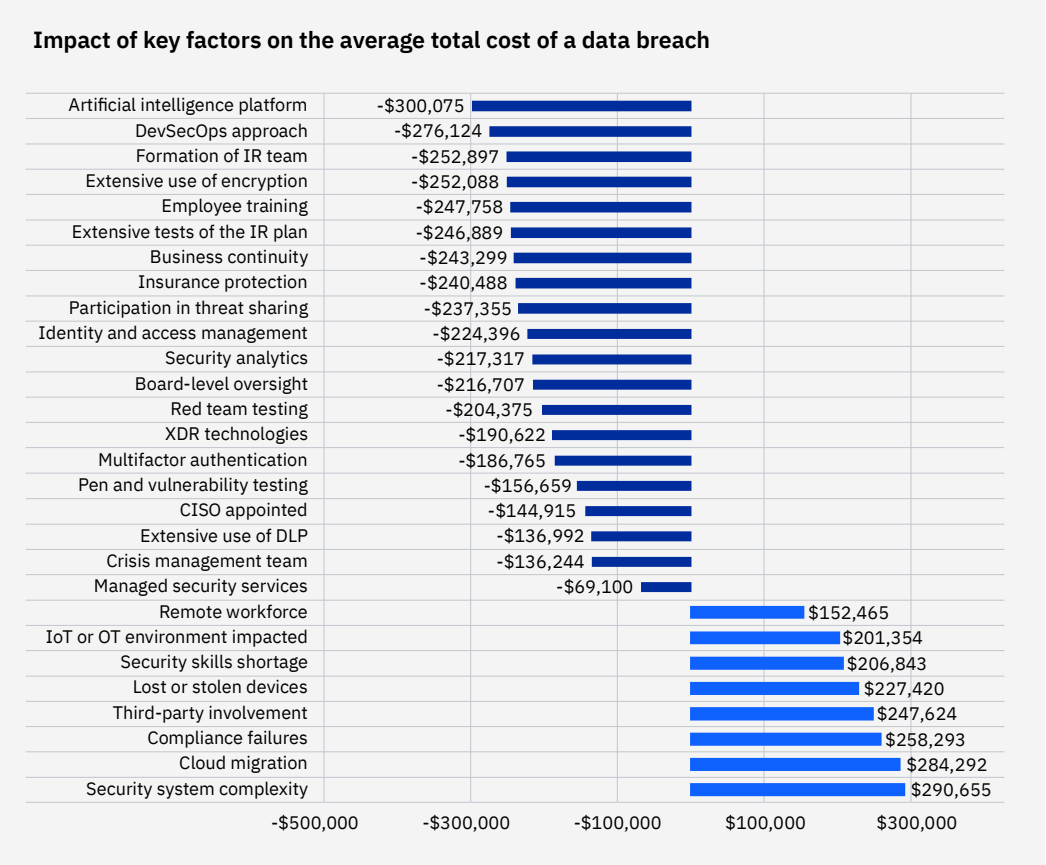


Figure 13: Measured in USD

Figure 14 looks at the three cost factors — out of 28 measured — with the greatest level of impact in potentially amplifying the average cost of a data breach.
This chart compares organizations with a high level of the cost factor to those with a low level of the cost factor. There was a difference of USD 2.47 million, or 58%, between high levels and low levels of security system complexity. A difference of USD 2.27 million, or 50.5%, occurred between high levels and low levels of cloud migration. There was a difference of USD 2.26 million, or 50.9%, between high levels and low levels of compliance failures. These data points showed that having high levels of these cost factors present was also associated with a significantly higher than average cost of a data breach. Organizations with a high level of cloud migration had a USD 5.63 million average cost that was USD 1.28 million higher than the average cost of a data breach, a difference of 25.7%.

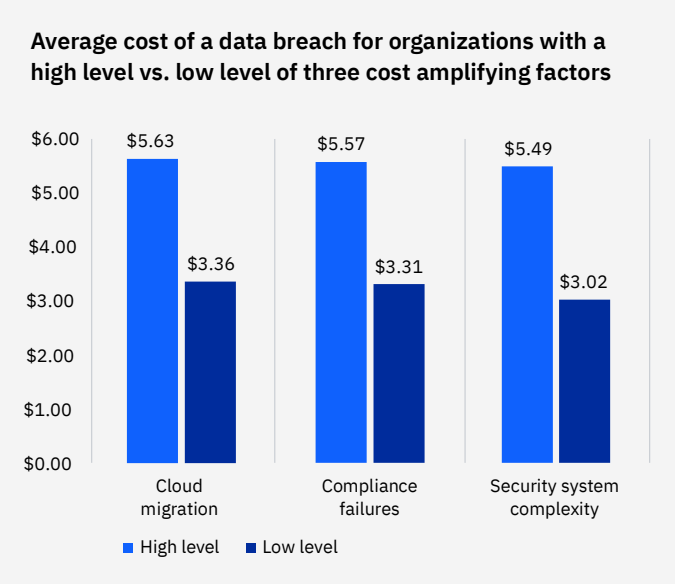


Figure 14: Measured in USD millions

Figure 15 looks at the three cost factors — out of 28 measured — with the greatest level of impact in potentially mitigating the cost of a data breach.
The chart compares organizations with a high level of the cost factor to those with a low level of the cost factor. Those organizations with high levels of use of security platforms that use AI had an average cost of a breach that was USD 2.39 million, or 55.3%, lower than those with low levels of use of an AI platform. Organizations with high levels of use of an IR team had an average cost of a breach that was USD 2.12 million, or 44.9%, lower than those with a low level of use of an IR team. Those organizations with a high level of use of a DevSecOps approach had an average cost of a breach that was USD 1.17 million, or 26.7%, lower than those with a low level of use of DevSecOps. Organizations with high levels of these cost factors present had a significantly lower than average cost of a data breach. Those organizations with high level use of an AI platform had an average cost of USD 3.13 million that was USD 1.22 million lower than the overall average cost of a data breach, a 32.6% difference.

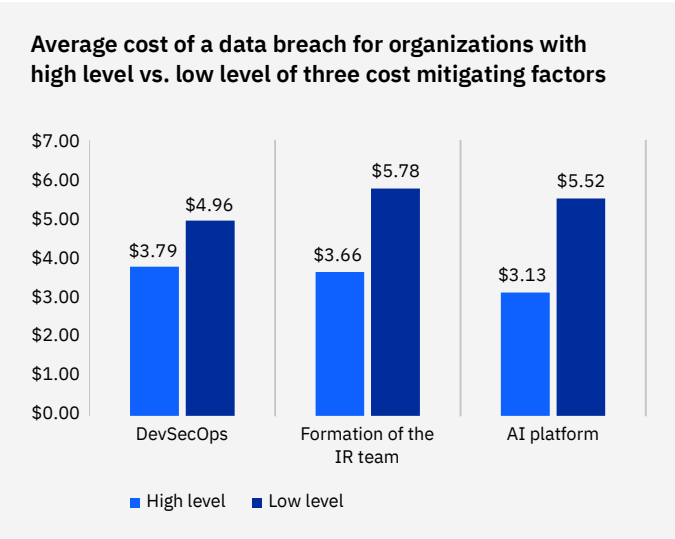


Figure 15: Measured in USD millions

USD 3.05 million

Average savings from fully deployed security AI and automation versus no security AI and automation

Security AI and automation

This was the fifth year we examined the relationship between data breach cost and security AI and automation. In this context, security AI and automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of incidents and intrusion attempts. Such technologies depend upon AI, machine learning, analytics and automated security orchestration.

On the opposite end of the spectrum are processes driven by manual inputs, often across dozens of tools and complex, nonintegrated systems, without data shared between them.

Figure 16: The share of organizations with fully or partially deployed security AI and automation increased by five percentage points, from 65% to 70%, between 2021 and 2022.
Fully deployed security AI and automation increased by six percentage points, from 25% to 31%, between 2021 and 2022 and by 10 percentage points, from 21% to 31%, between 2020 and 2022. The share of organizations with no security AI and automation deployed decreased from 35% in 2021 to 30% in 2022 and has decreased from 41% in 2020, a difference of 11 percentage points.

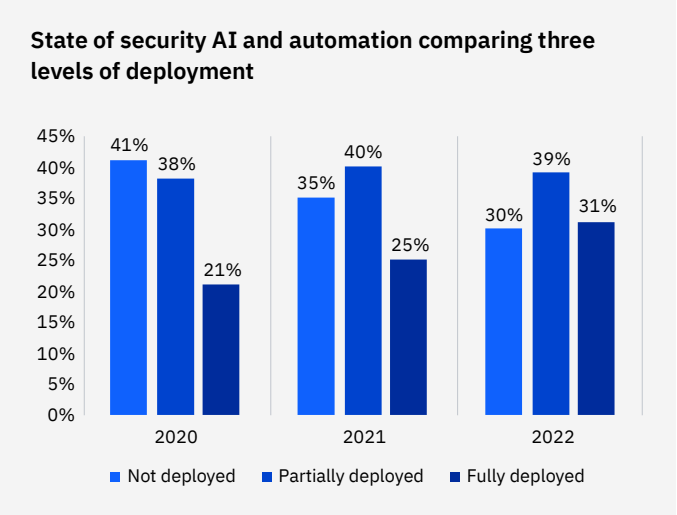


Figure 16: Percentage of organizations per deployment level

Figure 17: Fully deployed security AI and automation was associated with average breach costs that were USD 3.05 million lower than with no security AI and automation deployed, a difference of 65.2%, the largest cost savings in the study.

Organizations with fully deployed security AI and automation had an average total cost of a data breach of USD 3.15 million. This average total cost compared to USD 6.20 million for organizations without security AI and automation deployed. The difference between average cost of a breach with fully deployed security automation and no security AI and automation deployed was smaller in 2022 than in 2021, when the gap was USD 3.81 million, or in 2020, when the savings was USD 3.58 million.

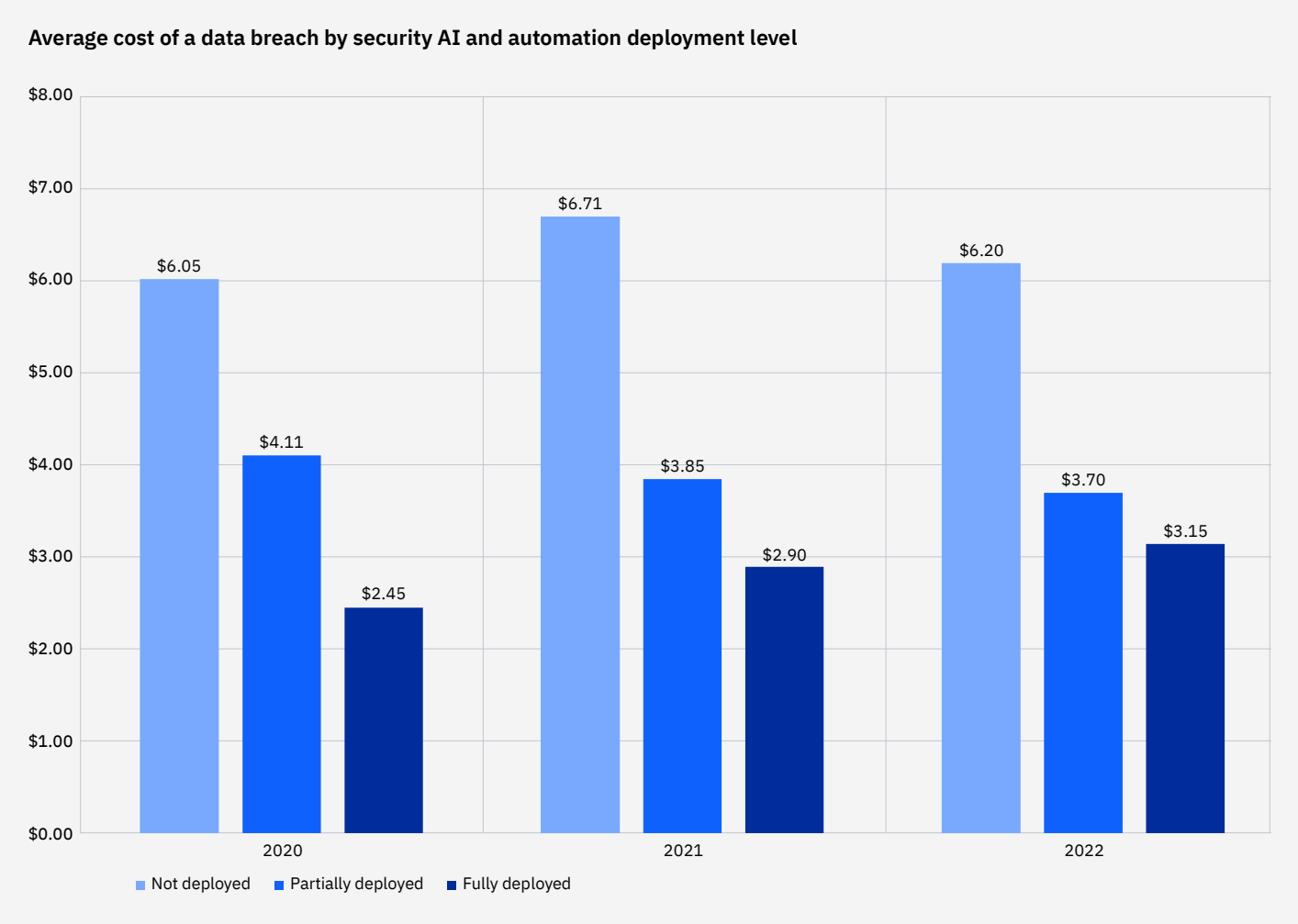


Figure 17: Measured in USD millions

Average time to identify and contain a data breach by level of security AI and automation

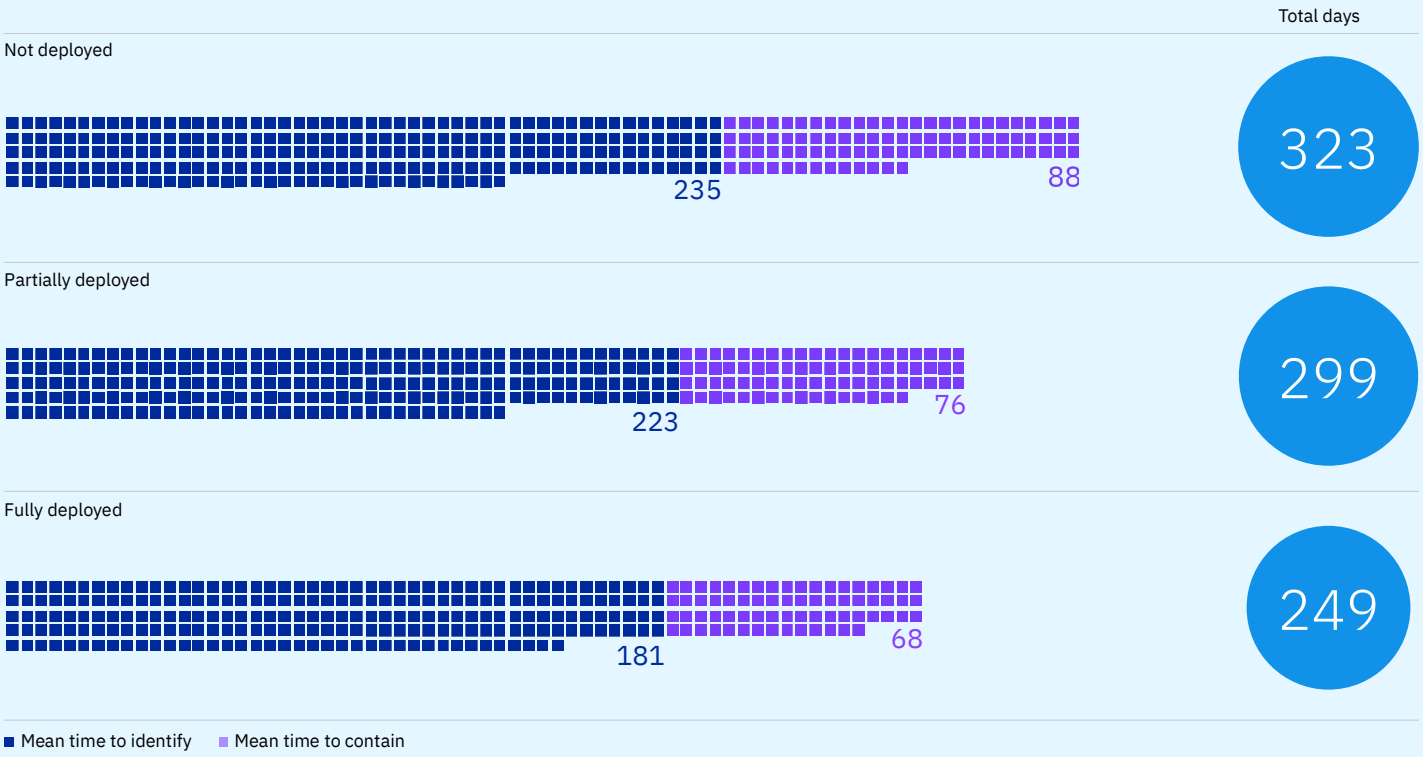


Figure 18: Measured in days

Figure 18: Organizations with fully deployed security AI and automation were able to detect and contain a breach much more quickly than organizations with no security AI and automation deployed.
Organizations with fully deployed security AI and automation took an average of 181 days to identify and 68 days to contain the data breach, for a total lifecycle of 249 days. Those organizations with no security AI and automation deployed took an average 235 days to identify and 88 days to contain a breach, for a total lifecycle of 323 days, which was 74 days longer than organizations with fully deployed security AI and automation. The average time to identify and contain a breach was a total of 299 days with partially deployed security AI and automation.

29 days

Organizations with XDR technologies identified and contained a breach 29 days faster than those without XDR

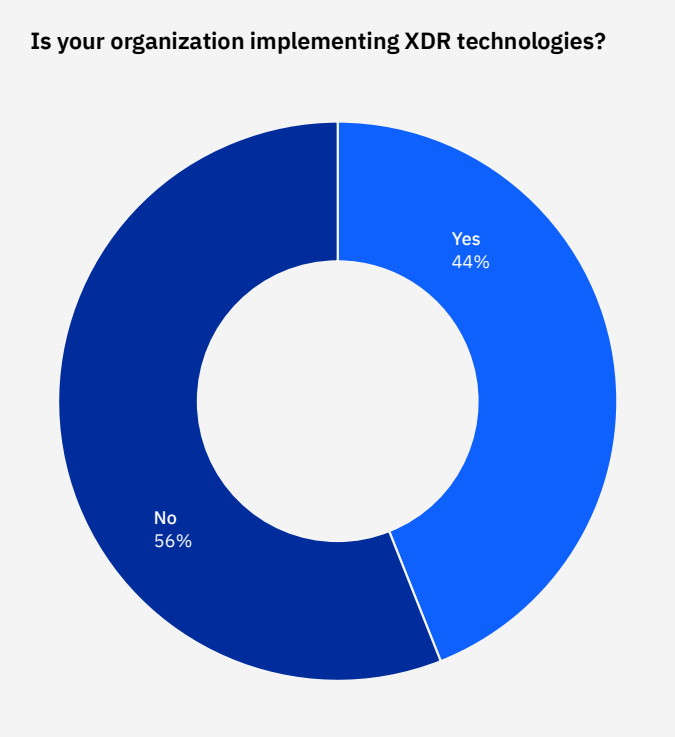


Figure 19

XDR technologies

For the first time, the study examined the effects of XDR technologies on the cost of a data breach. This section looks at the prevalence of XDR in the organizations studied, plus its impact on average total cost and the average time to contain data breaches.

Significantly, XDR impacted average breach costs with a savings of 9.2%. While these savings may appear humble at first sight, the true impact comes in the amount of time organizations saved in breach duration when they use XDR — nearly one month. Extra time to identify and contain a breach can add a lot to the overall cost of a breach and its consequences.

Figure 19: XDR capabilities were commonly used but not yet by a majority of organizations.
According to the survey of 550 organizations in the study, 44% are implementing XDR technologies, while 56% aren't implementing XDR technologies.

Figure 20: The use of XDR technologies was associated with a lower-than-average cost of a data breach.
Those organizations that are implementing XDR technologies experienced an average cost of a data breach of USD 4.15 million. Organizations that weren't implementing XDR technologies experienced an average cost of a data breach of USD 4.55 million. This cost was above the global average and USD 0.40 million more than breaches at organizations implementing XDR technologies, a difference of 9.2%.

Figure 21: The average time to identify and contain a data breach was significantly lower with XDR technologies.
Breaches at organizations with XDR technologies deployed took an average of 275 days to identify and contain the breach, which was 29 days less than breaches at organizations without XDR technologies deployed, at 304 days. That represents a 10% difference in mean time to identify and contain a breach between organizations with XDR technologies and those with no XDR technologies.

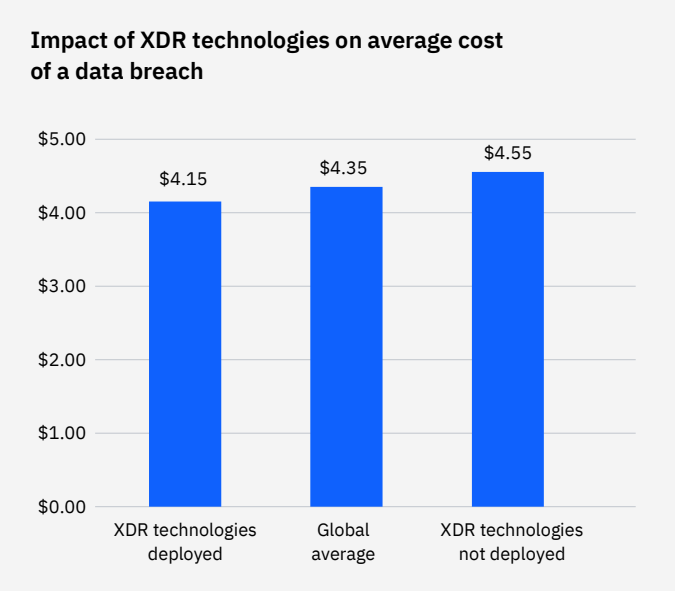


Figure 20: Measured in USD millions

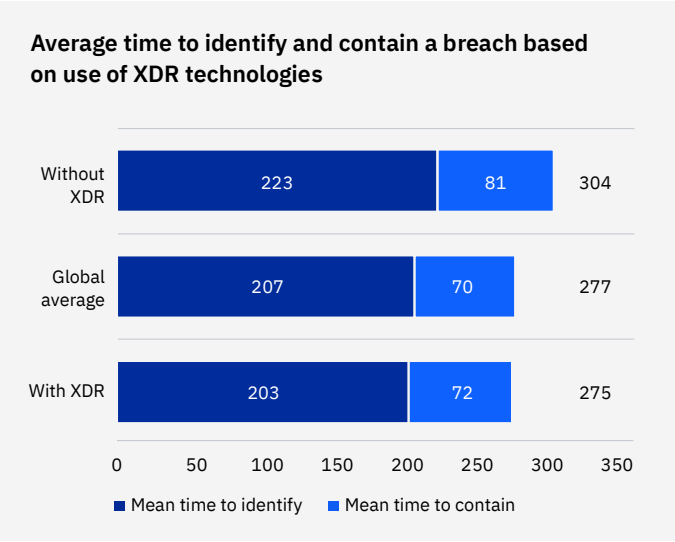


Figure 21: Measured in days

USD 2.66 million

Average breach cost savings at organizations with an IR team that tested an IR plan versus those with no IR team and had not tested an IR plan

Incident response

In previous years, this research has shown that the use of IR teams and testing of an IR plan significantly reduced the average cost of a data breach. In this year's analysis, we again looked at how IR teams, capabilities and processes impacted the cost of a breach.

Figure 22: A majority of organizations in the study had IR plans and testing of IR plans on a regular basis.
Nearly three-quarters of organizations in the study said they had an IR plan, with 73% saying they did have an IR plan and 27% saying they didn't have a plan. At organizations with an IR plan, 63% said they regularly tested the IR plan, with 37% saying they didn't regularly test the IR plan.

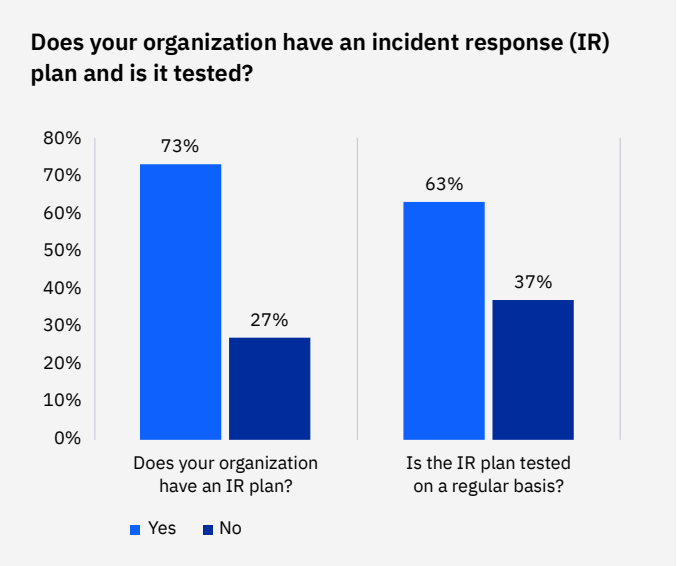


Figure 22

Average cost of a data breach with incident response (IR) team and IR plan testing

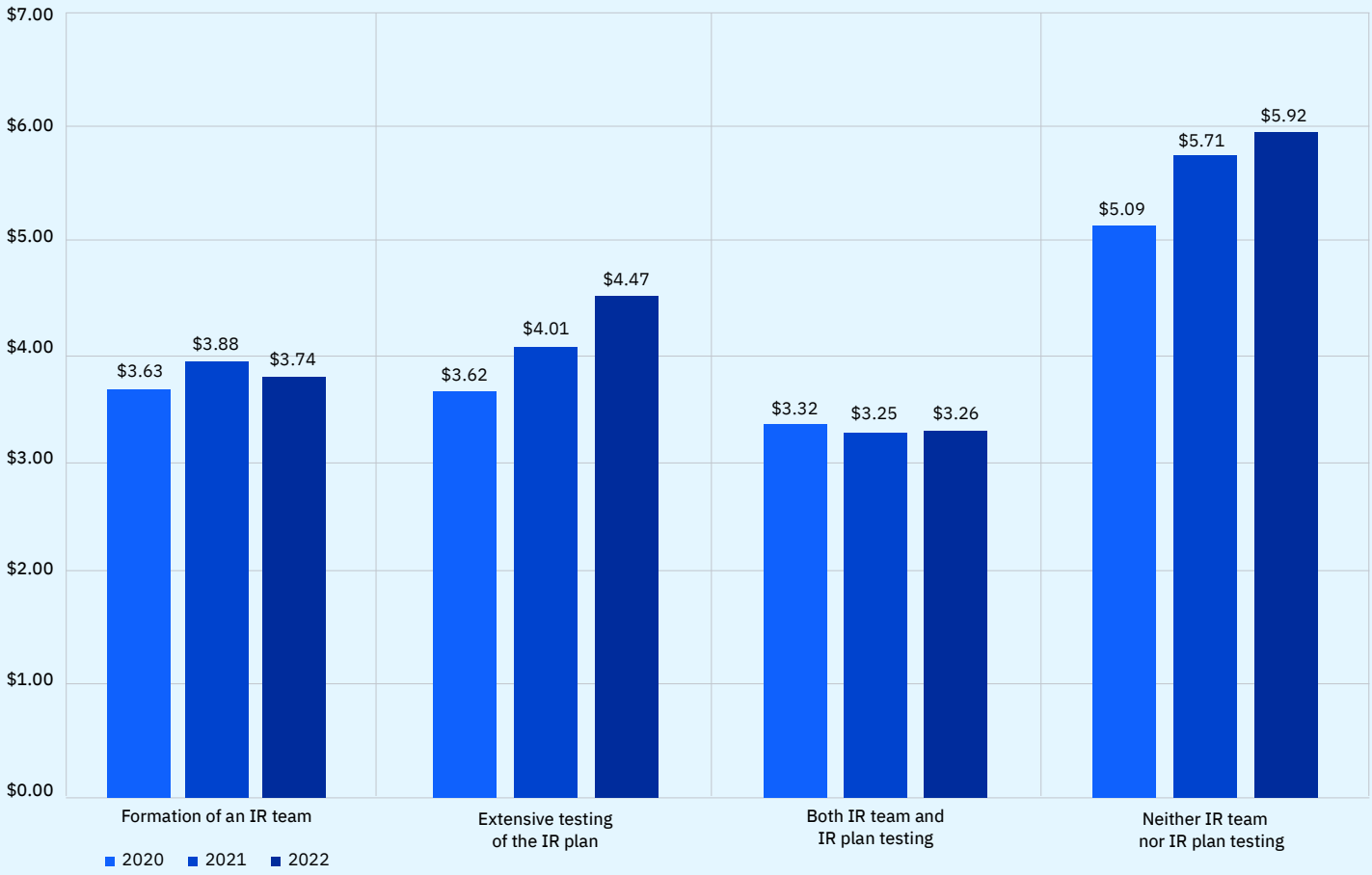


Figure 23: Measured in USD millions

Figure 23: IR teams and extensive IR plan testing continued to mitigate data breach costs in 2022.
The gap between the average data breach cost at organizations with both IR teams and IR plan testing and those with neither IR teams or IR plan testing continued to grow between the 2020 report and the 2022 report. Breaches at organizations with IR capabilities saw an average cost of a breach of USD 3.26 million in 2022, compared to USD 5.92 million at organizations without IR capabilities. This average cost was a difference of USD 2.66 million, or 58%. Those savings were an increase over 2021, when the average cost of a breach at organizations with IR capabilities saved USD 2.46 million, and in 2020, when the cost difference was USD 1.77 million. This finding indicates a growing cost-saving effectiveness of IR capabilities.

USD 2.10 million

Cost savings of breaches at organizations that use risk quantification techniques versus those that don't

Does your organization prioritize risks, threats and impacts based on risk quantification techniques?

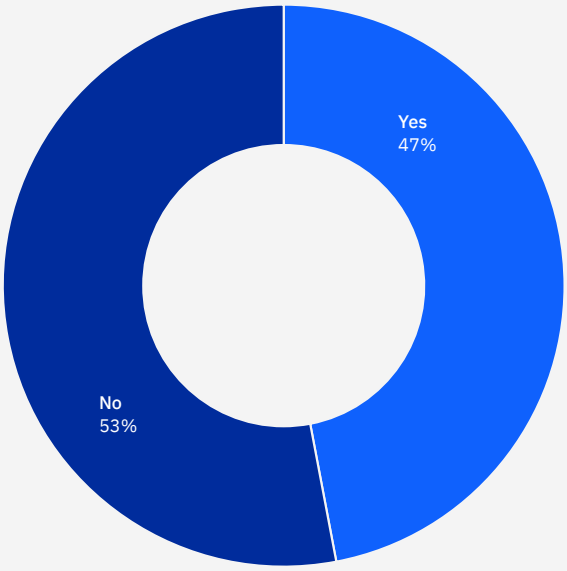


Figure 24

Risk quantification

Risk quantification looks at impacts, including financial impacts, availability of data and data integrity. Using risk quantification can highlight financial loss types by impact, including the following examples: loss of productivity; cost of response or recovery; reputation impact; and fines and judgments.

Chief information security officers (CISOs), risk managers and security teams can use benchmark research like the Cost of a Data Breach Report to infer general trends and cost averages in their industry or geography. However, using data specific to the organization, rather than industry averages, can clarify potential security gaps and how to reduce overall risk by quantifying security risk into financial terms.

This section looks at how many organizations are using risk quantification techniques to prioritize risks, threats and impacts and reviews the average cost impact of risk quantification techniques.

Figure 24: Less than half, 47%, said they prioritize risks, threats and impacts based on risk quantification techniques. Meanwhile, out of the 550 organizations studied, 53% don't prioritize risks, threats and impacts based on risk quantification techniques.

Figure 25: Risk quantification had a considerable effect on data breach costs, saving up to USD 2.10 million on average. Organizations that prioritized risks, threats and impacts based on risk quantification techniques had an average breach cost of USD 3.30 million. That cost was USD 2.10 million less than those that didn't use risk quantification, at USD 5.40 million, a savings of 48.3%. Risk quantification was associated with breach costs that were more than USD 1 million lower than the global average of USD 4.35 million.

Impact of risk quantification techniques on average cost of a data breach

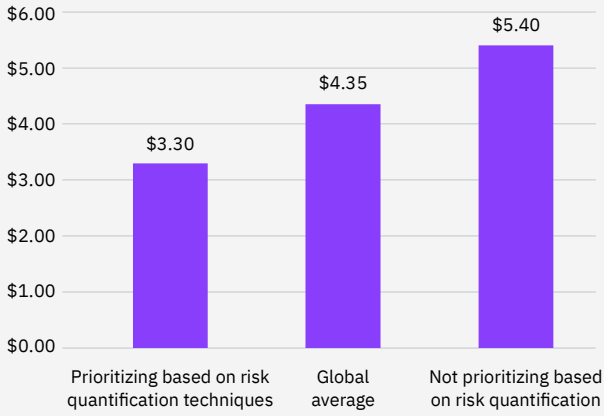


Figure 25: Measured in USD millions

USD 1.51 million

Average breach cost savings associated with a mature zero trust deployment versus early adoption of zero trust

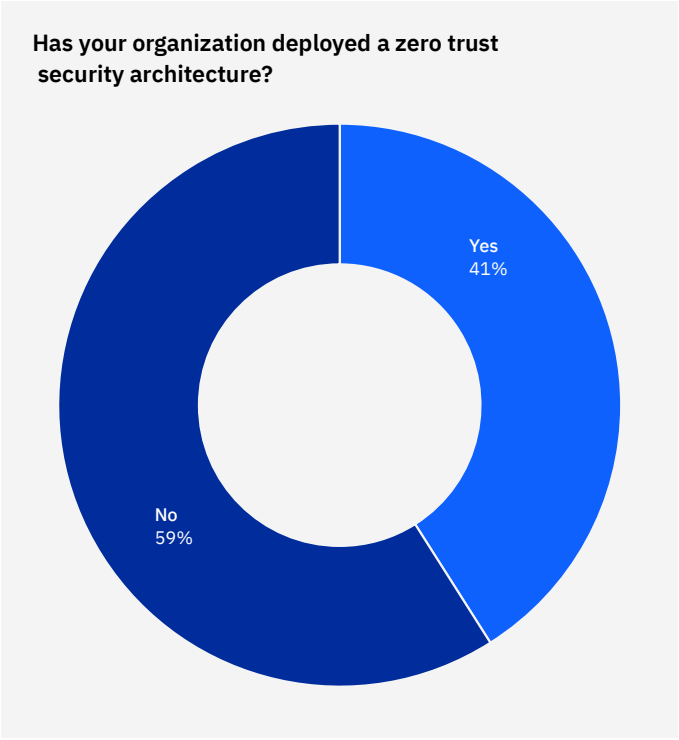


Figure 26

Zero trust

For a second year, this study examined the prevalence and financial impact of data breaches based on deployment of a zero trust security framework. The zero trust approach operates on the assumption that user identities or the network itself may already be compromised, and instead relies on AI and analytics to continuously validate connections between users, data and resources. As the data in this section shows, zero trust has a net positive impact on data breach costs.

Figure 26: In the 2022 study, 41% of organizations said they have deployed a zero trust security architecture, while 59% said they haven't.
This finding compares to the 2021 report when 35% said they had partially or fully deployed a zero trust architecture.

Figure 27: Organizations with zero trust deployed saved nearly USD 1 million in average breach costs compared to organizations without zero trust deployed.
The average cost of a data breach was USD 4.15 million at organizations with zero trust deployed, while the cost of a breach was an average USD 5.10 million at organizations without zero trust deployed. The difference was USD 0.95 million, representing a 20.5% savings for organizations with zero trust deployed.

Figure 28: Having a mature zero trust deployment was associated with breach costs that were more than USD 1.5 million lower than breaches at organizations with early adoption of zero trust.
Organizations with mature stage deployment of their zero trust security architecture, when zero trust is applied consistently across all domains, had an average data breach cost of USD 3.45 million. In midstage, when zero trust was applied in many areas of the organization, the average cost of a data breach was USD 3.96 million. For early adoption stage organizations that were beginning to implement a few practices, the average cost of a data breach was USD 4.96 million. This cost was USD 1.51 million more than breaches at mature organizations, a difference of 35.9%.

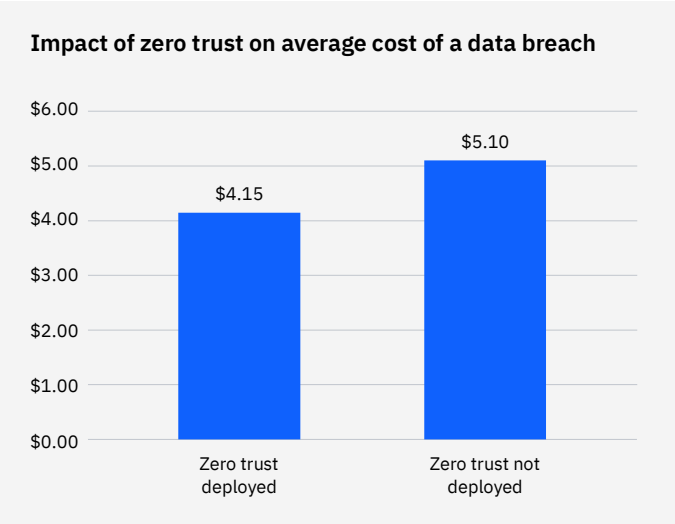


Figure 27: Measured in USD millions

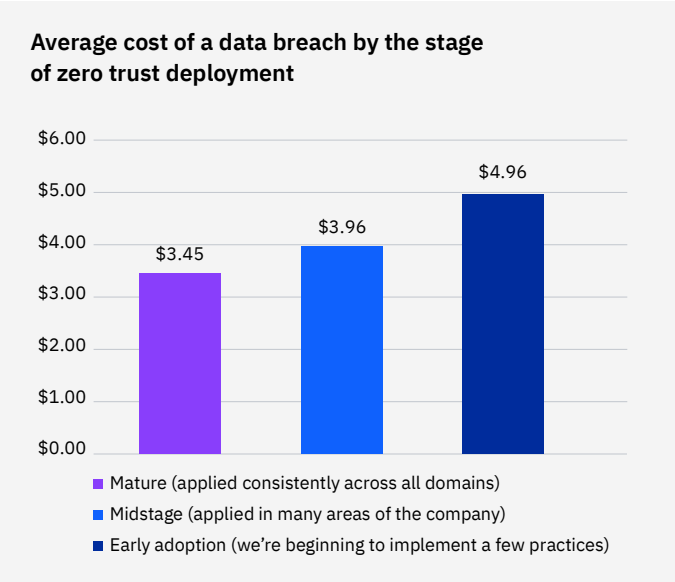


Figure 28: Measured in USD millions

49 days

Ransomware breaches took 49 days longer than average to identify and contain.

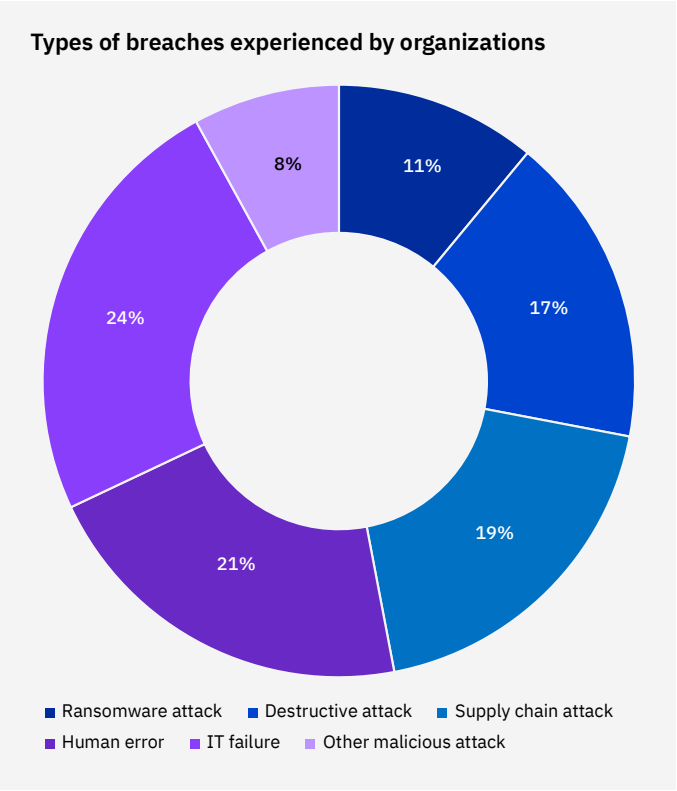


Figure 29

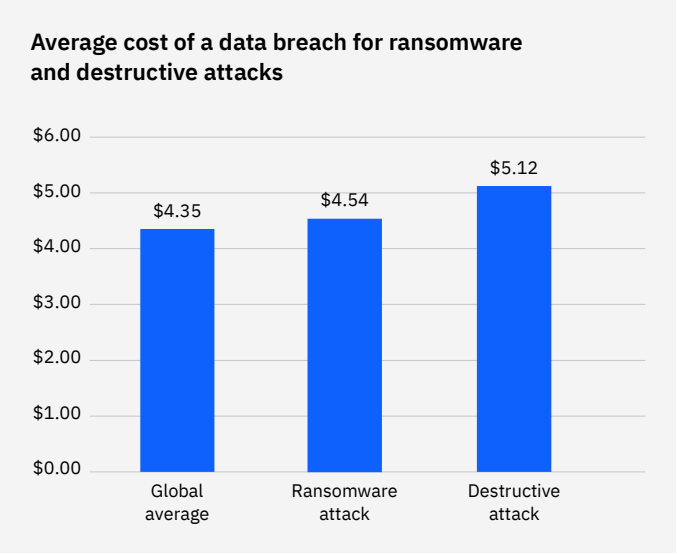


Figure 30: Measured in USD millions

Ransomware and destructive attacks

This was the second year that we examined the cost of ransomware and breaches. We also added destructive malware breaches to this year's study. Compared to last year, ransomware breach costs have declined slightly, from USD 4.62 million to USD 4.54 million. However, the frequency of ransomware breaches has increased — from 7.8% of breaches in the 2021 report to 11% in the 2022 study.

This year we looked at the lifecycle of these breaches, as well as what impact paying a ransom had on the non-ransom cost of the breach. Note: This study doesn't include the cost of the ransom itself in calculating the cost of a ransomware attack.

Figure 29: Ransomware was responsible for 11% of breaches, while destructive attacks were responsible for 17% of breaches.
Another 19% of breaches were caused by supply chain attacks, which were breaches caused due to a business partner being initially compromised. Human errors, meaning breaches caused unintentionally through negligent actions of employees or contractors, were responsible for 21% of breaches.

IT failures, which were caused by a disruption or failure in an organization's computer systems that led to data loss, were responsible for 24% of breaches. Such failures included errors in source code, or a process failure such as automated communication errors. The remaining 8% of breaches were other malicious attacks.

Figure 30: The average cost of a ransomware attack — not including the cost of the ransom itself — was USD 4.54 million, slightly higher than the overall average total cost of a data breach of USD 4.35 million.
The average cost of a destructive or wiper attack was USD 5.12 million, which was USD 0.77 million more than the overall average, a difference of 16.3%.

Figure 31: The average time to identify and contain a ransomware or destructive attack was significantly higher than average.
A ransomware attack took 237 days to identify and 89 days to contain, for a total lifecycle of 326 days. A destructive attack took 233 days to identify and 91 days to contain, for a total lifecycle of 324 days. Compared to the overall average lifecycle of 277 days, organizations took 49 days longer to identify and contain a ransomware attack, a difference of 16.3%. Additionally, organizations took 47 days longer to identify and contain a destructive attack, a difference of 15.6%.

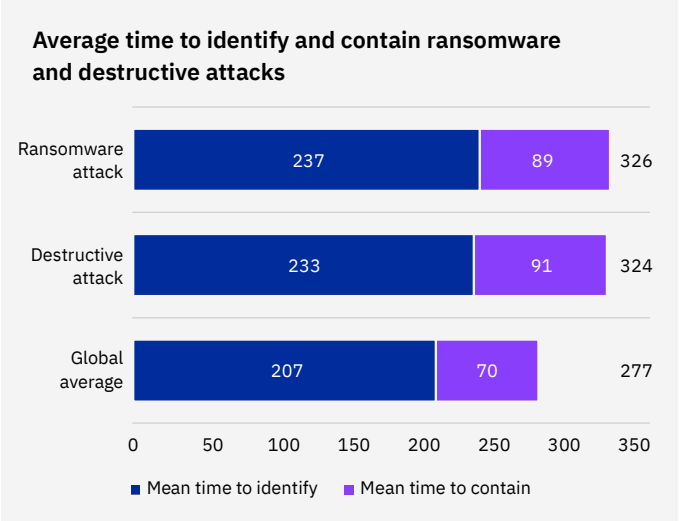


Figure 31: Measured in days

Figure 32: The average cost of a ransomware breach was higher for those that didn't pay the ransom.
The cost of the ransom wasn't included in the calculation of the cost of a ransomware breach. A ransomware breach's cost was based on activities, such as detection of the attack and loss of business due to system downtime. For those organizations that didn't pay the ransom, the average cost of the breach was USD 5.12 million. For organizations that did pay the ransom, the cost of the breach was USD 4.49 million. The difference in average cost was USD 0.63 million, or 13.1%.

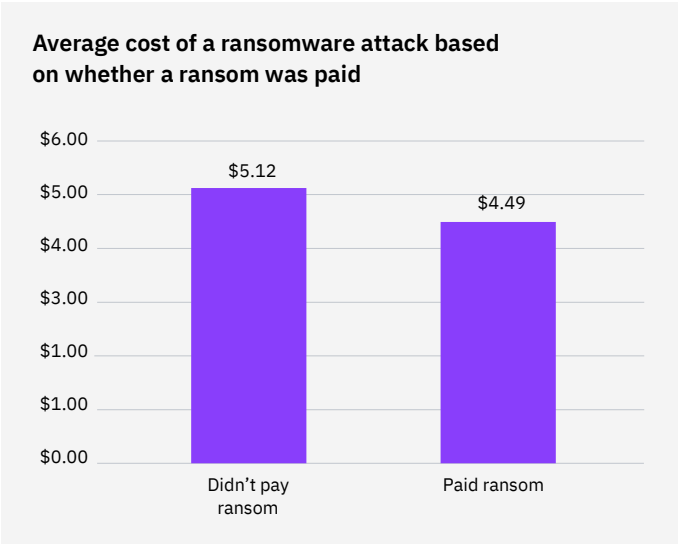


Figure 32: Measured in USD millions. Cost of ransom isn't included in this calculation.

26 days

A supply chain breach took on average 26 days longer to identify and contain than the global average

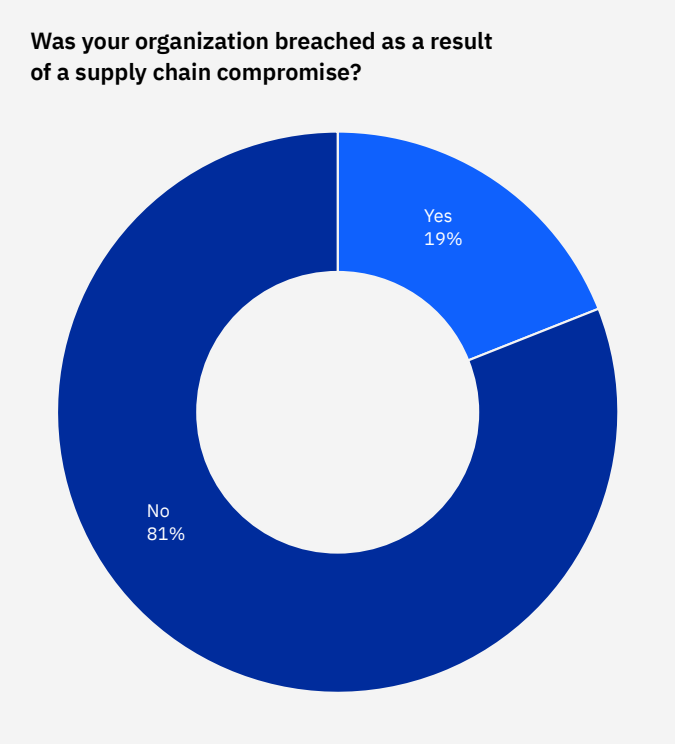


Figure 33

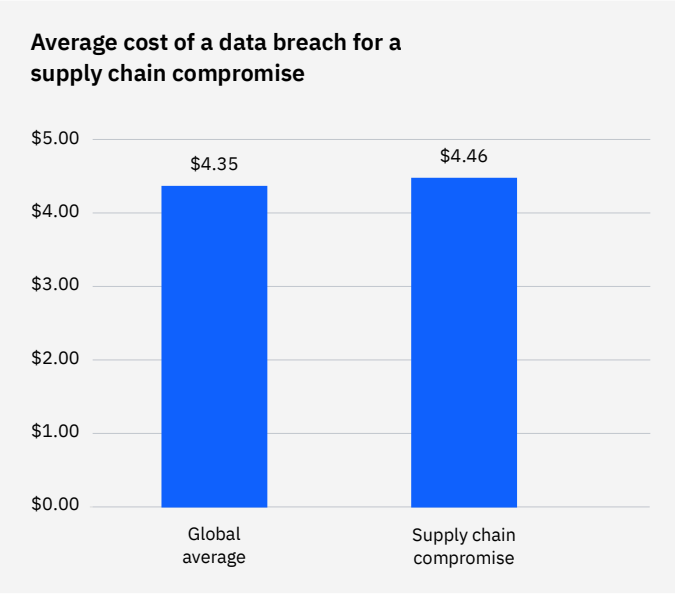


Figure 34: Measured in USD millions

Supply chain attacks

With a number of major supply chain attacks taking place in recent years, this year's report marked the first year that we examined data breaches in the context of supply chain attacks. A supply chain compromise is a breach resulting from a compromise of a business partner such as a supplier. As the research found, nearly one-fifth of breaches were caused by a supply chain compromise, and these compromises made breaches more expensive and resulted in longer lifecycles.

Figure 33: About one-fifth of breaches in the study were the result of a supply chain compromise.
Nineteen percent of organizations said yes, they were breached as a result of a supply chain compromise, and 81% said no.

Figure 34: The average total cost of a supply chain compromise was USD 4.46 million.
That cost was greater than the overall average cost of a data breach of USD 4.35 million, a difference of USD 0.11 million or 2.5%.

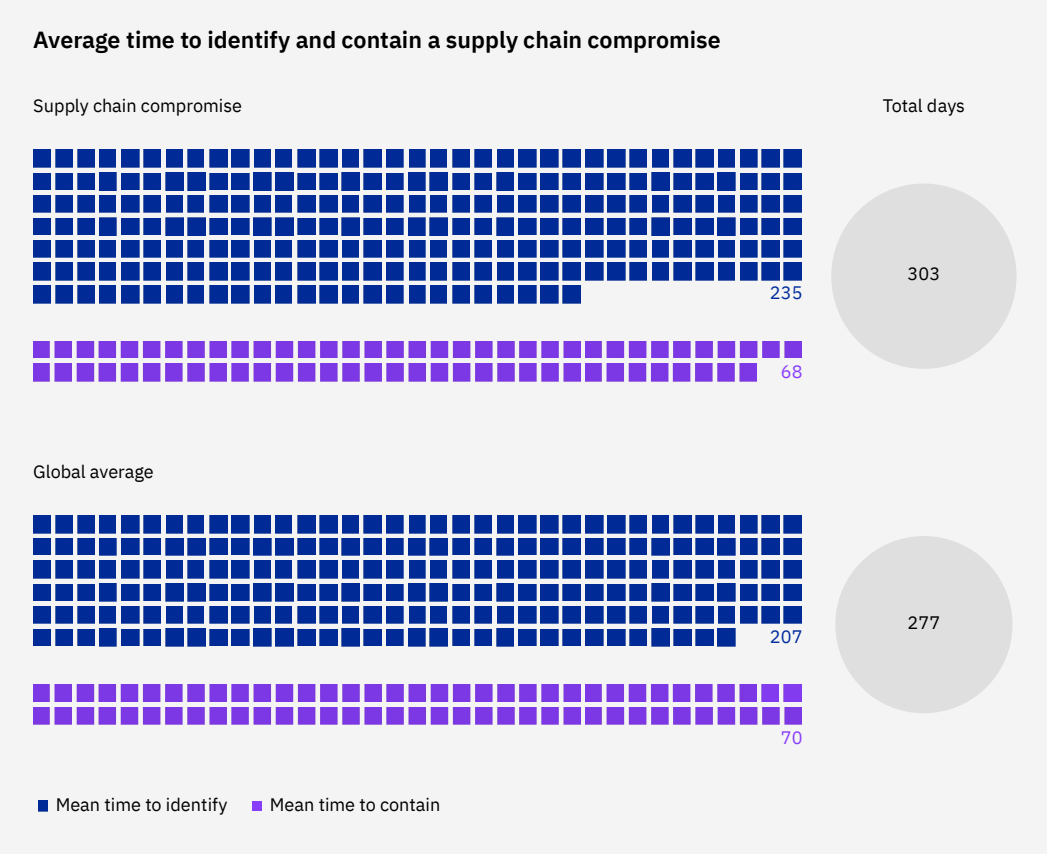


Figure 35: Measured in days

Figure 35: A supply chain compromise had a longer lifecycle than the global average.
Organizations took an average of 235 days to identify and 68 days to contain a supply chain compromise, for a total lifecycle of 303 days. The average lifecycle was 26 days longer than the overall average data breach lifecycle of 277 days, a difference of 9%.

79%

Share of critical infrastructure industries that didn't adopt a zero trust security approach

Critical infrastructure

This report marked the first year that we studied the cost and containment of data breaches in the context of critical infrastructure industries. Based on classification by the US Cybersecurity and Infrastructure Security Agency (CISA), critical infrastructure industries in this study included financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector.

One revelation of this analysis was that critical infrastructure industries had a much lower prevalence of zero trust security approaches than the global average. Critical infrastructure industries without zero trust strategies deployed had significantly higher data breach costs than average.

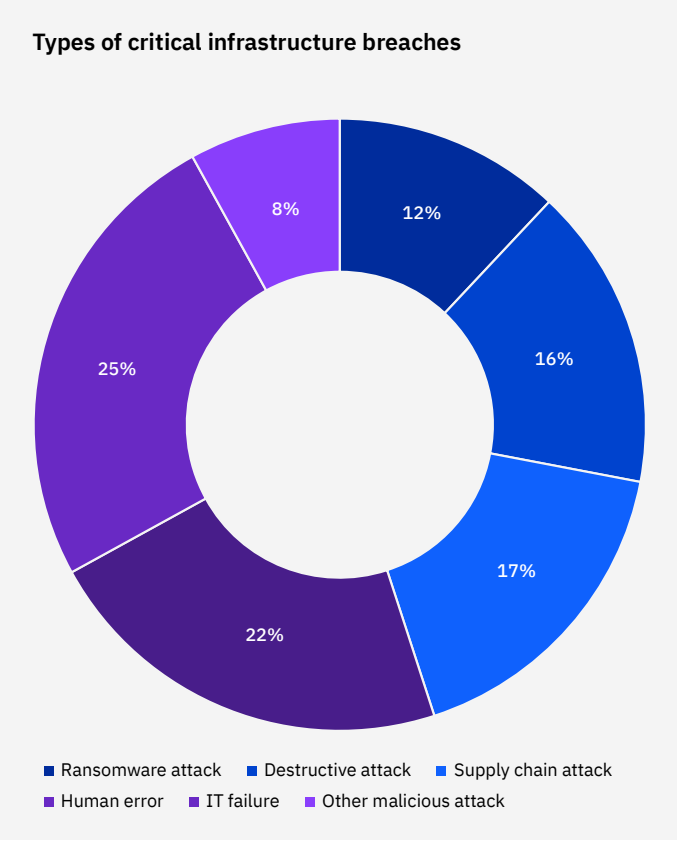


Figure 36

Figure 36: Ransomware and destructive attacks were responsible for more than a quarter of breaches in critical infrastructure industries.
Ransomware attacks accounted for 12% of critical infrastructure breaches, while destructive attacks were behind 16% of critical infrastructure breaches, for a combined 28%. Another 17% of breaches on these industries were supply chain attacks where a third-party business partner was the attack vector. Meanwhile, breaches caused by human error or IT failures accounted for 22% and 25%, respectively. The remaining 8% of critical infrastructure breaches were other malicious attacks.

Figure 37: The average cost of a data breach in critical infrastructure organizations was USD 4.82 million.
Critical infrastructure organizations had an average cost of a data breach USD 0.99 million higher than USD 3.83 million for organizations in noncritical infrastructure industries, a difference of 22.9%. Noncritical infrastructure industries included those organizations in pharmaceuticals, services, entertainment, consumer goods, media, hospitality, retail and research.

Figure 38: Critical infrastructure industries identified and contained data breaches more quickly than other industries.
The lifecycle of a data breach in critical infrastructure industries took fewer days than the global average or noncritical infrastructure industries. The mean time to identify in critical infrastructure industries was 204 days, compared to 211 days for other industries. The mean time to contain for critical infrastructure industries was 69 days, compared to 71 days for other industries. The combined average of 273 days to identify and contain a breach in critical infrastructure was four days shorter than the overall global average of 277 days. Additionally, the combined average for critical infrastructure industries was nine days shorter than the 282 days average for other industries.

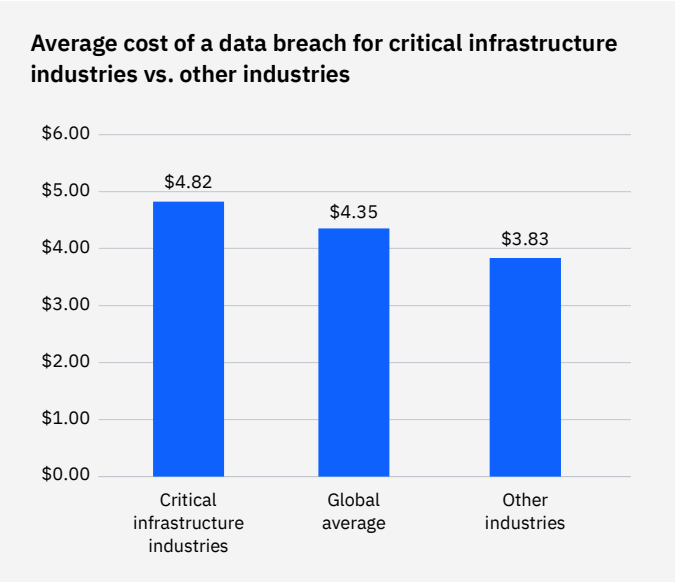


Figure 37: Measured in USD millions

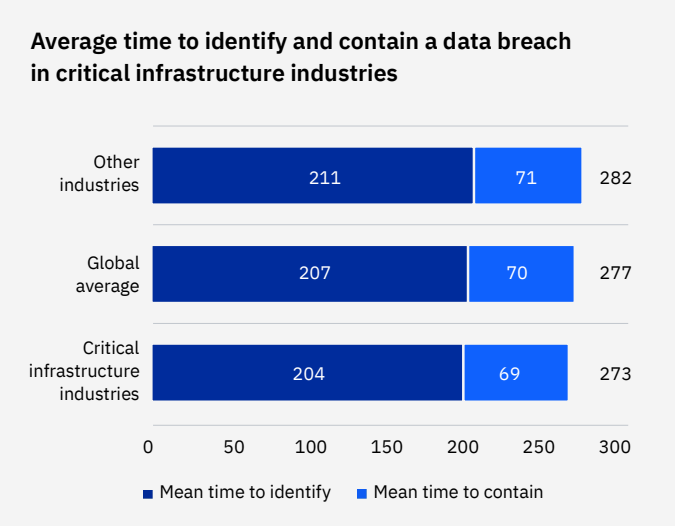


Figure 38: Measured in days

Figure 39: Only one-fifth of critical infrastructure organizations had deployed a zero trust approach to security — half as many as the overall global average.
Twenty-one percent of critical infrastructure organizations had deployed a zero trust approach, while 79% had not. That percentage compares to the overall global average of 41% of organizations with a zero trust strategy.

Figure 40: Organizations in critical infrastructure industries that implemented a zero trust approach to security had an average cost of a data breach of USD 4.23 million.
At those critical infrastructure organizations that didn't deploy a zero trust approach, the average cost of a breach was USD 5.40 million. The result was a difference of USD 1.17 million, or 24.3%, more than those that did implement a zero trust strategy.

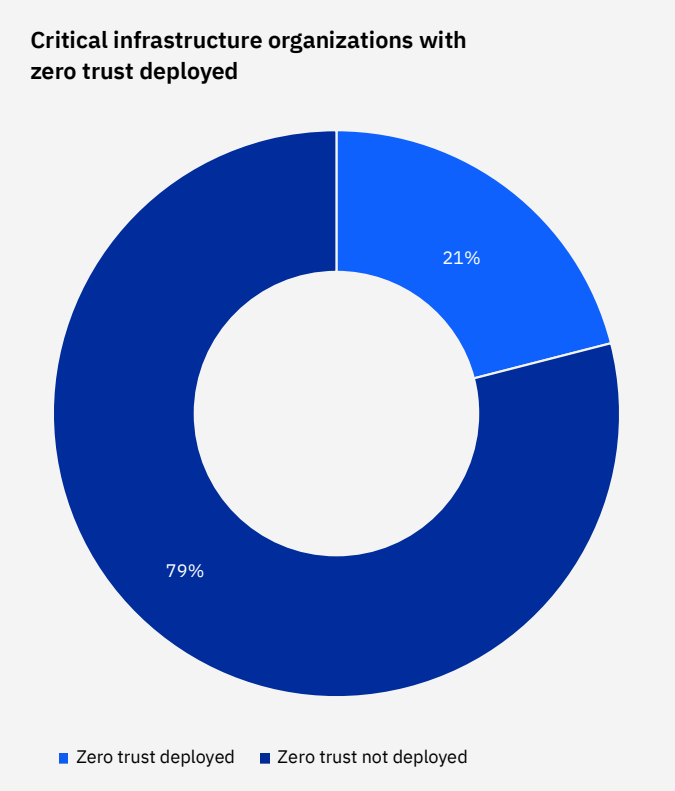


Figure 39

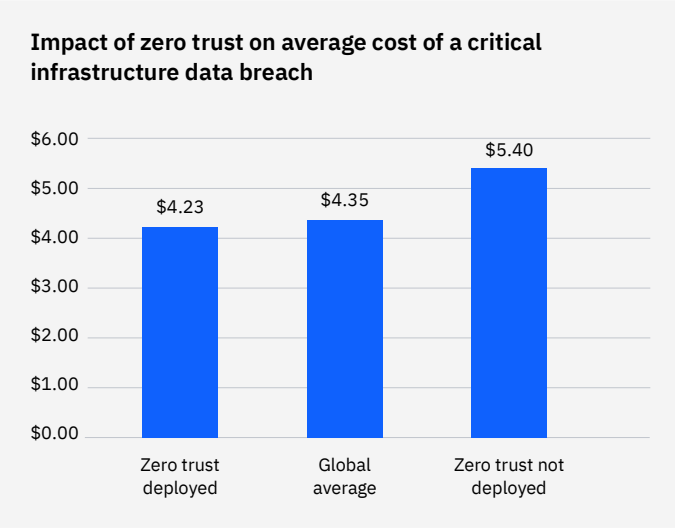


Figure 40: Measured in USD millions

43%

Share of organizations that were in early stages or had not started applying security practices to safeguard their cloud environments

Cloud breaches and cloud model

For a second year in this report, we've taken a close look at the impact of cloud model and maturity of cloud security on the cost of a data breach. The research found that 45% of breaches occurred in the cloud, but those in the public cloud cost considerably more than breaches at organizations with a hybrid cloud model. However, analysis of the research also shows that organizations still need a mature cloud security posture, regardless of cloud model.

Figure 41: A plurality of study participants had a hybrid cloud IT operating model, with 45% indicating they had a hybrid cloud model.
Meanwhile, 28% said their IT model was fully on-premises, and 27% said their IT model was completely cloud-based.

Figure 42: Nearly half of organizations experienced a data breach in the cloud.
Forty-five percent said the data breach occurred in the cloud, whereas 55% said the data breach didn't occur in the cloud.

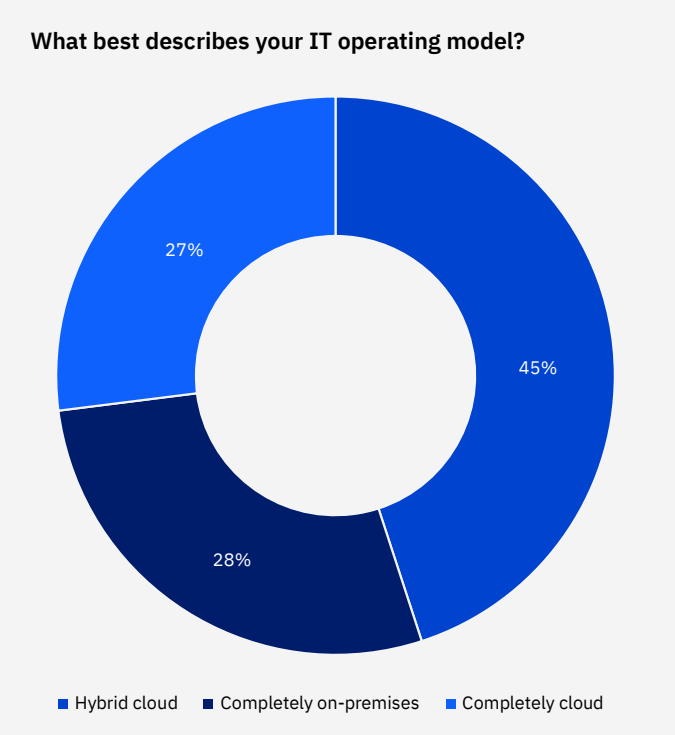


Figure 41

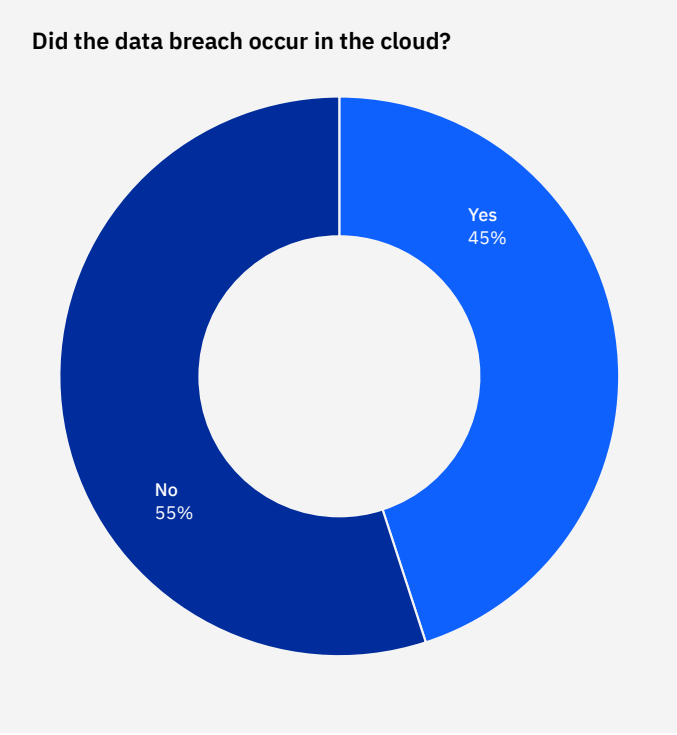


Figure 42

State of security maturity in the cloud environment

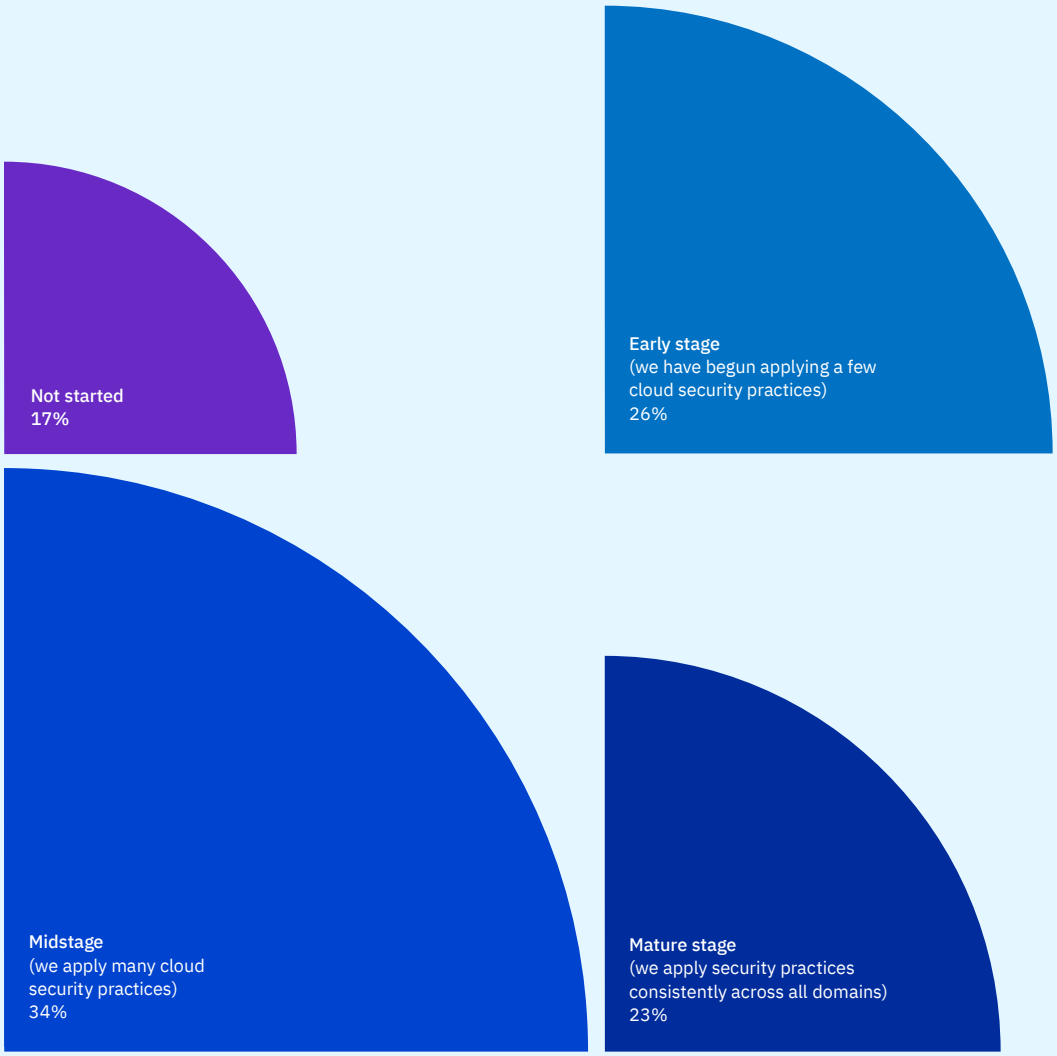


Figure 43

Figure 43: Nearly half, or 43%, of organizations had not started or were in early stages of applying practices to secure their cloud environments.
Meanwhile, 34% were at the midstage and were applying many cloud security practices, and 23% were in the mature stage and were applying security practices consistently across all domains. Another 26% of organizations said that they were in the early stage, meaning that they had begun applying a few cloud security practices. Finally, 17% of organizations said that they had not started their journey in securing their cloud environments.

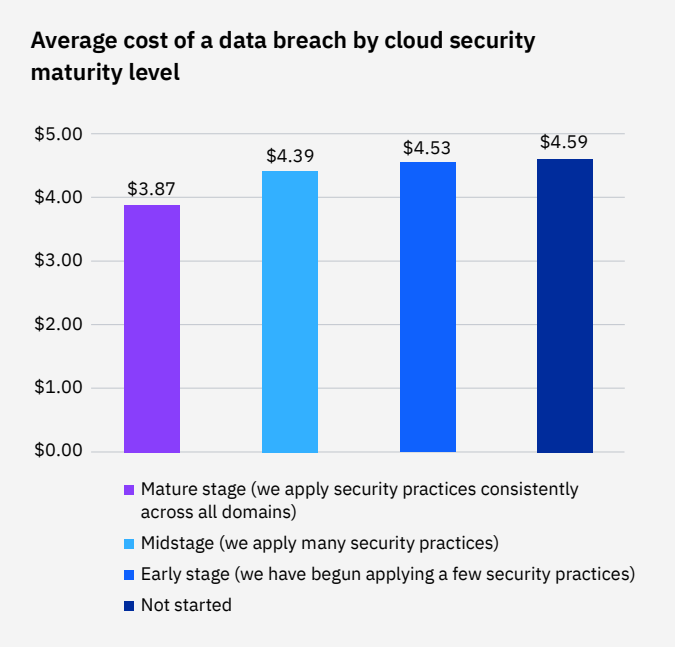


Figure 44: Measured in USD millions

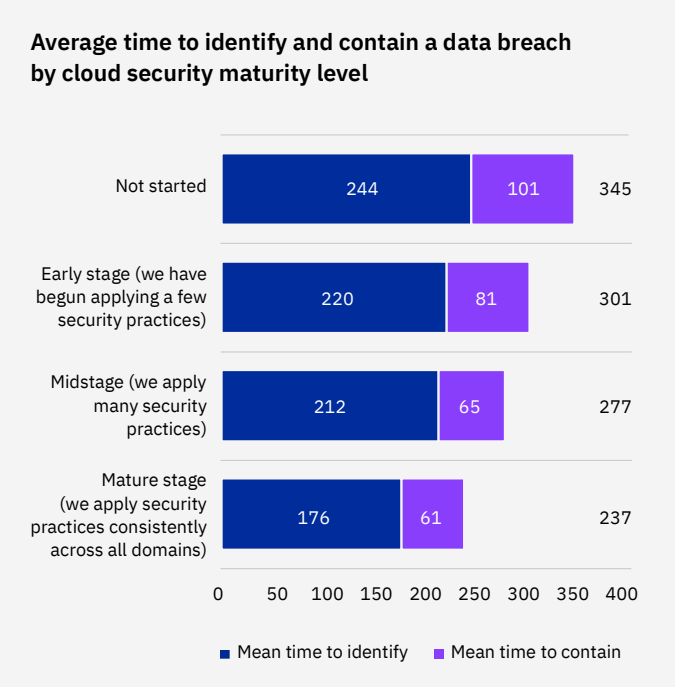


Figure 45: Measured in days

Figure 44: Organizations with mature cloud security had a lower-than-average cost of a data breach.
At mature organizations, breach costs were on average USD 0.66 million less than organizations in the early stages of securing their cloud environments. Breaches at mature-stage organizations cost an average of USD 3.87 million, compared to USD 4.39 million at midstage organizations, USD 4.53 million at early-stage organizations and USD 4.59 million at organizations that had not started their cloud security journey. The cost difference between mature stage and early stage represented a 15.7% savings for mature stage organizations. Note: Breach costs in this analysis refer to any type of breach, not just cloud-based breaches.

Figure 45: Organizations in the mature stage of securing their cloud environments were able to identify and contain the data breach much more quickly than organizations in the early stage.
Mature stage organizations took an average of 176 days to identify and 61 days to contain a breach, or 237 days combined. This lifecycle was 40 days less than the global average of 277 days and 64 days less than early-stage organizations — more than two months, or a 23.8% difference. Those organizations who had not started their cloud security journey took much longer to identify and contain the breach. The average for those organizations was 345 days, more than 100 days longer than mature-stage organizations. For midstage organizations, the average time to identify and contain the data breach was 277 days, the same as the overall global average.

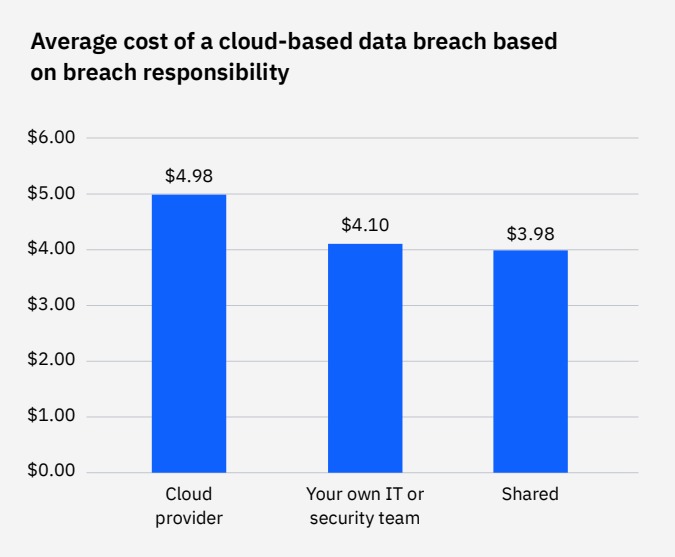


Figure 46: Measured in USD millions

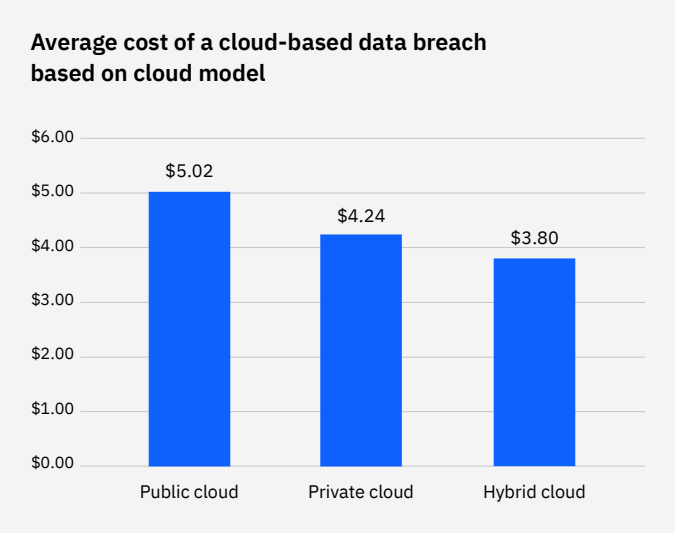


Figure 47: Measured in USD millions

Figure 46: Breaches that were deemed the responsibility of the cloud provider had the highest average total cost of a breach based on cloud provider.
Breaches that were the responsibility of the cloud provider had an average total cost of USD 4.98 million. Breaches deemed the responsibility of the organization's own IT or security team cost an average of USD 4.10 million. Those breaches that were the shared responsibility of the cloud provider and the organization's IT or security team cost an average of USD 3.98 million. This shared responsibility average cost is USD 1 million less than for those breaches where the cloud provider had responsibility, a difference of 22.3%.

Figure 47: Breaches in the public cloud were costliest.
Breaches in a public cloud cost an average USD 5.02 million, whereas breaches within a private cloud cost an average USD 4.24 million. Within a hybrid cloud model, breaches cost an average USD 3.80 million, about USD 1.2 million less costly than breaches within a public cloud, for a difference of 27.7%.

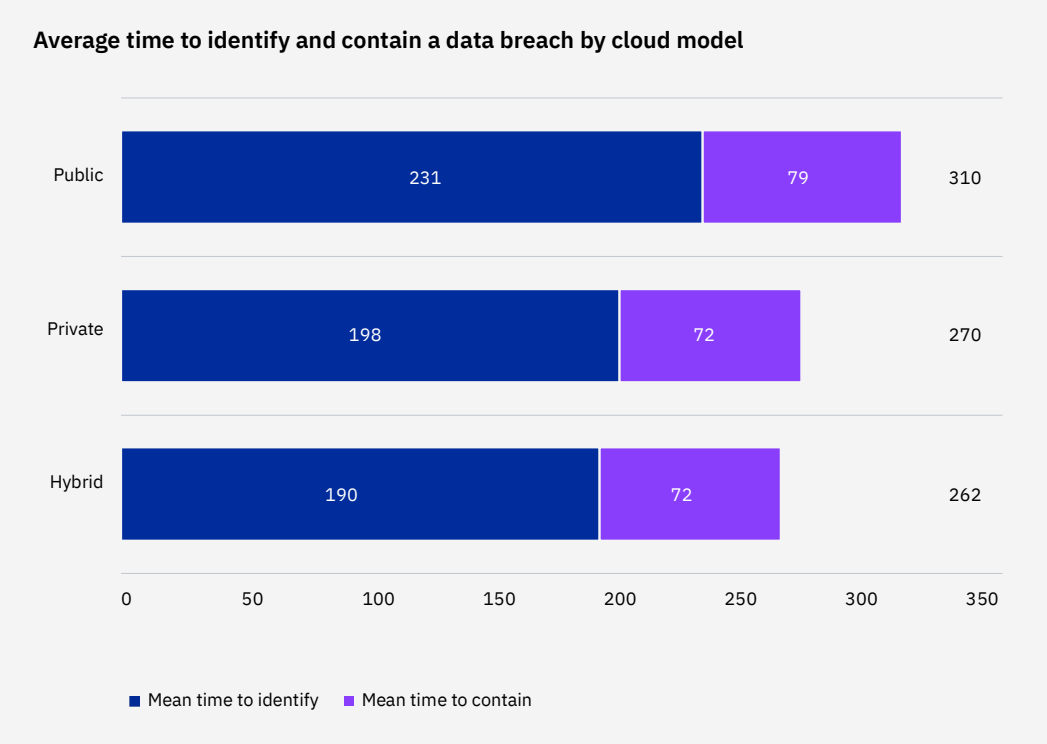


Figure 48: Measured in days

Figure 48: Organizations with a hybrid cloud model were able to identify and contain a breach significantly faster on average than those with public or private cloud models.
The average time to identify and contain a breach with a hybrid cloud model was 262 days. This lifecycle was 15 days less than the global average of 277 days and eight days less than private cloud. Breaches at organizations with a public cloud model took an average of 310 days to identify and contain the breach. This lifecycle was 48 days longer than hybrid cloud, or a difference of 16.8%. Note: Since hybrid cloud implementations vary, this analysis included on-premises breaches, not just purely cloud-based breaches.

USD 1 million

Breach costs where remote working was a factor in causing the breach were about USD 1 million more than breaches where remote work wasn't a factor

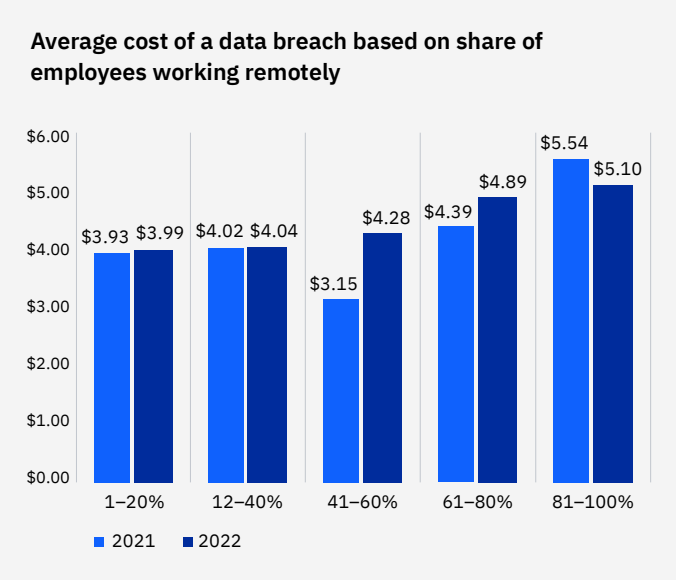


Figure 49: Measured in USD millions

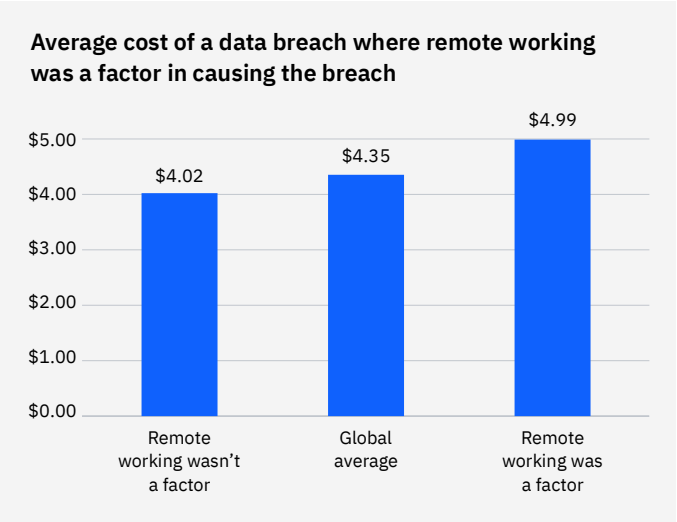


Figure 50: Measured in USD millions

Remote work

This is the third time this report has been published since the start of the COVID-19 pandemic. In the context of the pandemic, starting with last year's report, we've examined the impacts of work-from-home arrangements on data breach costs. Remote working has had considerable effects on the cost of a breach when remote work was a factor in causing the breach, such as a remote-working employee having credentials stolen. The study also found that breach costs were highest for organizations with most of their employees working remotely.

Figure 49: There was a strong correlation between remote working and cost of a data breach, where more employees working remotely was associated with higher data breach costs.
For those organizations with the largest share of employees working remotely — 81% to 100% — the average cost of a data breach was USD 5.10 million. That cost was a slight decrease in this category from last year. For organizations with the smallest share of employees working remotely — less than 20% — the average cost was USD 3.99 million. The difference between highest and lowest share of employees working remotely was USD 1.11 million, a difference of 24.4%.

Figure 50: The average total cost of a data breach was nearly USD 1 million greater when remote work was a factor in causing the data breach.
Organizations that indicated remote work was a factor in the breach experienced an average cost of a data breach of USD 4.99 million. In contrast, the average cost of a data breach was USD 4.02 million when remote work wasn't a factor in causing the breach, a difference of USD 0.97 million or 21.5%. When remote work was a factor, the cost was also USD 0.64 million more than the overall global average, a difference of 13.7%.

USD 550,000

Average data breach cost savings of a sufficiently staffed organization versus insufficiently staffed

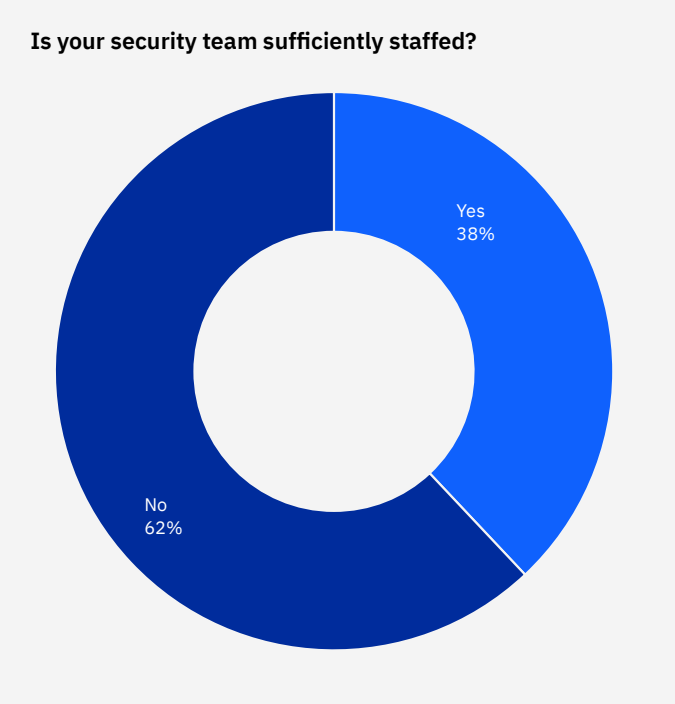


Figure 51

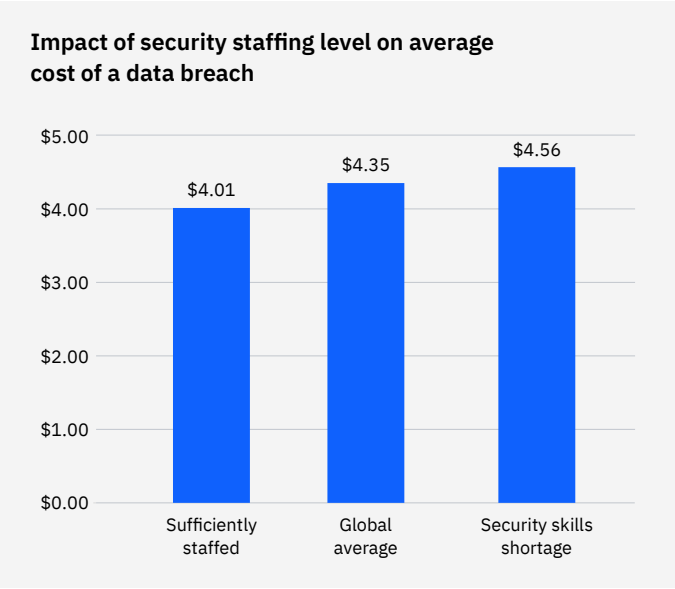


Figure 52: Measured in USD millions

Skills gap

Many organizations struggled to fill positions on their security teams. Those organizations that said they were sufficiently staffed saw considerable cost savings in terms of data breach costs, compared to those without enough employees to staff their teams. This was the first year of this report that we took a deeper look at the security skills gap.

Figure 51: There was a widespread security skills shortage among organizations in the study.
Only a little more than one-third of organizations had sufficiently staffed security teams. Just 38% of organizations said their security teams were sufficiently staffed to meet their security management needs, while 62% said they weren't sufficiently staffed.

Figure 52: Organizations that said their security teams had a skills shortage had a higher-than-average cost of the data breach.
At organizations with a sufficiently staffed security team, the average cost of a data breach was lower than average. The average cost of a data breach at sufficiently staffed organizations was USD 4.01 million. In contrast, the average cost of a data breach was USD 4.56 million at organizations with insufficiently staffed security teams, a difference of USD 0.55 million, or 12.8%.

USD 387 million

Average total cost for breaches of 50 million to 60 million records

Mega breaches

Mega breaches — those with more than 1 million compromised records — aren't normal experiences for most businesses. But mega breaches have an outsized impact on consumers and industries.

This study included 13 companies that experienced a data breach involving the loss or theft of 1 million to 60 million records. The study of the mega breaches involved a distinct methodology from the other 550 breaches in this study, each of which had no more than 102,000 lost records. For a full explanation of the research methodology, see the "Data breach FAQ" at the end of this report.

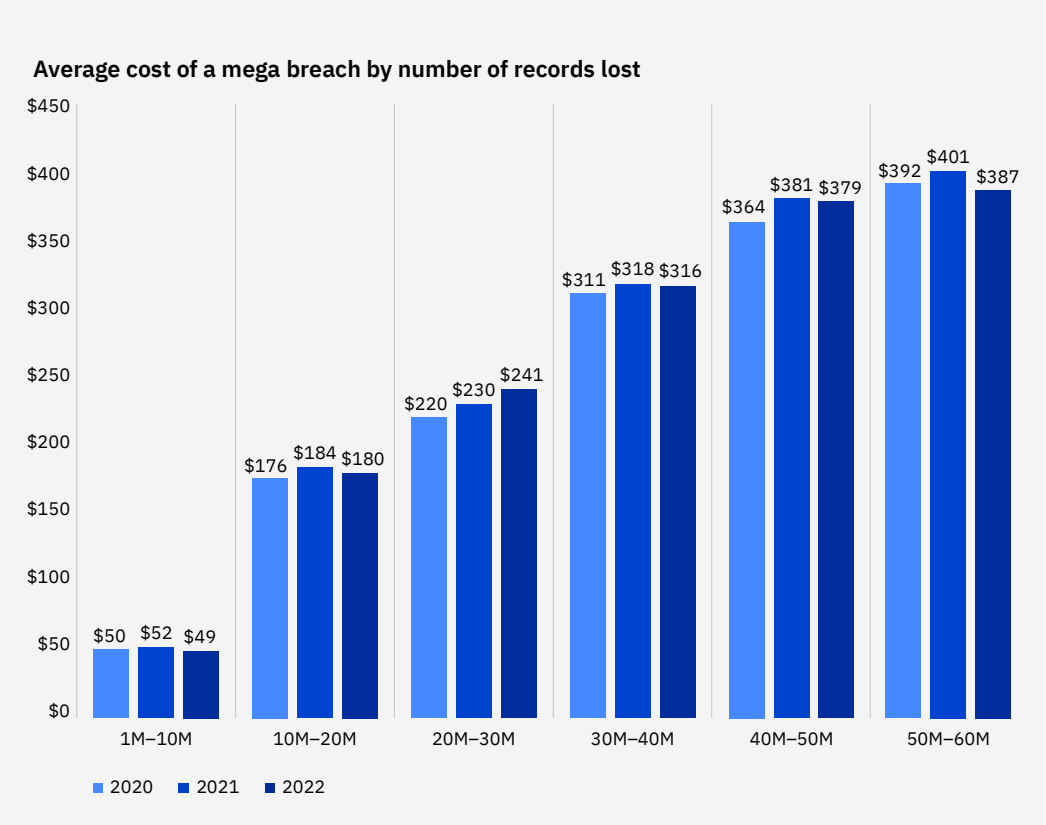


Figure 53: Measured in USD millions

Figure 53: In 2022, the average cost of a mega breach decreased slightly.
Mega breach costs saw a decrease from 2021 in six of seven breach size cohorts. The cost of the largest mega breaches of 50 million to 60 million records decreased from USD 401 million in 2021 to USD 387 million, a drop of USD 14 million or 3.6%. The cohort for 20 million to 30 million records was the only cohort where the average increased from last year. In that cohort, the average total cost of a mega breach increased from USD 230 million to USD 241 million, an increase of USD 11 million or 4.8%.