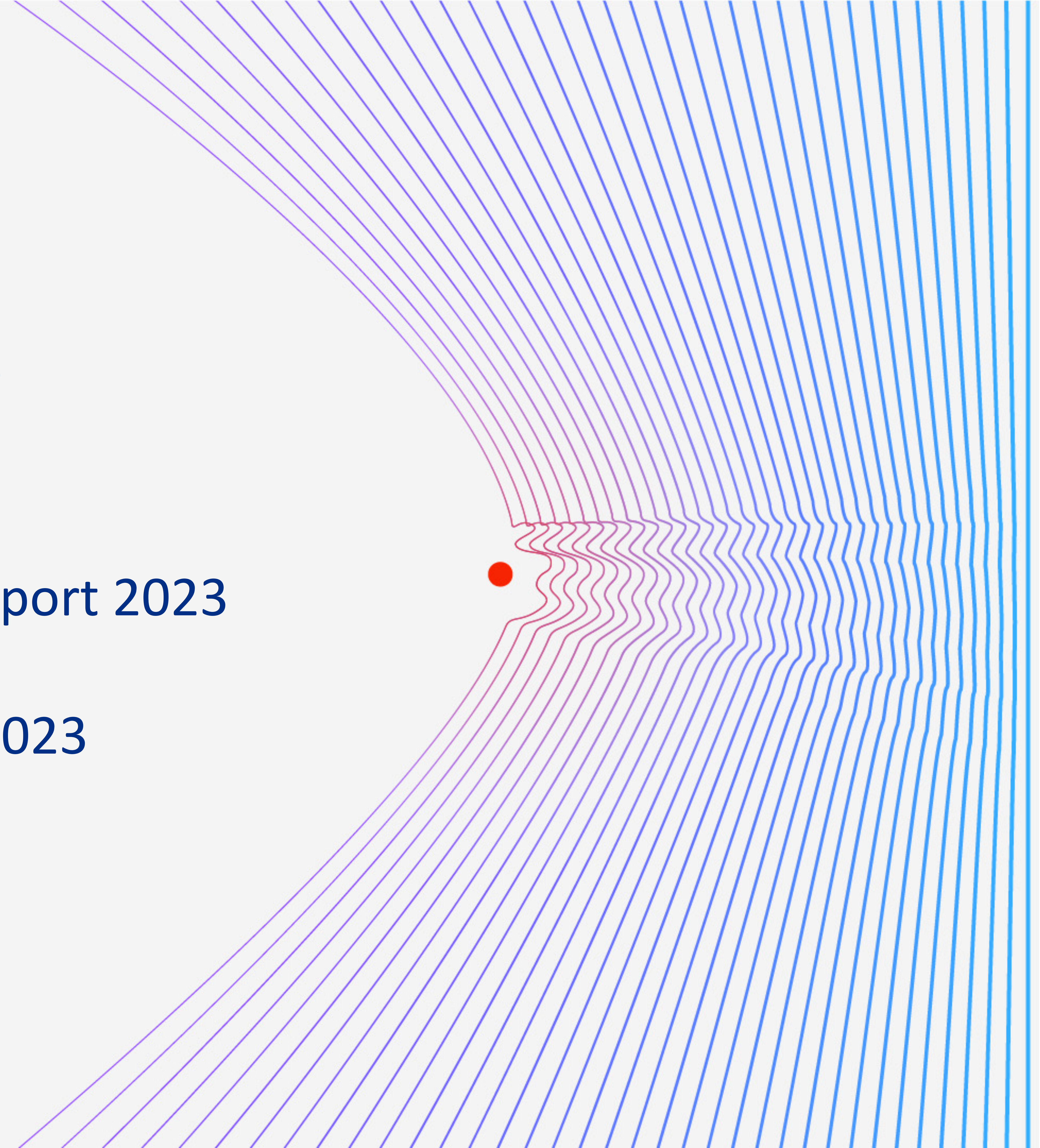
IBM **Security**

Explore Trends to Stay Ahead of Threats:

Cost of a Data Breach Report 2023

IBM X-Force Cloud Threat Landscape Report 2023

IBM X-Force Threat Intelligence Index 2023



Who is X-Force?

Hacker-driven offense. Research-driven defense. Intel-driven protection.

X-Force Red

- Vulnerability & attack surface management
- Penetration testing
- Adversary simulation
- Application security testing

X-Force Incident Response (IR)

- IR preparedness services
- 24x7x365 emergency IR support
- Threat hunting
- Cyber range simulated experiences

X-Force Threat Intelligence

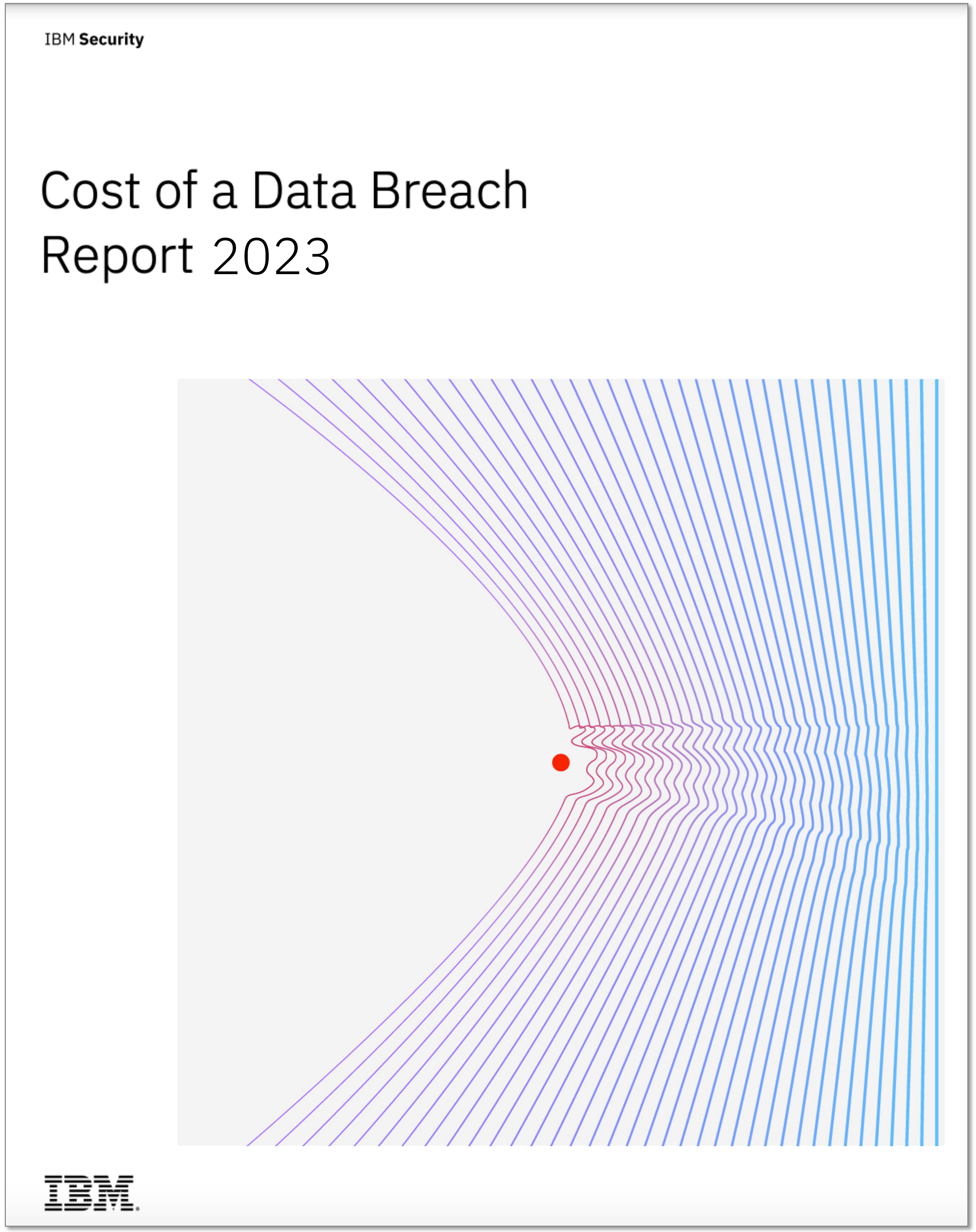
- Threat intel insights, sharing platform
- Threat program assessments
- Dark web analysis
- Malware reverse engineering

Report Overview

Offers a detailed investigation of factors that influence financial impacts to organizations. Organizations can learn what security measures can mitigate costs.

- ✓ Proprietary research
- ✓ 3,600+ interviews
- ✓ 550+ breaches analyzed
- ✓ 16 countries/regions
- ✓ 17 industries
- ✓ 18th year

Who is this report for? All business leaders concerned with protecting the organizations finances, reputation, customer data and privacy, as well as limiting risk and managing compliance.



IBM Security

Cost of a Data Breach Report 2023

IBM

Average cost of a data breach

Reached an all-time high of USD 4.45M

Increased by 15% in the last 3 years

Total cost of a data breach

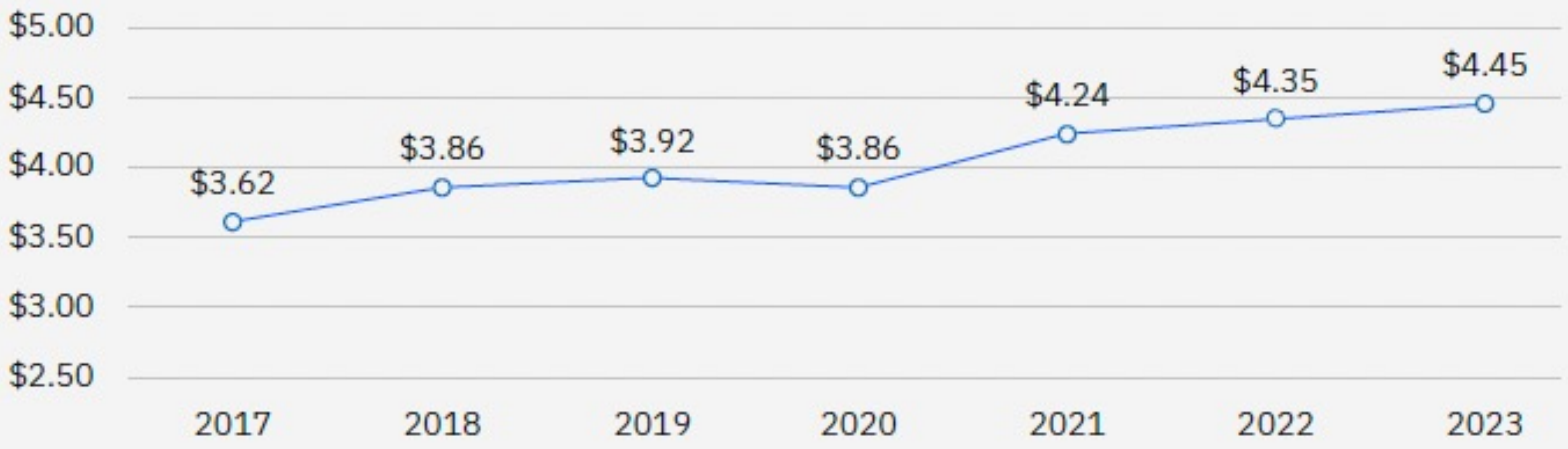


Figure 1. Measured in USD millions

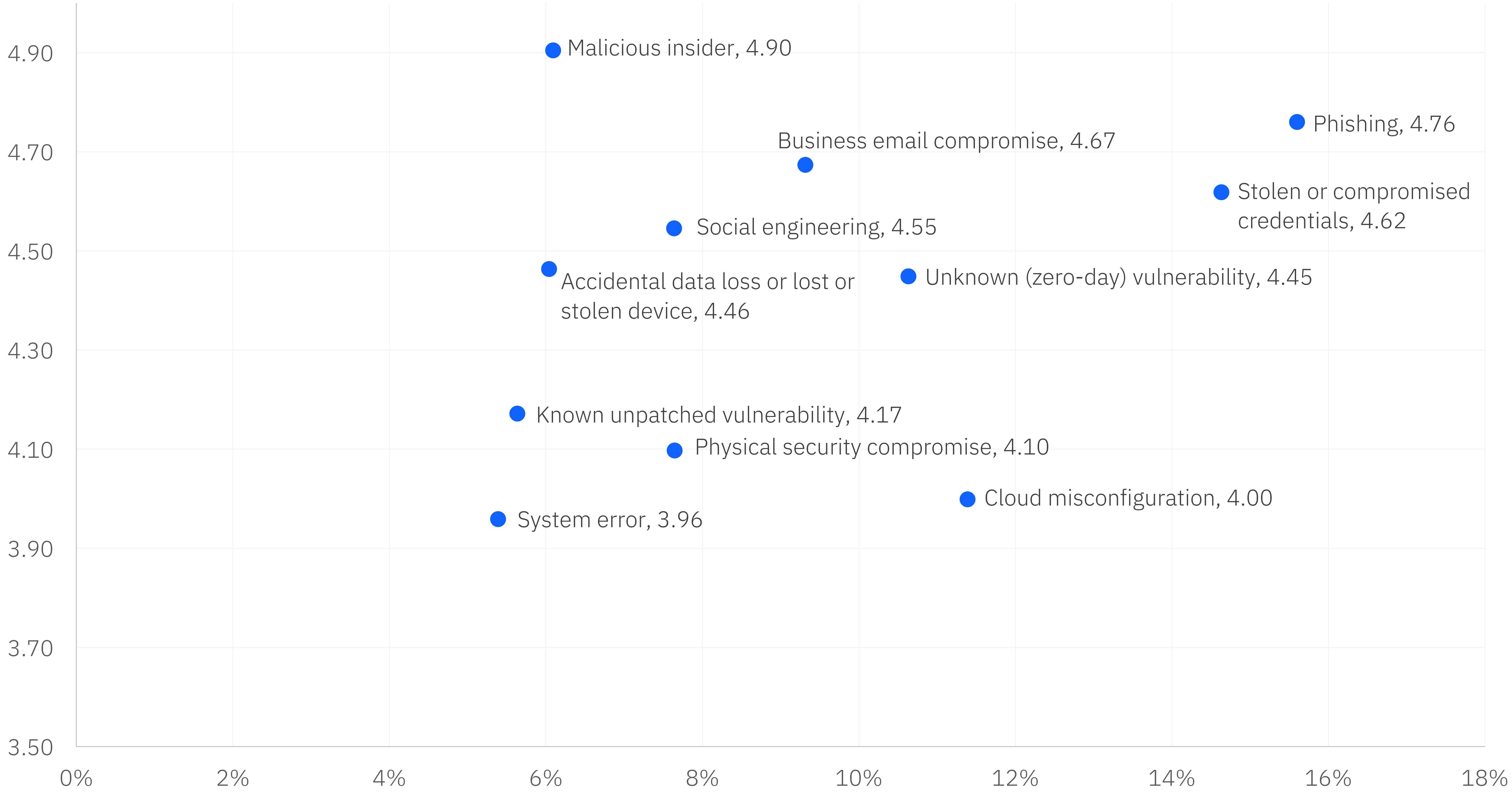
Industries ranked by cost

1. Healthcare – USD 10.93 million
2. Financial – USD 5.90 million
3. Pharmaceuticals – USD 4.82 million
4. Energy – USD 4.78 million (+1)
5. Industrial – USD 4.73 million (+2)
6. Technology – USD 4.66 million (-2)
7. Services – USD 4.47 million (-1)
8. Transportation – USD 4.18 million (+5)
9. Communications – USD 3.90 million (+3)
10. Consumer – USD 3.80 million (-1)
11. Education – USD 3.65 million (-1)
12. Research – USD 3.63 million (-4)
13. Entertainment – USD 3.62 million (-2)
14. Media – USD 3.58 million (+1)
15. Hospitality – USD 3.36 million (+1)
16. Retail – USD 2.96 million (-2)
17. Public sector – USD 2.60 million

- Avg breach cost increased YtY
- Average breach cost decreased YtY
- +/- indicates movement of rank

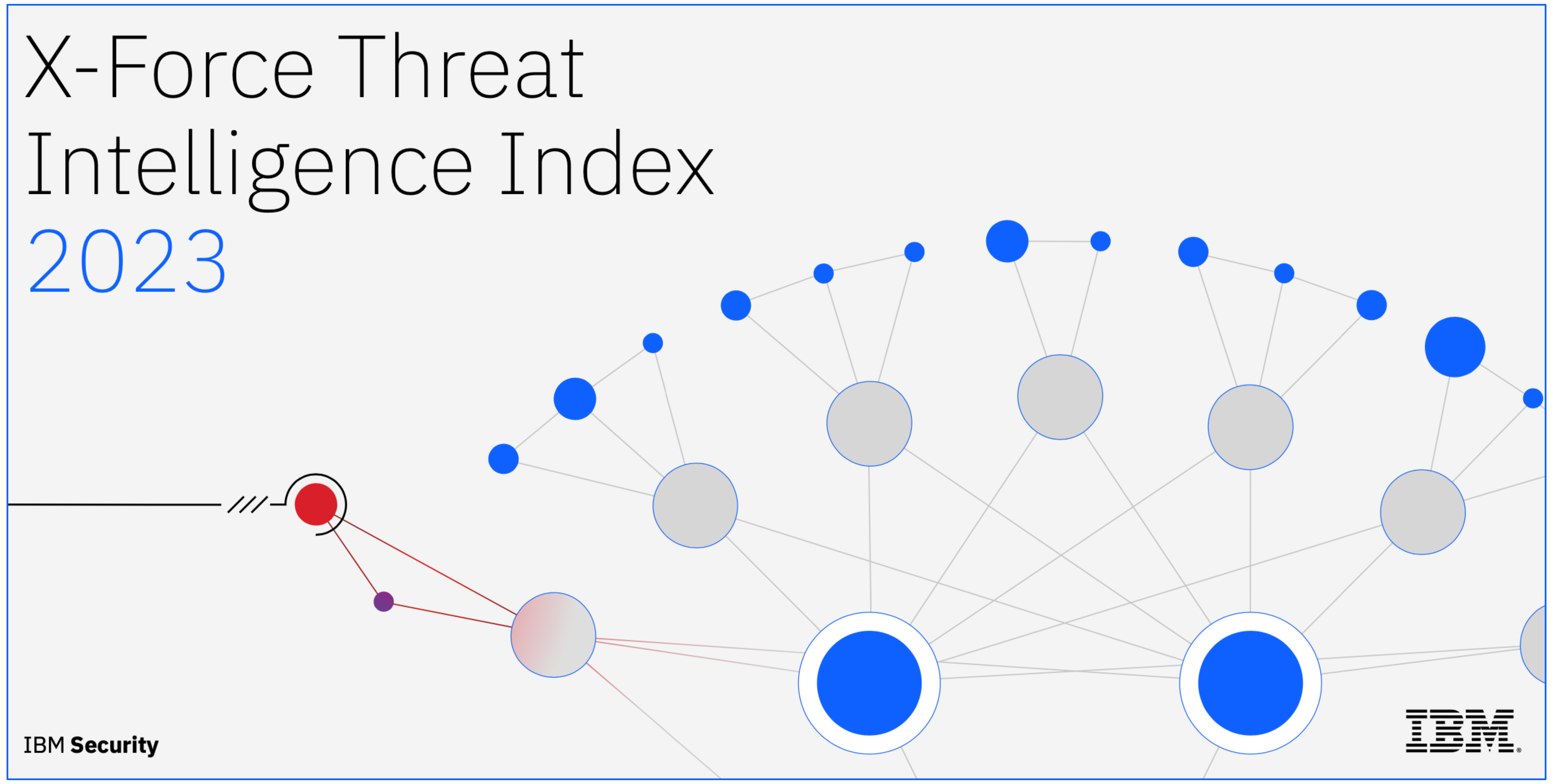
Average cost and frequency of data breaches by initial attack vector

USD millions



Report Overview

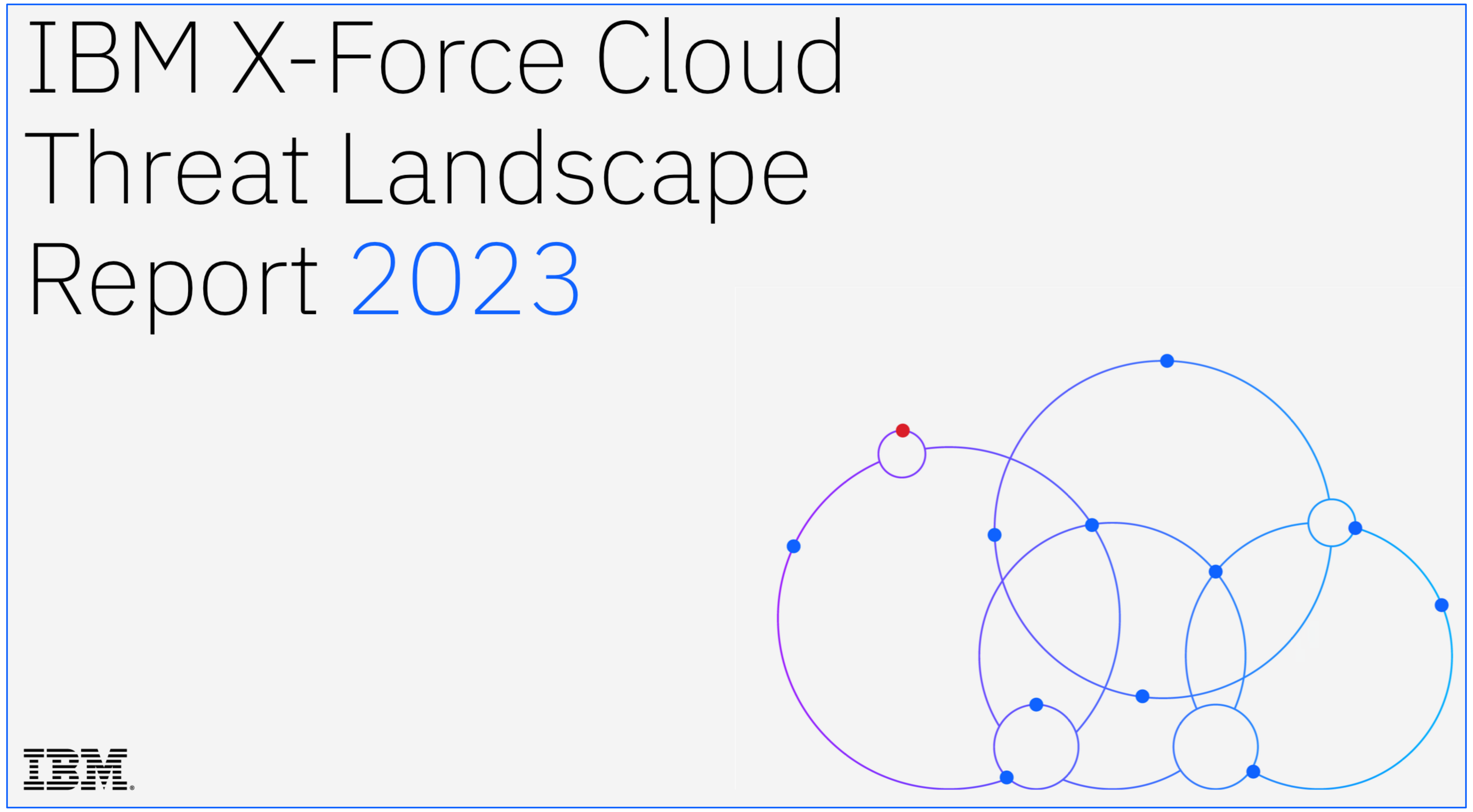
IBM Security X-Force Threat Intelligence Index tracks new and existing trends and attack patterns and includes billions of datapoints ranging from network and endpoint devices, incident response (IR) engagements, vulnerability and exploit databases and more.



X-Force Threat Intelligence Index 2023

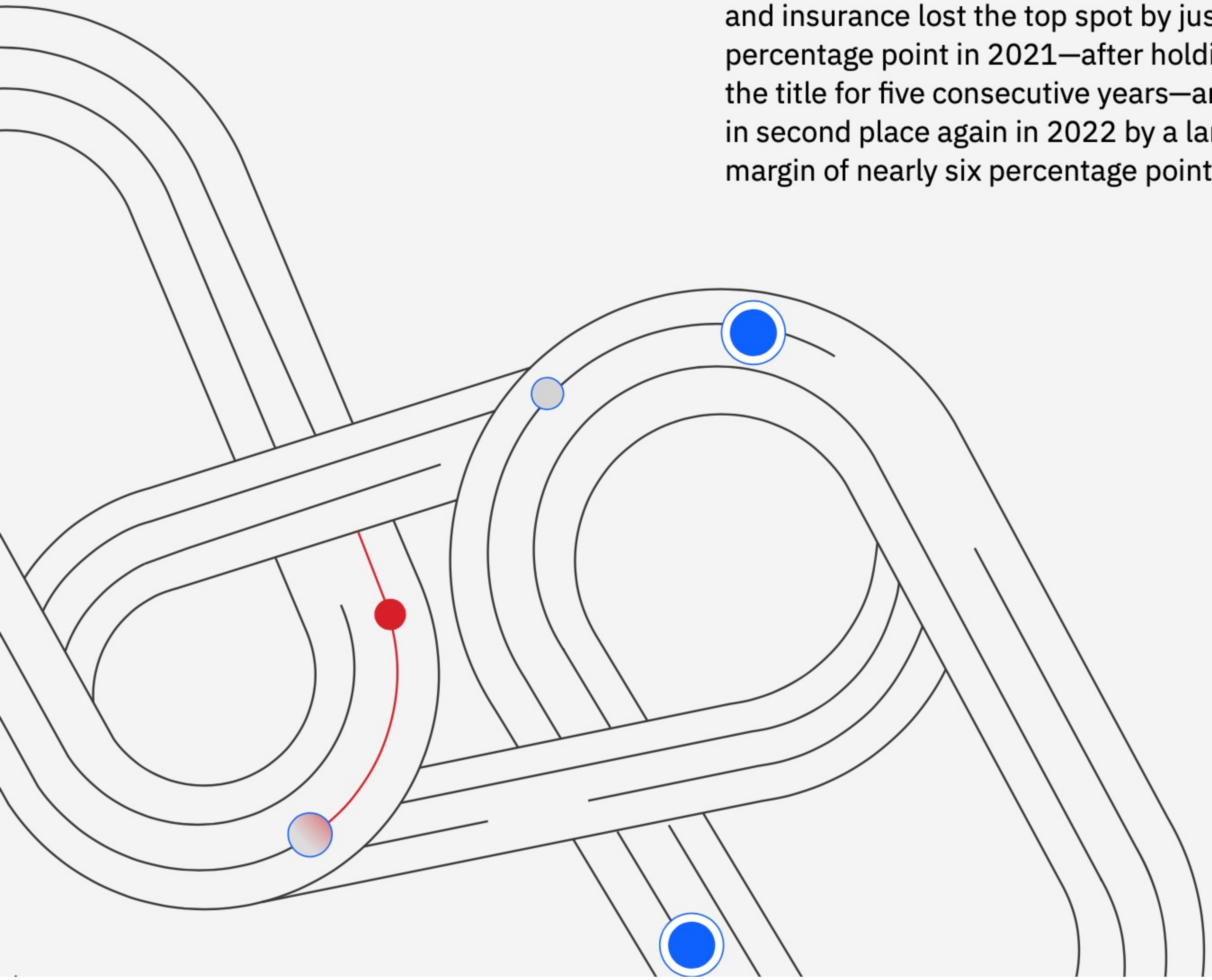
IBM Security

IBM X-Force Cloud Threat Landscape Report aids clients and the broader community with their cloud security strategy. Our findings reveal the various ways we've observed threat actors compromising cloud environments and the types of malicious activities they pursue when inside.



IBM X-Force Cloud Threat Landscape Report 2023

Industry trends



For the second year in a row, manufacturing was the top-attacked industry, according to X-Force incident response data. Finance and insurance lost the top spot by just one percentage point in 2021—after holding the title for five consecutive years—and is in second place again in 2022 by a larger margin of nearly six percentage points.

Share of attacks by industry 2018 – 2022

Industry	**2022**	**2021**	**2020**	**2019**	**2018**
Manufacturing	24.8%	23.2	17.7	8	10
Finance and insurance	18.9%	22.4	23	17	19
Professional, business and consumer services	14.6%	12.7	8.7	10	12
Energy	10.7%	8.2	11.1	6	6
Retail and wholesale	8.7%	7.3	10.2	16	11
Education	7.3%	2.8	4	8	6
Healthcare	5.8%	5.1	6.6	3	6
Government	4.8%	2.8	7.9	8	8
Transportation	3.9%	4	5.1	13	13
Media and telecom	0.5%	2.5	5.7	10	8

41%

Percentage of incidents involving phishing for initial access

Phishing operations continued to be the top pathway to compromise in 2022, with 41% of incidents remediated by X-Force using this technique to gain initial access.

100%

Increase in the number of thread hijacking attempts per month

There were twice as many thread hijacking attempts per month in 2022, compared to 2021 data. Spam email leading to Emotet, Qakbot and IcedID made heavy use of thread hijacking.

52%

Drop in reported phishing kits seeking credit card data

Almost every phishing kit analyzed in the data sought to gather names at 98% and email addresses at 73%, followed by home addresses at 66% and passwords at 58%. Credit card information, targeted 61% of the time in 2021, fell out of favor for threat actors—data shows it was sought in only 29% of phishing kits in 2022, a 52% decline.

62%

Percentage of phishing attacks using spear phishing attachments

Attackers preferred weaponized attachments, deployed by themselves or in combination with links or spear phishing via service.

26%

Share of 2022 vulnerabilities with known exploits

Twenty-six percent of 2022's vulnerabilities had known exploits. According to data that X-Force has tracked since the early 1990s, that proportion has been dropping in recent years, showcasing the benefit of a well-maintained patch management process.

31%

Share of global attacks that targeted the Asia-Pacific region

Asia-Pacific retained the top spot as the most-attacked region in 2022, accounting for 31% of all incidents. This statistic represents a five percentage point increase from the total share of attacks to which X-Force responded in the region in 2021.

Cloud Threat Landscape Report

Key takeaways

Misuse of legitimate credentials plagues the cloud landscape

- IR data indicates that the use of valid credentials was the most common initial access vector in cloud security incidents, occurring in 36% of cases.
- The X-Force team discovered plaintext credentials located on user endpoints in 33% of engagements involving cloud environments.

Container security concerns are on the rise

- The X-Force Red team reported a large uptick in custom resource definition use in organizations' Kubernetes clusters, which can become security concerns if implemented poorly or without the appropriate level of security-inclusive development processes.

Vulnerabilities are increasingly being discovered and disclosed

- The X-Force team tracked 632 new cloud-related common vulnerabilities and exposures (CVEs) during the reporting period. This number is a 194% increase from the prior year.

The impact felt by the exploitation of these CVEs is varied

- Just over 40% of the CVEs discovered during the reporting period could allow an attacker to either obtain information (21%) or gain access (20%).

Cloud is still a hot commodity on the dark web

- Credentials comprised nearly 90% of cloud assets for sale on the dark web during the reporting period.
- The average price for these credentials was USD 10.68, representing a slight decrease from the previous reporting period.

194%

increase of new cloud-related CVEs from the prior year

IBM