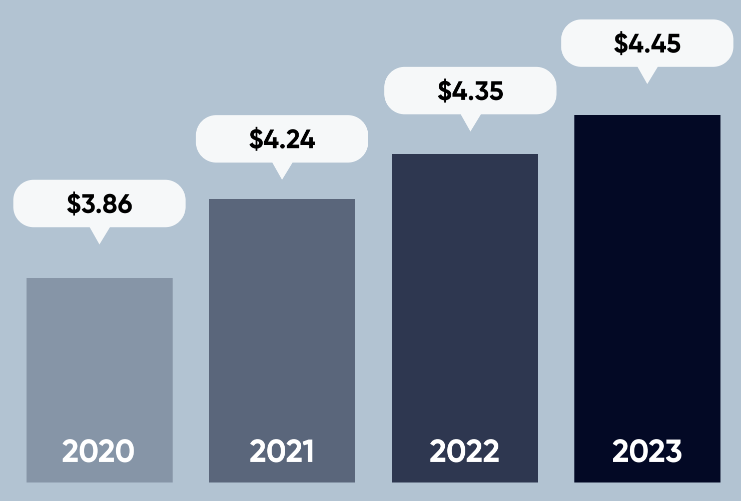
IBM REPORT
KEY FINDINGS

BRANDEFENSE LOOK

AVERAGE TOTAL COST



15.3% increase over **3years**

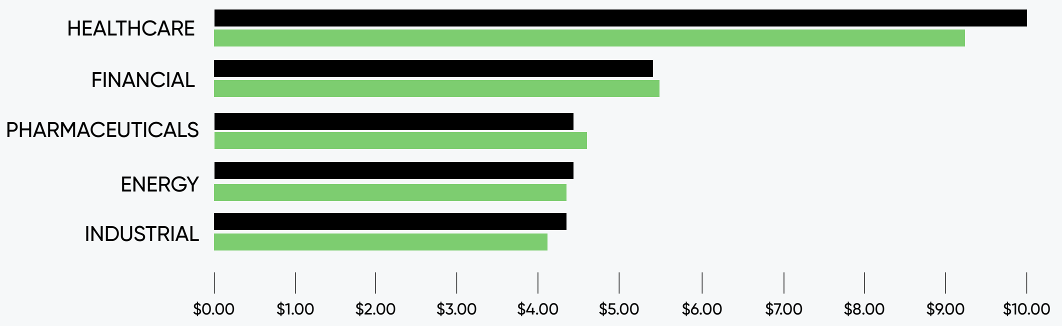
This year's average total cost is USD 4.45M, which is the highest cost all the time.

SECTORS and COUNTRIES-REGIONS

Compared to the 2022 and 2023 reports, in the top 5 countries-regions list, there is only one change.

2022	2023
United States	United States
Middle East	Middle East
Canada	Canada
Germany	United Kingdom
Japan	Germany

According to the report, this year UK's data breach costs decreased. Japan is also has decreased as far as last year but they are still in this year's top 5 list.



When we talk about industries, *"healthcare"* is still first. After started COVID-19, the healthcare industry crashed by cyber-attacks and these attacks caused the highest data breach costs 13th year in a row.

AVERAGE DATA BREACH LIFE CYCLE and HOW to DECREASE IT?

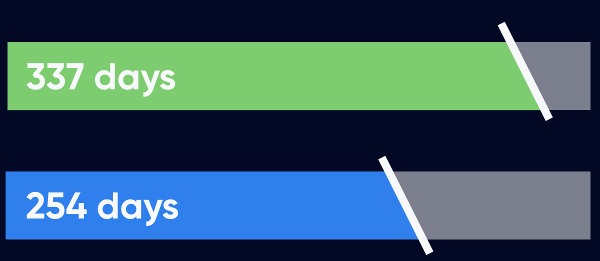
277 days The overall time to identify and contain a data breach is 277 days.

51% of companies that are part of this research have indicated they increased their security investment.

According to their statements, their top three security will be

- IR Planning and Testing
- Employee Training
- Threat Detection and Response Technologies

Attack Surface Management (ASM)



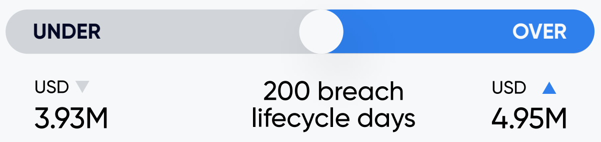
Learn How Brandefense Attack Surface Management Helps You

2.5 months

Without ASM solutions, identifying and containing a data breach time is 337 days/11 months. However, they are decreasing this time to 254 days which means the time for identifying a data breach is almost 8,5 months. The time gained for companies is nearly 2.5 months.

DIFFERENCE FROM BREACH LIFECYCLE EQUALS 1.02 M

Breach lifecycle explains as time to identify and contain breaches.



DETAILS OF ATTACKS

1 in 3

Only 1/3 of companies can be discovered data breaches with their own security teams, but they also say that they need better threat detection.

TOP INITIAL
ATTACK VECTORS

PHISHING

Phishing is responsible for 16% of data breaches in the 2023 report, and this put phishing attacks first place. Also, it is the second most expensive attack vector. The phishing attacks' total cost is USD 4.76 million. For phishing attacks mean time to identify and contain a data breach is 293 days, or we can say it takes about 10 months.

- **USD 4.76 million**
- **293 days**
- **10 months**

STOLEN CREDENTIALS

Second initial attack vector for the data breach report is stolen or compromised credentials. It has 15% of breaches. One of the highest times for identifying and containing a data breach belongs to stolen or compromised credentials. It takes 308 days / 10 months.

- **308 days**
- **10 months**

O-DAYS

Regarding zero-day vulnerabilities, the report has explained that this attack vector took part in this research for the first time. 0-day vulnerabilities cost USD 4.45 million in 2023. It takes 272 days to identify and contain breaches.

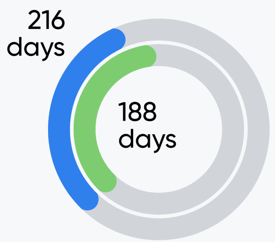
- **USD 4.45 million**
- **272 days**

BUSINESS E-MAIL COMPROMISE

This attack vector has %9 of data breaches' causes and USD 4.67 million.

- **USD 4.67 million**

DETAILS OF ATTACKS



Using threat intelligence services decrease identified breach time by 28 days.

Threat intelligence services decrease the average cost by almost **USD 197K**

Learn How Brandefense Threat Intelligence Solution Helps You

brandefense.io

BRANDEFENSE