



# Data Breach: Only a matter of time.

PROTECT YOUR COMPANY'S  
ASSETS WITH APARAVI®



# Data Breach: Only a matter of time.

The damage caused by data theft is increasing dramatically.

## Initial situation: It happens to the best of organizations.

Continental, Facebook, Caritas, Marriott Hotels, HiPP – the list is growing all the time. Together, these companies lost 1.3 billion data sets over the past 4 years. In most cases, personal data was stolen and sold on the darknet.

The costs are enormous, not only for the organization itself. In addition to the high fines imposed for GDPR violations, it is the costs for recovery and restoration that really hurt. At the same time, the impacted customers also pay a high price – with their sensitive data and the fatal consequences that may follow when it is passed on.

### When your nightmares come true

A scenario that gives IT managers and management boards sleepless nights: Cyber criminals manage to hack into the IT infrastructure. Or a key member of staff leaves their notebook or smartphone containing unencrypted data on the public transport. What then – simply hope that the data breach will blow over? But according to an old proverb, hope is the meadow where fools graze. At APARAVI, we are realistic.

**That is why we advise you to get prepared in case disaster strikes – with a well-conceived strategy and digital tools.**

4.35  
MILLION



4.35 Million euros is the average cost of a data breach according to an IBM study from 2022\*

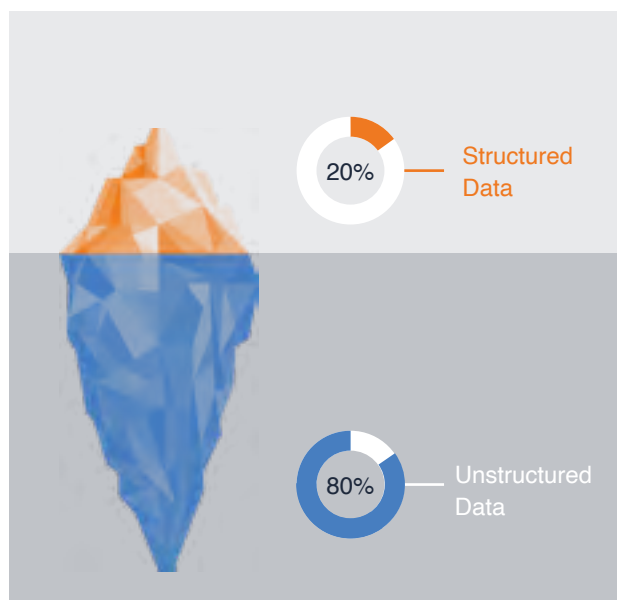
# Data Breach: Only a matter of time.

80 Percent – the great unknown.

## The challenge: Rampant growth in unstructured data

Most data theft involves information in Office files, PDFs, images, emails, CAD and many other file formats. In the meanwhile, the systems of a typical organization are crammed with these kinds of files. Most of these are unused, useless and unknown.

Remarkably, 80 percent of your data is unstructured. And the proportion is growing steadily. It is precisely this unstructured data which makes life easy for attackers when a breach occurs. They gain extensive access to sensitive data distributed across numerous file storage systems - on-premises and cloud-based - and various locations.



## Let's first take a moment to define a data breach more exactly.

A breach is a security event in which unauthorized persons copy, transmit, view, steal or use sensitive, protected or confidential data.

### Breaches mostly result from:

- Data leaks
- Malware und ransomware
- Phishing / Spear-phishing
- Zero-day attacks
- Stolen access credentials
- Social Engineering
- Unencrypted hardware in wrong hands

# Data Breach: Only a matter of time.

No matter how big or small:  
Everyone is at risk.



## The case of Continental. Lessons learned?


**What happened, and when?** In July 2022, the DAX-listed company Continental fell victim to a cyberattack by the RaaS gang Lockbit. An employee had downloaded an unauthorized web browser onto his laptop and provided a gateway for hackers to gain access to Continental's data swamp. For four long weeks, the hackers were able to forage unnoticed through sensitive data and tap it off.

A small mistake which could cost up to 4% of the company's global turnover in regulatory fines – for Continental well over 1 billion euros!

**Which data was involved?** In total, the hackers were able to loot 40 TB of corporate data, including extensive information about investments, customers, suppliers & partners, personal information about employees, strategy plans, confidential documents and the threads of chats between board executives – the list is long. So long, in fact, that it took the company four months to get an overview of its own data.

The total package was then put up for sale on the darknet for the "bargain price" of only 50 million euros.

4



### What does this mean for you?

Not if, but when: Every company, regardless of its size, turnover or supposedly well-organized IT security can fall victim to a criminal cyberattack. One false click is enough to allow the hackers undetected access to all your company's data.



# Data Breach: Only a matter of time.

Your response needs to be rapid AND accurate.



## Reacting quickly to a data breach

Speed of response is of paramount importance following a data breach! The longer those impacted remain unaware that their sensitive data has been stolen, the more severe the repercussions of a data breach are likely to be. When a breach occurs, it is not only essential to respond quickly, but also

accurately. Once the compromised data has been identified, organizations have to establish how critical the information is and how much sensitive data has leaked out of the company. Achieving precision is incredibly time-consuming, as examining and categorizing the data can very often only be carried out manually by experts.

3  
DAYS



Organizations are only given three days to inform the relevant authorities of a data breach and to document how they plan to remedy the situation.

5

**APARAVI** recommends

### Develop a strategy!

You can prepare your organization for the day you experience a data breach. Avert more substantial damage to you, your employees, your customers and your partners! As experts in unstructured data, we take a holistic approach to counteracting data privacy violations with preventive and emergency remedial measures.

# Data Breach: Only a matter of time.

The holy grail:  
The General Data Protection Regulation.



The 3 most important questions about the GDPR

A computer monitor displaying a warning icon (an orange triangle with a white exclamation mark) and the text "DSGVO". A curved arrow points from the icon towards the right.

**Reduce your GDPR risks**  
Find out more on our website:

# Data Breach: Only a matter of time.

Your worst case scenario has come true: You have been hacked.



To prove it, the hackers have sent you a file with excerpts of your data. Don't panic – firstly, you need to check whether the data included in the hacker file is indeed yours. To achieve this, you are definitely going to need the right software, which is able to match the data quickly and precisely. This provides you with a basis for deciding whether the breach needs to be reported to the authorities.

## Preparation is everything: Emergency assistance and prevention for data breaches.

- **Data protectors and data security auditors are aware that all organizations are at risk:** It all depends on the quality of your preventive and remedial measures!
- **Maintain a good overview of your data at all times:** Taking stock of your data comprehensively on a regular basis helps you determine within 72 hours whether YOUR data has really been stolen (duty to report!).
- **The challenge is to be quick and accurate:** The sooner you analyze the compromised data pool, the earlier you can notify the authorities and inform impacted customers and suppliers.

# Data Breach: Only a matter of time.

A holistic approach  
to data breaches.



## Solution: Immediate remediation and prevention powered by APARAVI

Our platform helps you gain a clearer understanding of data breaches which have occurred, minimize their impact quickly and report them as required. This plays a crucial role in avoiding unnecessary harm to impacted data subjects.

And once you have started engaging with this important issue, our combined intelligence and automation technologies can prevent future incidents occurring. Powerful, customizable search options, indexing and classification, rule-based pattern recognition and much more ensures that your stored data remains clean and uncluttered. In this way, we help you avoid the next data breach.

You benefit from two  
fundamental aspects.





# Data Breach: Only a matter of time.

A holistic approach  
to data breaches.



## 1. Rapid, accurate immediate remediation following data breaches

Data theft and especially data privacy violations can cause huge damage and result in enormous costs for your company. They are also extremely unpleasant to deal with. Make sure that you avoid suffering the associated embarrassment or reputational damage. We provide your teams with quick insight into the impacted data, full transparency for all parties concerned and practical assistance with reporting the event.

### In detail this means:

- User-centricity through classification options determined by users (RegEx / regular expressions)
- Rapid identification of users who last accessed the impacted files
- Checking the validity of data sets as a basis for making decisions about subsequent steps
- Required reporting to feed into specific analysis tools
- Simplified notification of authorities through customizable reporting options in the APARAVI cockpit

9

**3x**  
**FASTER**



Fewer than 10 days with APARAVI, compared with the typical 30 days usually taken to find & classify files containing personal data and generate accurate reports (Case study global business consultancy).

# Data Breach: Only a matter of time.

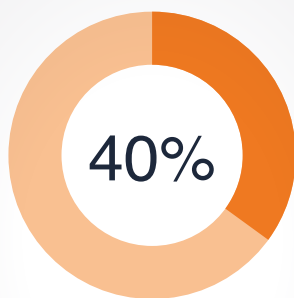
A holistic approach  
to data breaches.



## 2. Targeted prevention of data breaches

“Prepping” in advance of a digital disaster? This might sound strange to some. Still, it is better to be overly cautious in advance of a data breach than suffer from a massive loss of trust, reputation and money as a result of one. With a cleansed data pool, you also directly reduce your costs for storage space, power, backup and administrator efforts.

### SAVINGS



Proactive data management enables you to save up to 40% on your costs for storage and computational capacity – while effectively safeguarding your company’s valuable assets.

### How APARAVI helps you avoid the worst case:

- Taking stock of your data professionally on a regular basis ensures your data remains low-risk and clean. This allows you to analyze compromised data sets more quickly and accurately, while also reducing regulatory fines by proving the implementation of extensive TOM.
- Continual scanning of all your data for duplicates and other ROT data, which may serve as gateways into your network
- Automated deletion processes for these duplicates to avoid unnecessary, time-intensive analysis of duplicate data sets following breaches
- Daily high-speed scanning of your data including details about the storage location, name, signature, creation or modification dates of the files, etc.
- Rule-based data pattern recognition, which helps minimize the risk of data breaches at an early stage. Applicable for personal data, intellectual property such as source code, or business and trade secrets such as CAD formats.
- Reporting for purposes of comparison and potential recognition of data patterns

# Data Breach: Only a matter of time.

PROTECT YOUR COMPANY'S  
ASSETS WITH APARAVI.



## Better protection for what you value.

Are you aiming to establish a strategic approach for combatting data theft and ensuring a clean pool of data – and are you looking for an automated solution?

**Let's talk about it! Set up your individual appointment with APARAVI's data security experts.**

Phone: [+49 \(0\)89 5404 3992](tel:+49(0)8954043992)

Email: [sales.eu@aparavi.com](mailto:sales.eu@aparavi.com)