APARAVI®

Automate your data forensics

FOR IT INVESTIGATIONS WHICH DELIVER RESULTS TODAY, RATHER THAN TOMORROW

Automate your data forensics

IT forensics on the march

Initial situation: Fighting for light in the darkness of the data swamp

Unstructured data poses problems for all those fighting on the “light side of the force” – investigators combatting organized crime, finance controllers, companies in their fight against money laundering and sexual harassment, as well as data protection officers. Finding, comprehending and processing unstructured data poses considerable difficulties for them. This is where data forensics comes into play. The need for intelligent, automated software logic which can accomplish this essential task is growing ever bigger.

What is the problem with having unstructured data?

In brief: There is just too much of it. Unstructured data makes up 80 percent of all data stored at companies. And it proliferates rapidly. At the same time, it is like a black box – nobody knows what it contains. It may be content or metadata from private or business documents, contract PDFs, lists of financial results, CVs, ID photos or work chat threads on a private smartphone. All this unstructured data provides a convenient gateway for cybercriminals.

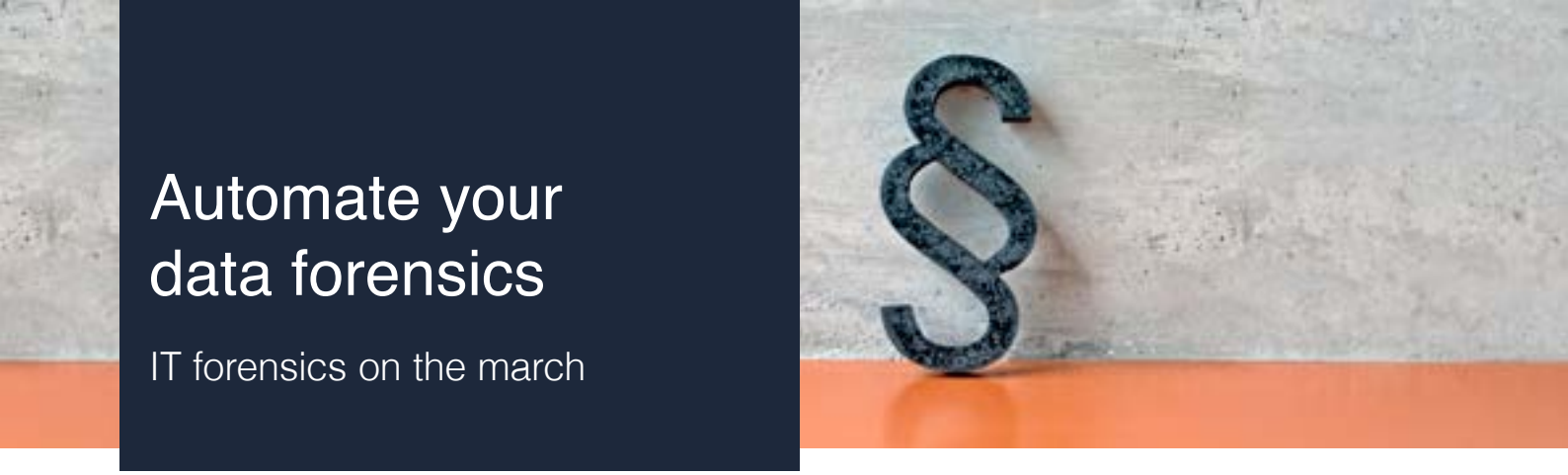
Alright, but how bad can it really be? Here are some key figures:

350%

CYBERCRIME

+350 Percent Rise in incidents of cybercrime around the globe since 2007. Causing 225 billion euros in financial damage*

Source:
**German Federal Criminal Police Office (BKA), Cybercrime - Cases recorded up to 2021*



Automate your data forensics

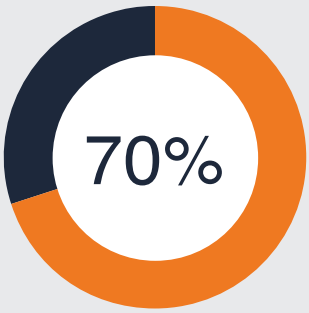
IT forensics on the march

Out of sight, out of mind?

Sticking your head in the sand may work for ostriches, but it will not help you with data breaches. Both known and undetected breaches are on the rise, and they both carry a duty to report. Otherwise, it may become tremendously expensive. Failing to report a data breach yourself within 72 hours could result in a fine of 10 million euros or two percent of the company's global turnover, according to Article 83 paragraph 4 of the GDPR**.

But how can one cope with this requirement?
How can one manage to find the corrupted data in such a short time? Companies, authorities and investigators are being pushed to their limits when searching for the internal and external causes of data breaches – in data sources and storage locations which are usually chaotic and convoluted.

SUCCESSFUL
Attacks



More than 70% of German companies were subject to a successful attack in the past 12 month.

Source:
***https://www.dataguard.de/blog/datenschutzverstoss*

Automate your data forensics

Mission impossible?

The challenge: Recognizing data search as a value proposition – The search for relevant data has become a Sisyphus task

Those involved in IT forensics often experience the identification, gathering and organizing of data as a labor of Sisyphus, the mythical Greek figure whose personal hell consisted of having to shove a heavy stone up a mountain. However, before he could get to the top, the cursed stone would always roll back down into the valley and Sisyphus would have to start all over again.

Combing through Petabytes of data in countless formats, while at the same time bearing any new regulations in mind, is a job requiring a high level of frustration tolerance. Still, if one fails to do it, we all know how costly it can get.

What makes it so difficult?

Finding data in various sources is tricky, time-intensive and unfortunately prone to human error. In huge, decentralized infrastructures, specialized data search & analysis tools are employed – first to ensure that the relevant data is complete and correct, and then to organize it. Here are the five biggest challenges facing IT forensics:

1. **Determining the scope of relevant data**
   The wide variety of the data is especially problematic. Unstructured data does not have a fixed format, originates from innumerable sources, is sometimes physically inaccessible where it is stored, and yet all this data still needs to be examined.

2. **Speed of data processing**
   To recognize potential threats before they cause harm, it is essential to detect data patterns rapidly. Yet it is a huge effort to pick all the required information out of unstructured data. The processing time is heavily dependent on the volume of data and the performance of the servers.

Automate your data forensics

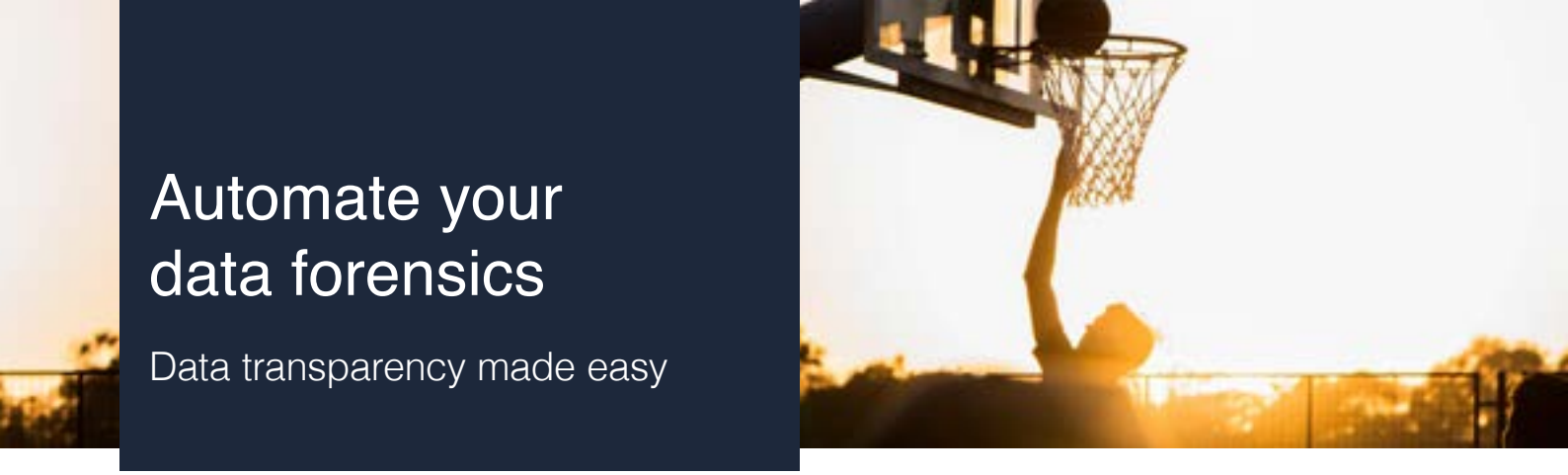
Mission impossible?

3. **Reliability of the data**
   Validating whether all the information gathered from the data is correct is very difficult, but this forms the basis for any case where data forensics is applied. The quality needs to be high, as the results obtained will ultimately have to be legally watertight.

4. **The value of the data**
   It is much more difficult to extract valuable clues from unstructured data than when it is structured. A poorly maintained pool of data also increases the costs of the forensic work.

5. **Risks to forensic data investigations**
   And then there are still the “usual suspects”, which always impede forensic processes: data tampering, compliance guidelines, complex data management and unknown parameters.

Yet there is still hope ...



Automate your data forensics

Data transparency made easy

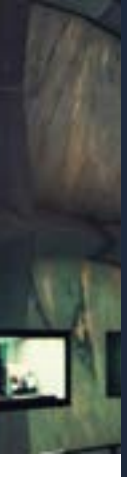
The solution: Automated data forensics with the APARAVI® platform

As you now know, the correct assessment of critical data sets crucially requires that all unstructured data can be found, comprehended and organized. Rely on APARAVI® for your data forensics if you would like to conduct automated, resource-saving, legally compliant data investigation processes.

APARAVI recommends

To conduct a successful data forensics procedure, our experienced data forensics experts advise you follow these tried and tested "first steps":

- **Core Scan** to take stock of the file structure and files, providing you with an initial inventory
- This overview serves as the basis for an **initial assessment** of the collected data and signatures (identifying duplicates to reduce the amount of data)
- **Indexing - Deep Search** for file contents using combinations of over 30 search criteria
- **Classification** - Metadata can be verified according to content aspects by way of 250 predefined and unlimited customer-specific classes



Automate your data forensics

Data transparency made easy

Achieve data transparency faster – here's how

Gain transparency for your own data. This is the first step to taking (back) control over compliance requirements. The key: Analyzing all the data in each relevant file. APARAVI's powerful search tools allow every file to be located and examined – including the entire content and file context – without any language barriers.

5 Major benefits APARAVI® grants your IT forensics

- **Full transparency:** automated search through all stored data, whether on-premises or in the cloud
- **Quick comprehensive overview** by way of the APARAVI® Cockpit, which displays all data including the storage location, in a convenient user interface
- We support over **6,000 file types**
- **Time saved through the deep search engine** which facilitates easier access to distributed data sets and avoids wasting time importing and exporting data
- **Comprehensive, but targeted classification** of all unstructured contents thanks to more than 150 predefined country and sector specific guidelines
- **Faster creation of reports owing to** intuitive Query Builder and filter for generating intelligent, adaptable, all-in-one reports

Automate your data forensics

For IT investigations which deliver results today, rather than tomorrow

Fast and legally compliant!

Would you like your forensic investigations to be automated, legally compliant and re-source-saving, rather than continue rolling rocks up a mountain?

Let our data forensics experts advise you and take the opportunity to put APARAVI® to the test!

Phone: +49 (0)89 5404 3992
Email: sales.eu@aparavi.com

www.aparavi.eu

APARAVI Software Europe GmbH
Lothstrasse 5
80335 München