THALES
Building a future we can all trust

Data Security Fabric

Data Risk Analytics &
Data Risk Intelligence
File Activity Monitoring

www.thalesgroup.com


THALES
Building a future we can all trust
Data Risk Analytics
(DRA)

93%

of enterprises reported an increase in threats

49%

of organizations reported being breached sometime in their history

Source:

Data Breaches are still a HUGE Problem

- During Q1/2023 **6.41 million data records** were leaked in worldwide data breaches
- During 2023 over **353 million individuals were affected** by data compromises
- Data breach is expensive - global average in 2023 - **$4.45 million**
- Data breaches often lead to the loss of customers → **decrease in sales**

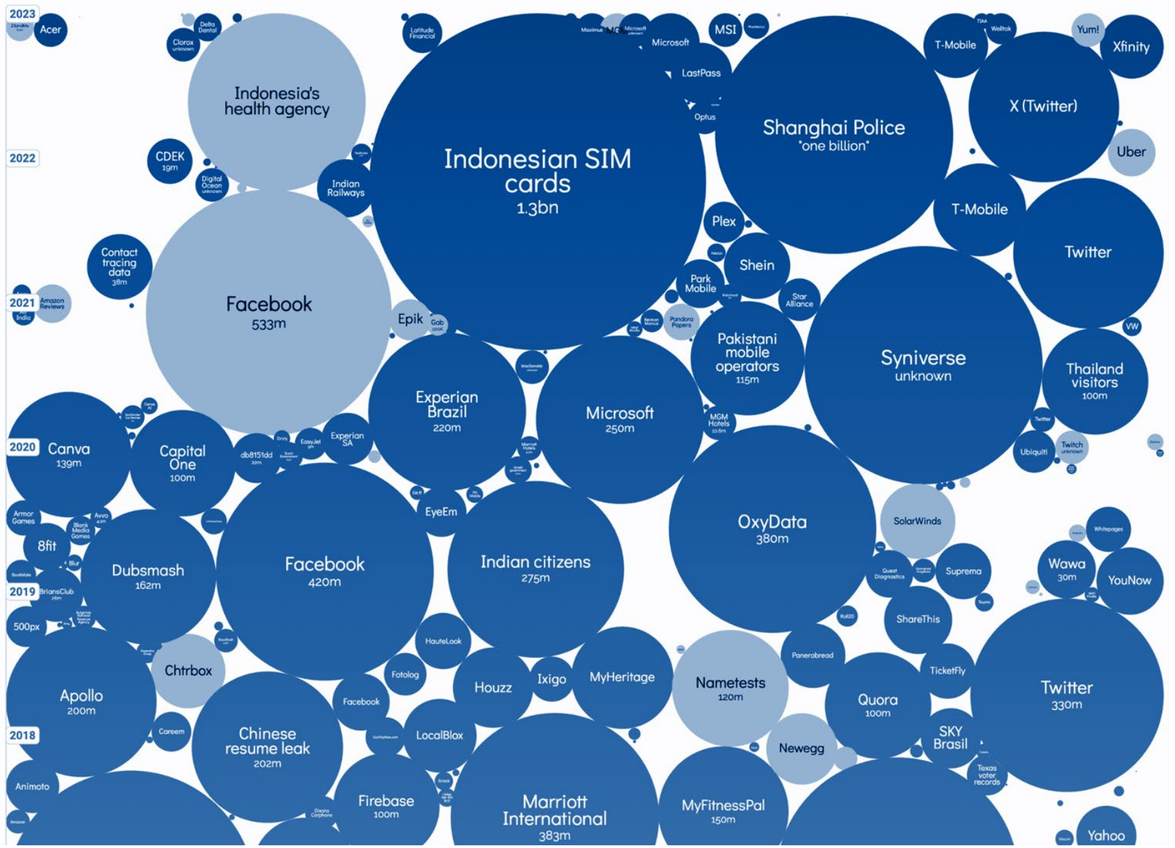
277 DAYS

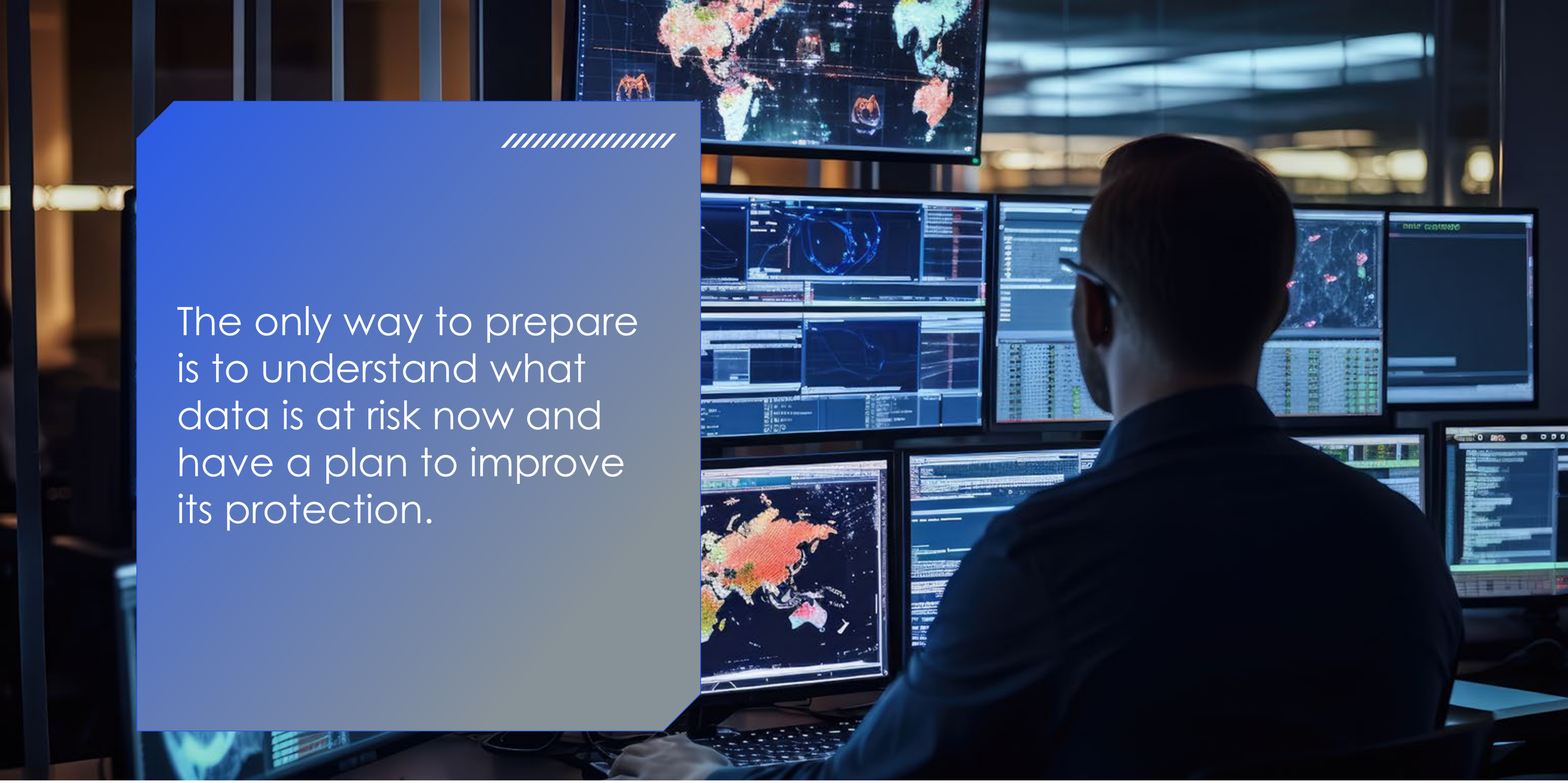
Average days it takes for a breach to be detected and contained

(Ponemon Institute)

World's Biggest Data Breaches & Hacks

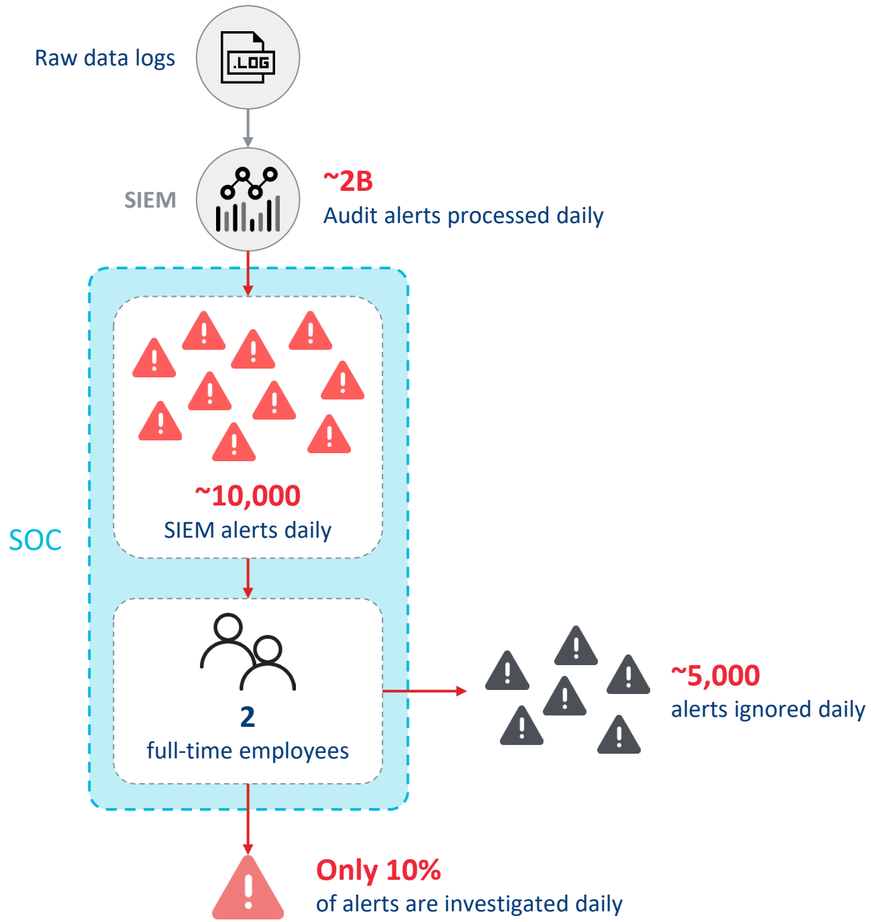
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/





The only way to prepare is to understand what data is at risk now and have a plan to improve its protection.

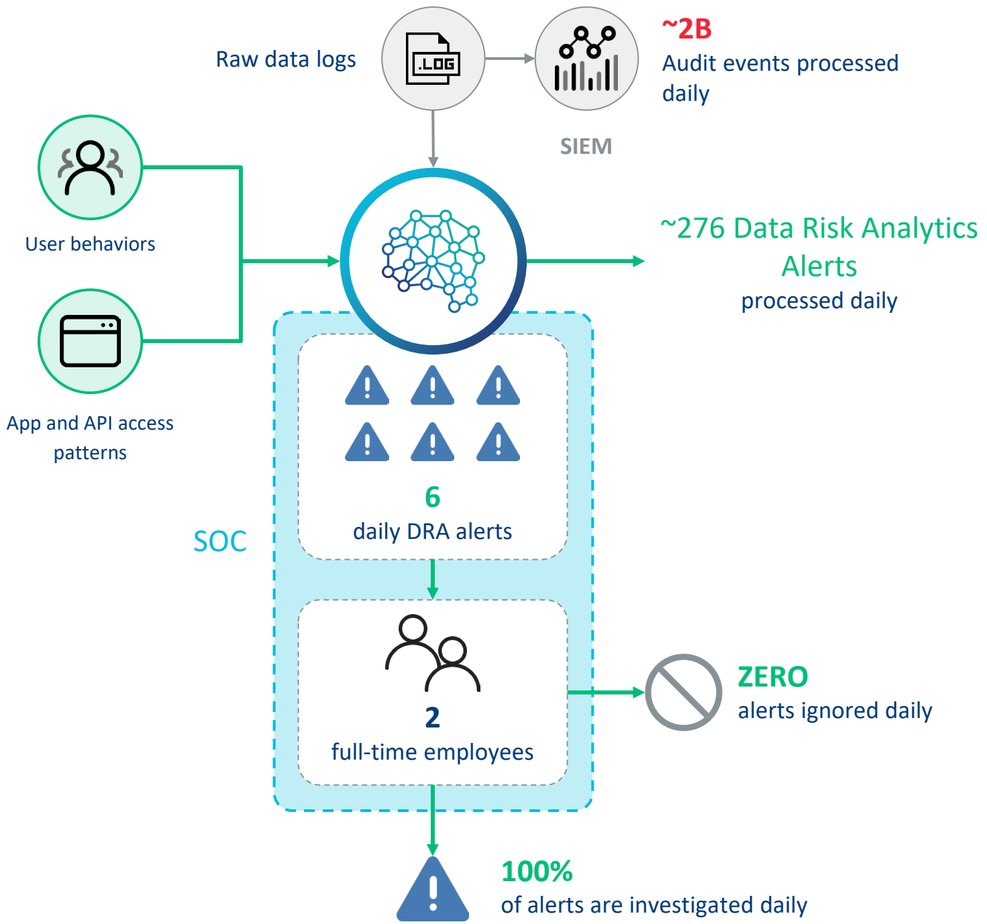
SIEM/UEBA Solutions Don’t Nail It



SOC teams are inundated with unprioritized alerts in cryptic SQL statements

- SOC teams are faced with billions of audit events
- SIEM/UEBA reduce audit events to thousands of alerts - number is still **too high to handle** by security teams
- SIEM/UEBA produces alerts on any abnormal behavior, which is not necessarily a security incidents → **many false positives** - waste of security teams time
- SIEM/UEBA **doesn’t** know how to **identify data related high-risk incidents** (doesn’t understand SQL language, for example) → misses real alerts (many false negatives)
- SIEM/UEBA **alerts are unexplainable** since there is no understanding of the context between data risk events

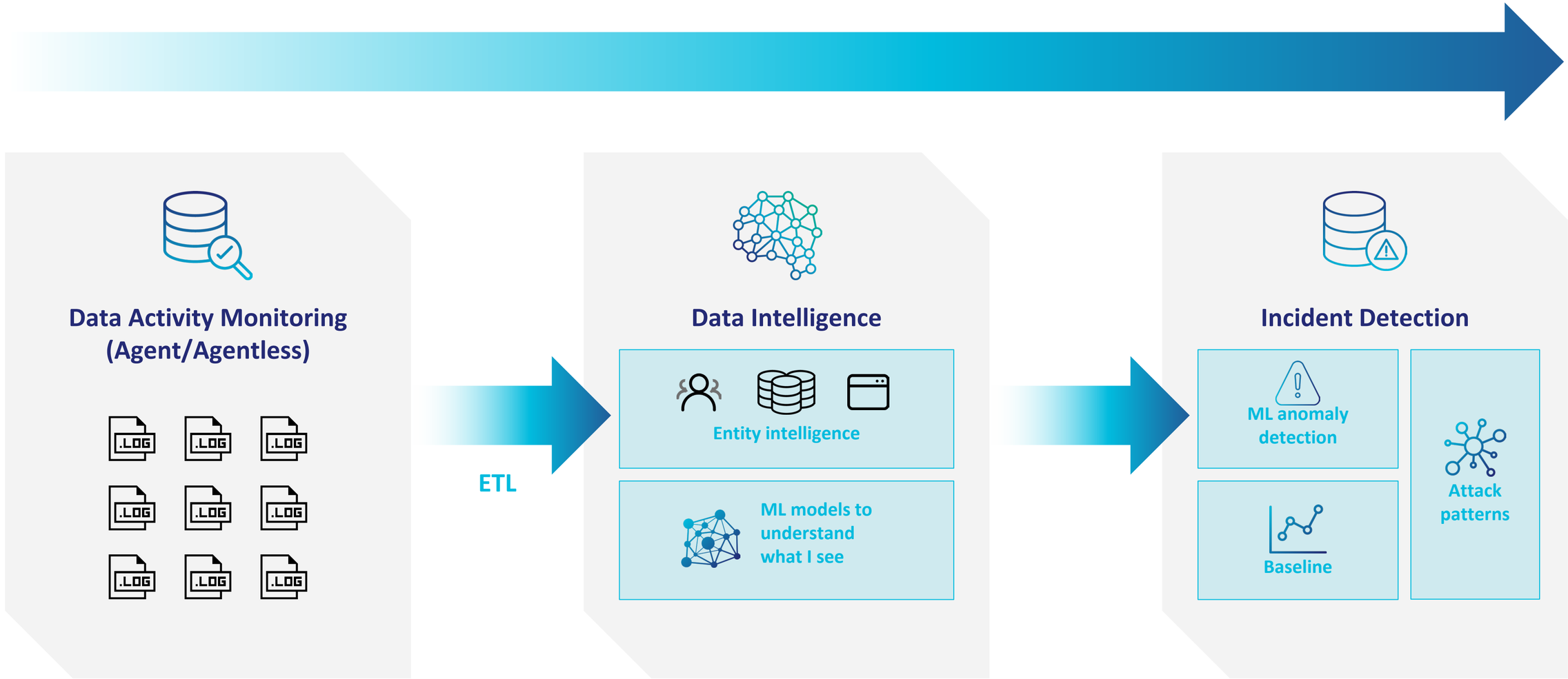
Imperva Data Risk Analytics (DRA) Protects your Data



Imperva Data Risk Analytics (DRA) uses AI/ML to analyze, prioritize, and group high-risk incidences into risk-related insights to elevate the capabilities of your IT and security staff

- Built based on Imperva **20+ years** of data security **domain expertise**
- Tested on **real data of hundreds** of Imperva customers
- Detects **bad security practices** that might be exploited by attackers as well as **real data breaches** → Ongoing **risk reduction**
- Doesn't alert on any **abnormal behavior**, only on the ones that might **indicate a data breach**
- Looks for **insider attackers** - malicious, compromised and careless - which are extremely difficult to detect
- Detects incidents across the **data kill chain** - to **hermetically** protect that data
- Doesn't need any information on the organization from the customers - everything is **learnt independently** by DRA
- All risk incidents are **prioritized**
- All incidents are **explained** in simple English and with all relevant context

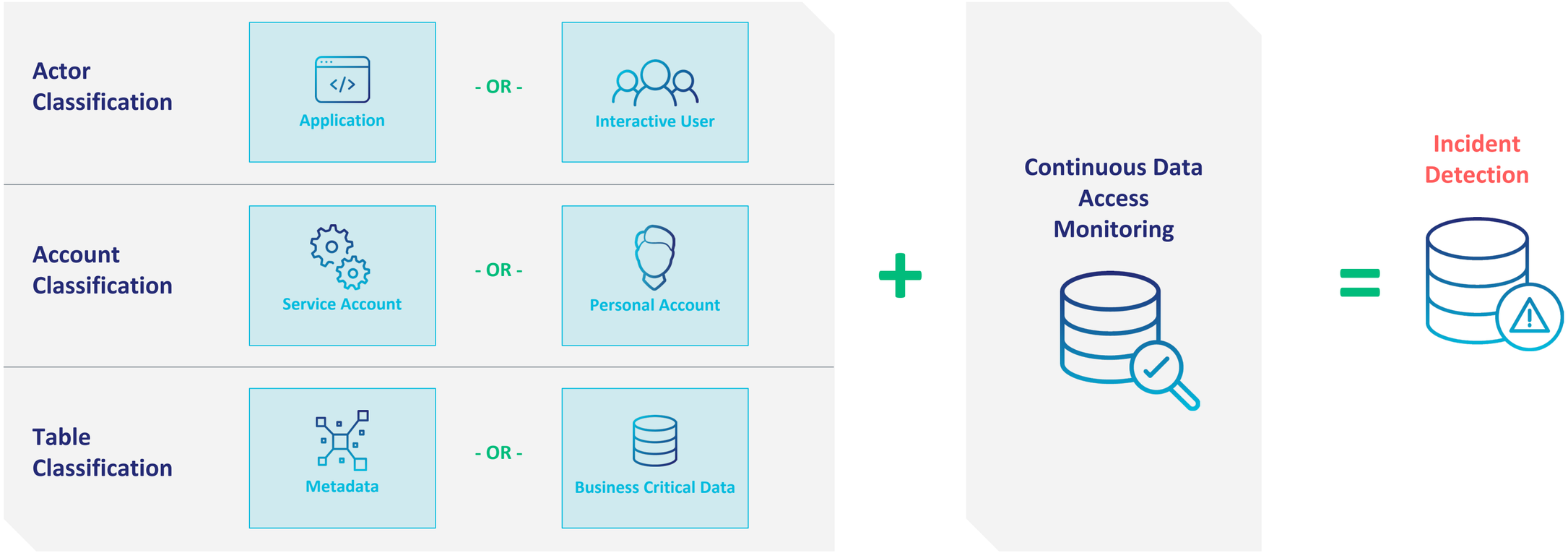
DRA Flow



Data Intelligence - Entities Identification

Leverage machine learning to understand the environment

- Receives data from ETL
- Automatic learns entities in the organization



Data Intelligence - Profiling

Creates the baseline based on last few weeks of data

- The daily average of DB records accessed by each user and their peers
- The daily average of DBs accessed by each user and their peers
- For each user - does he access sensitive system tables? What tables?
- For each host - who are the users that usually use it

Incidents Detection

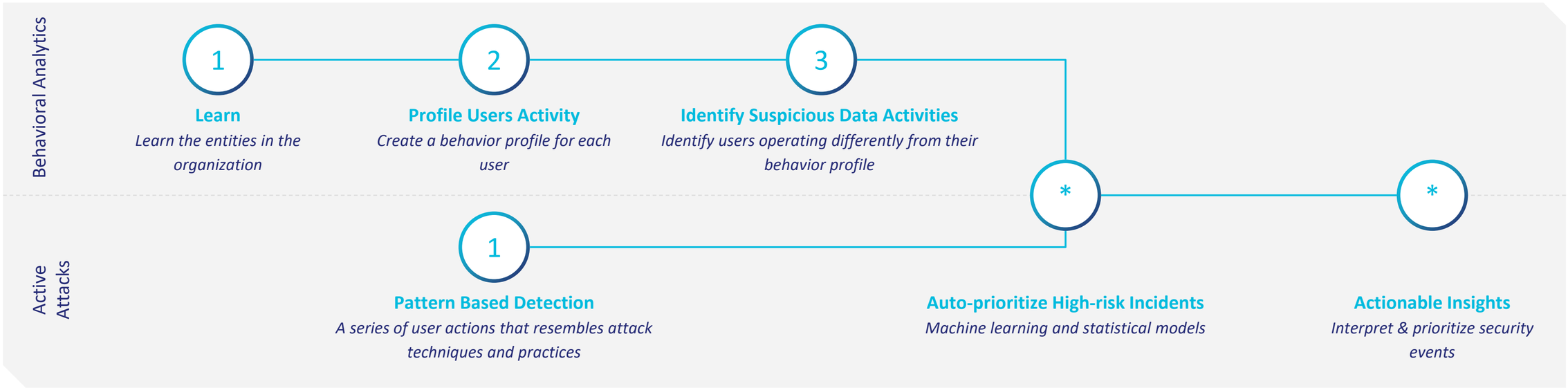
Two Types of Detection

Risk reduction

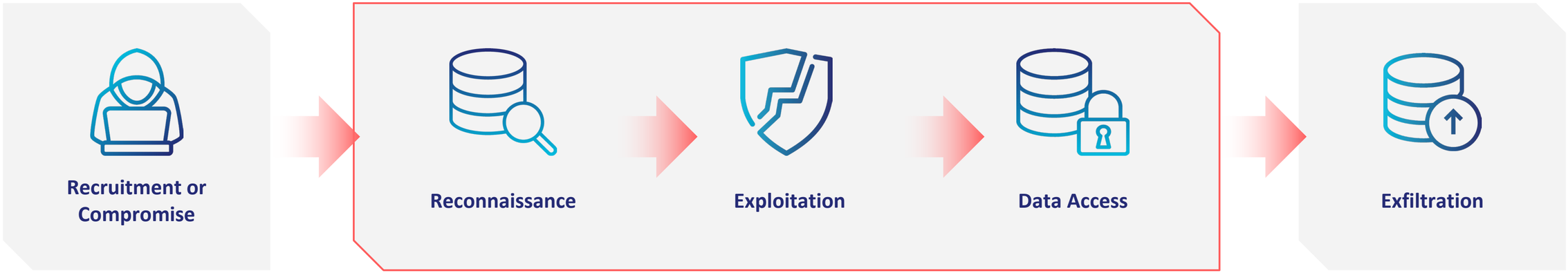
- Bad security practices

Breach detection

- Behavioral analytics
- Active attacks



Detecting Incidents Along the Kill Chain



- System tables scan
- Massive DB scan
- Many login attempts

- Open command shell
- Machine takeover
- Commands sequences not aligned with user role

- Service account misuse
- Retrieve many records
- Access business critical data

General Signs

- Work in non-standard hours
- Use dynamic SQL

DRA detection models

4 Hours update intervals

- Active Attack on Database - Audit Tampering
- Active Attack on Database - Command Execution
- Active Attack on Database - Credentials Extraction
- Active Attack on Database - Data Exfiltration
- Active Attack on Database - Database Weaponization
- Active Attack on Database - Malware Deployment
- Active Attack on Database - OS File Read
- Active Attack on Database - Privilege Escalation
- Active Attack on Database - Ransomware

24 Hours interval update

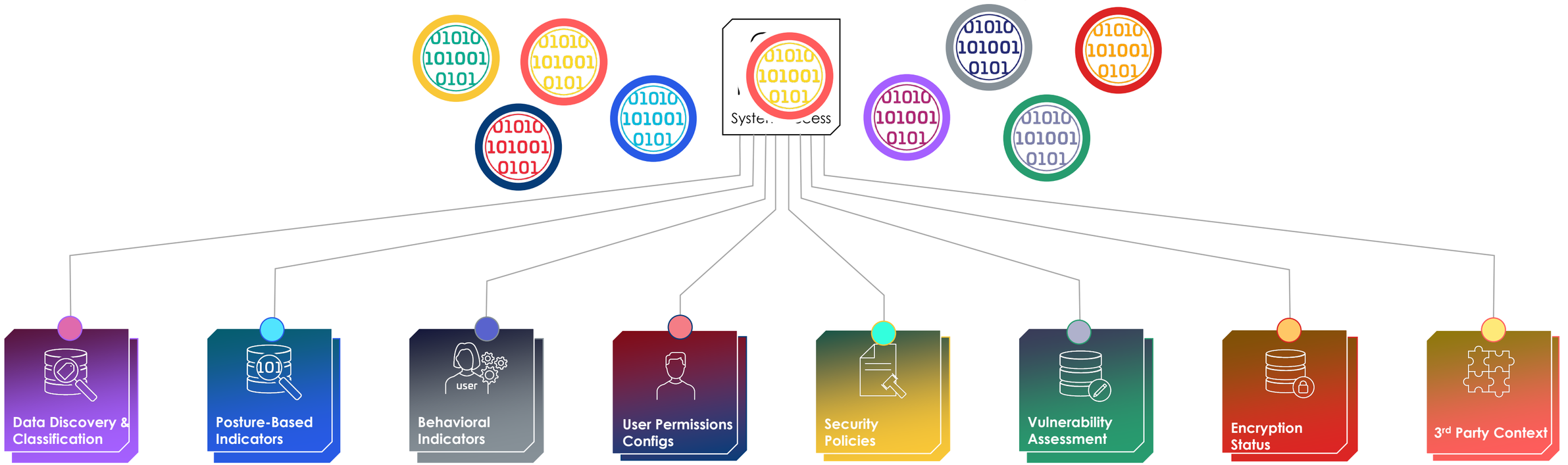
(Near-Real-Time ETA 2025)

- Database Access at Non-standard Time
- Database Service Account Abuse
- Excessive Database Record Access
- Excessive Failed Logins
- Excessive Failed Logins from Application Server
- Excessive Multiple Database Access
- Machine Takeover
- Suspicious Application Data Access
- Suspicious Database Command Execution
- Suspicious Dynamic SQL Activity
- Suspicious OS Command Execution
- Suspicious Sensitive System Tables Scan


THALES
Building a future we can all trust
Data Risk Intelligence
(DRI)

Today’s Siloed Approach Does Not Deliver A Clear Data Risk Picture

Countless hours and resources invested in navigating through systems and interfaces
to construct a view of the data risk landscape



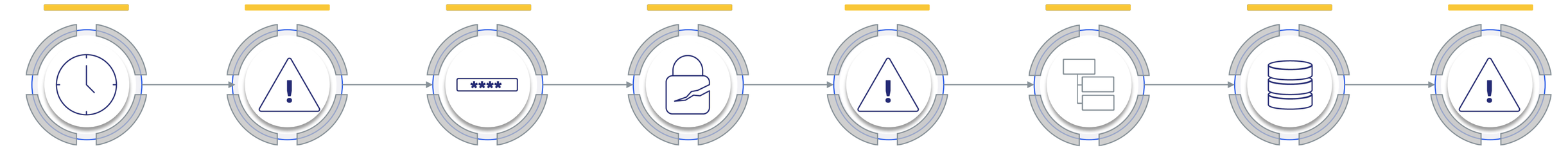
Does not connect risk indicators and context

Inaccurate risk scores lead to ineffective prioritization of incidents

Attack vectors are often missed – leaving the organization vulnerable

Organizations Usually Focus on a Subset of Risks

Particularly Those They Can Manage



Database access at non-standard time

Active attack on DB credentials: Extraction

Excessive failed logins

Known vulnerabilities

Active attack on DB: Privilege Escalation

Excessive DB records access

DB contains sensitive unencrypted data

Active attack on DB: Exfiltration

Risk Score: 86

Imperva™ Data Security Fabric

Data Risk Intelligence

First GA – Q4 2024

Combines key data risk indicators into an actionable view, using a unified solution to help you understand where and why your data is at risk to quickly address attack vectors.

Data Risk Intelligence: Delivering High Accuracy Risk Scoring

3: A **customized risk score** aligned to the organization is presented

4: **Incidents** are **prioritized**, and **suggested courses of action are delivered**. Users can **drill down for deeper investigation.**

Risk Score Presentation

Prioritized
Actionable Insights

System Access

Risk Score Calculation
Customized Weight per Indicator

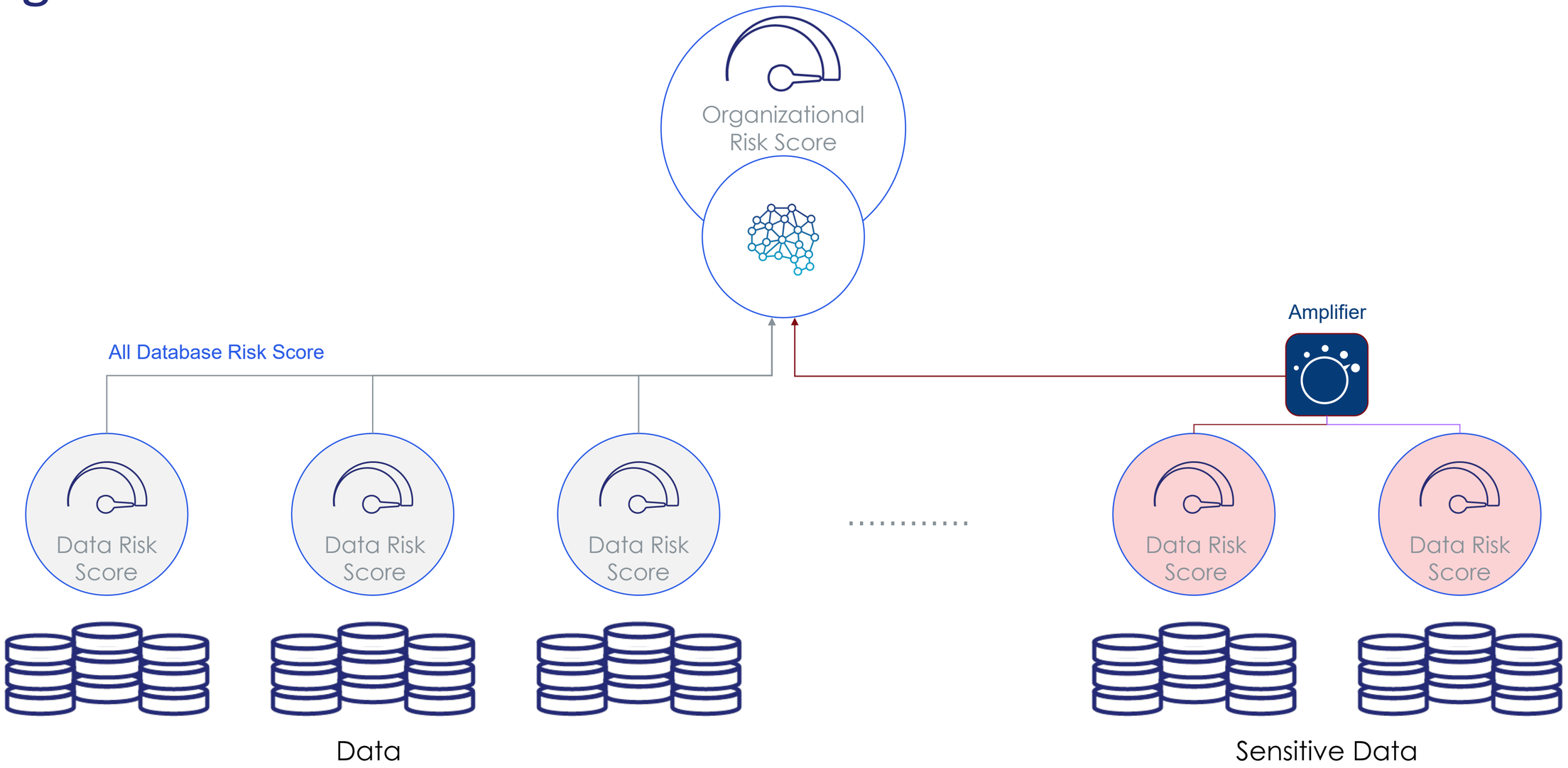
2: Acquired information is **weighted** and **combined**

1: **Data**, **Risk Indicators**, and **Context** are acquired from multiple sources

- Posture-Based Indicators
- Behavioral Indicators
- Discovery & Classification
- Vulnerability Assessment
- Security Policies
- User Permissions Configs
- Encryption Status
- 3rd Party Context

Data Source Risk Score

Organization Risk Score



Bring Together Posture and Behavioral Indicators

Posture Indicators

Static indicators identify policy violations or attack vectors commonly used by threat actors.

Vulnerabilities

Common CVEs | Insufficient Audit | Default User not removed

User Permissions Misconfigurations

Excessive permissions | Excessive access grants | How long ago were they granted | User account access elevated to service account

Coverage

Number of databases monitored as total

Sensitive Data

Data sources with sensitive data

Encryption

Data sources encryption status

Behavior Indicators

Dynamic indicators that identify deviations from normal behavior for early threat detection.

Active Attacks on Databases

Audit Tampering | Command Execution | Credential Extraction | Data Exfiltration | Etc.

Suspicious Scans

Sensitive system table scans

Suspicious Logins

Multiple Failed Logins | Excessive Failed Logins from App. Server

Suspicious Command Execution

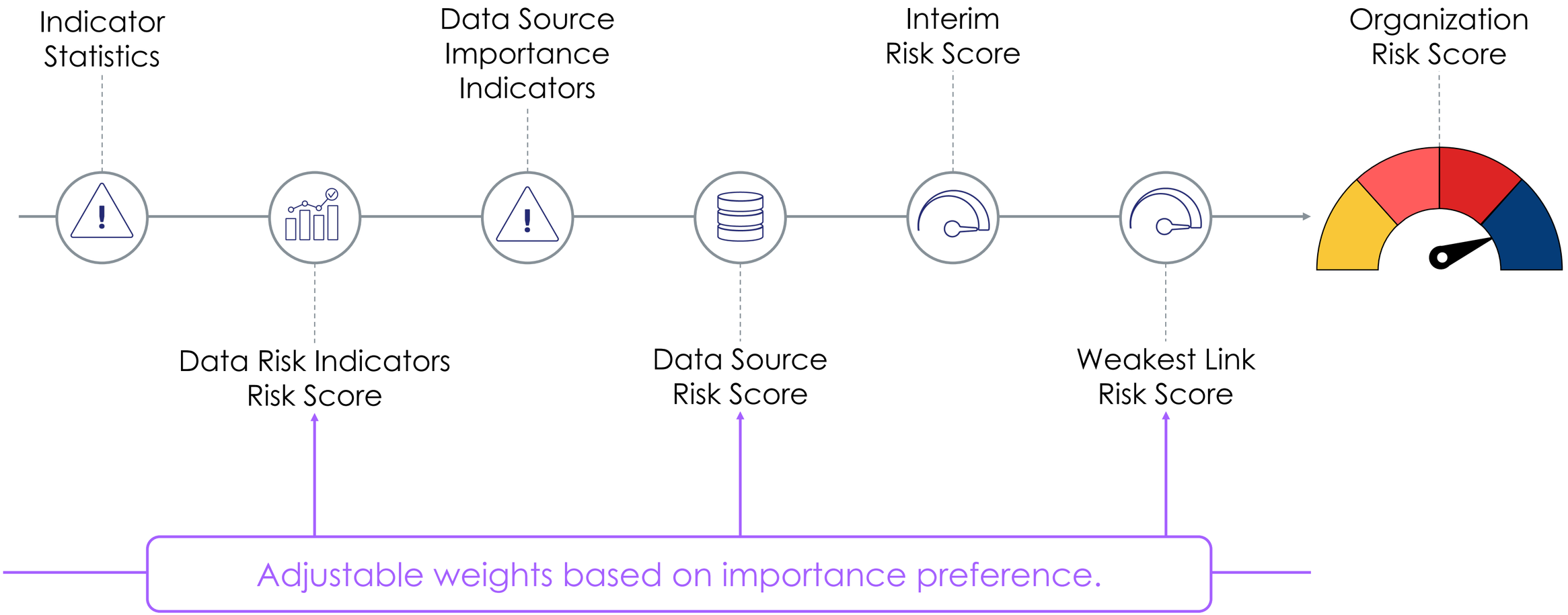
Operating System | Dynamic SQL Activity

Suspicious DB Access Scenarios

Application Data Access | Excessive Data Access | Machine Takeover | Etc.

...and more

Customize Risk Score - According to Organization's Practice

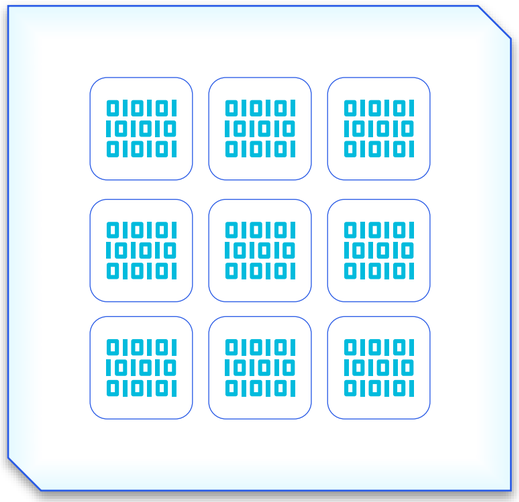


File Activity Monitoring (FAM)

Not All Data is Created Equal

Types of Data

Structured



Organized in fixed fields and formats, typically stored in relational databases (e.g., spreadsheets, SQL tables)

Unstructured

Lacks a predefined format or schema, making it harder to search and analyze (e.g., emails, PDFs, videos)

Semi-structured

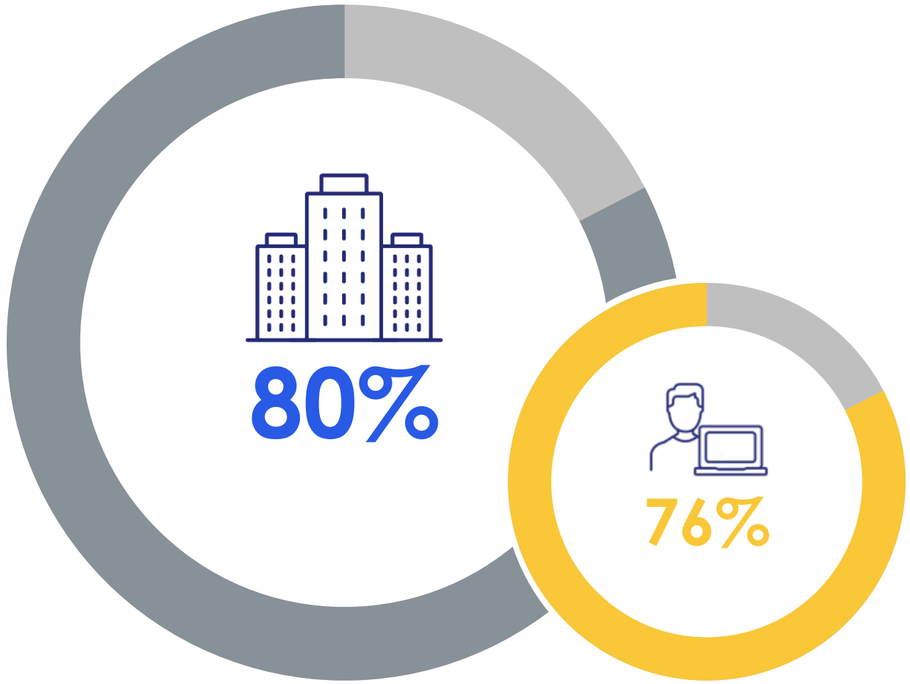
Contains some organizational properties but doesn't fit neatly into tables (e.g., JSON, XML, NoSQL databases)

60%

of data breaches involve unstructured data sources like file shares, email attachments, and collaboration platforms *

* Ponemon Institute

The Importance of Monitoring Unstructured Data



- Over **80%** of enterprise data is unstructured
- **76%** of IT leaders say they don't have complete visibility into where sensitive unstructured data lives*

High Risk of Leaks

Unstructured data often contains sensitive information (e.g., personal data, trade secrets, financial information) that can be easily exposed in the event of a breach

Compliance and Legal Risks

Regulations like GDPR, HIPAA, CCPA, and PCI DSS require organizations to secure sensitive data, much of which resides in unstructured formats (e.g., emails, contracts, health records)

Visibility Challenges

Unlike structured data (e.g., databases), unstructured data is scattered across multiple locations, including endpoints, file shares, collaboration tools, and cloud services

Insider Threats

Employees or contractors can unintentionally (or maliciously) expose or misuse unstructured data stored in shared drives, emails, or local machines

Missed Opportunities

Unstructured data is not just a security liability — it can be a strategic asset if managed properly; if left unsecured or unmonitored, businesses lose opportunities to leverage valuable insights

* BusinessWire

You Can’t Protect What You Can’t See

Structured Data

Unstructured Data

Amazon S3

Azure Blob

Azure File Shares

NAS over CIFS or SMB

Windows Network Drives (SMB)

Linux Network Drives (SMB and SSH)

MacOS Network Drives (SMB and SSH)

Google Drive for Workspace

SharePoint Online

Gmail for Google Workspace

Email archives

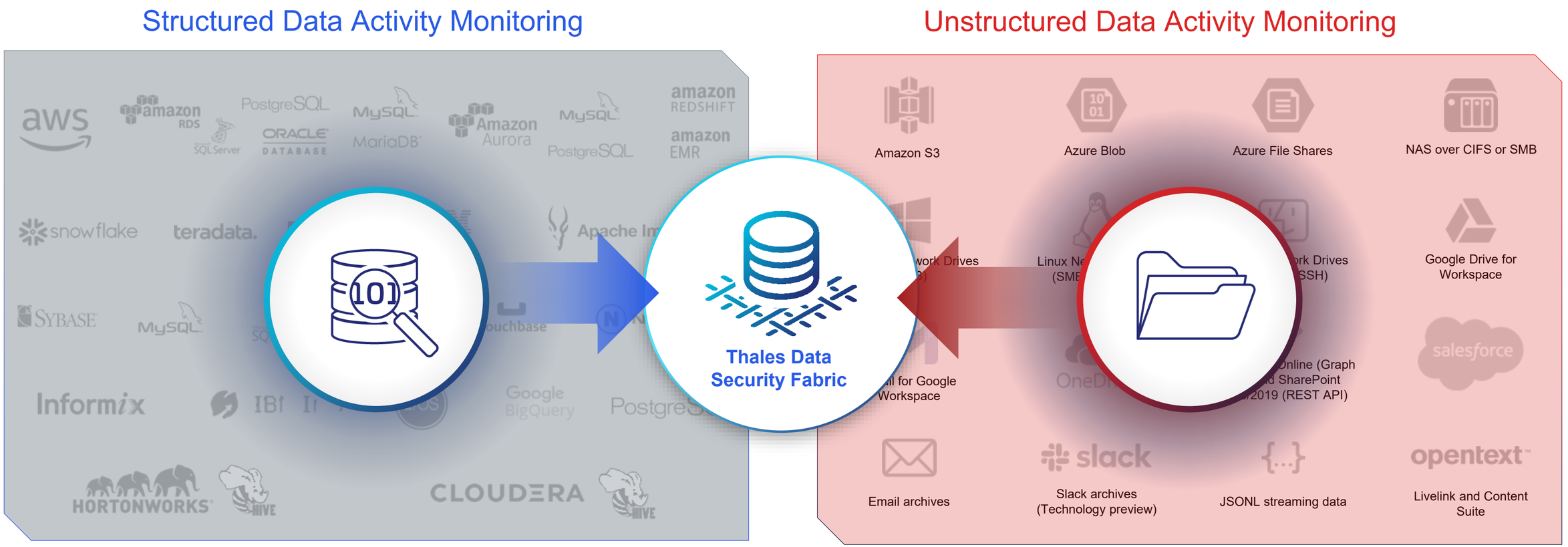
Slack archives

JSONL streaming data

Unstructured data lacks consistent metadata, formats, or schemas, making it difficult for traditional tools to index, classify, or search effectively

Extending Data Activity Monitoring to Unstructured Data

Unstructured data that was previously unmonitored can now be effectively tracked and audited



High Level Roadmap

File Activity Monitoring

Uncovering Sensitive Data

File Entitlement Management

Proactive Threat Detection

Threat Response

H1 2025 | **Q4 2025** | **2026**

Q1 2025: Beta

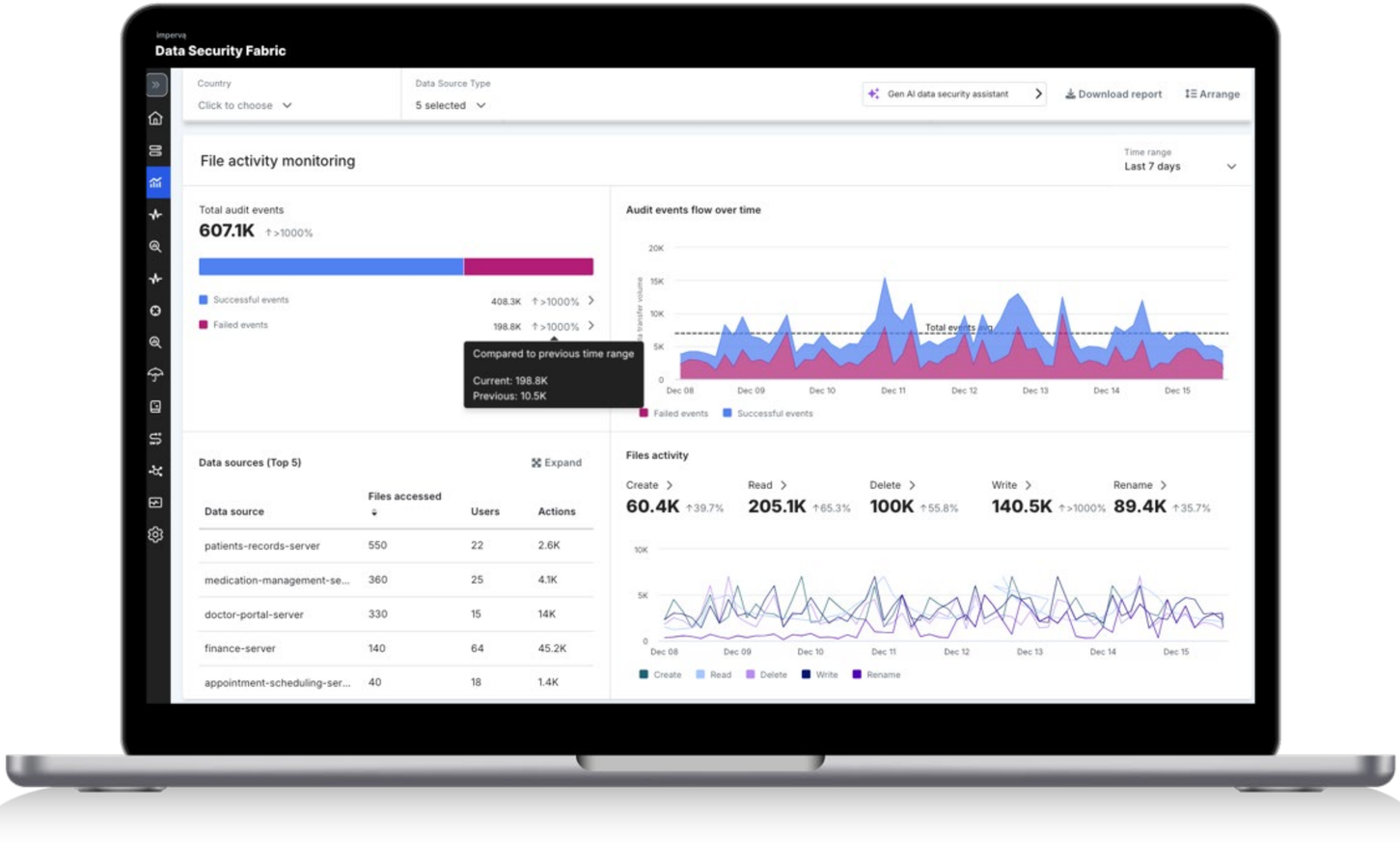
Q2 2025: GA

Coverage & Timeline

	Q1 2025 FAM Beta	Q2 2025 FAM GA	Q3 2025*	Q4 2025*
AGENT MONITORING	Local storage Windows Local storage Linux Network storage NFS Share Network storage SMB/CIFS Share			AWS S3 Salesforce
AGENTLESS MONITORING	Microsoft 365 One Drive Microsoft 365 SharePoint on-line	Microsoft 365 Exchange on-line	Google Drive	Microsoft Teams Microsoft Azure blobs

* Subject to changes based on customers' feedback

FAM MVP - Immediate Data Security Value to your Organization



- **Discover and classify** sensitive data
- Automatically **monitor accesses**
- **Manage compliance**
- **Gen AI** powered data security assistant to streamline workflows
- **Enrich audit** with encrypted information
- Simple & Intuitive **UX**

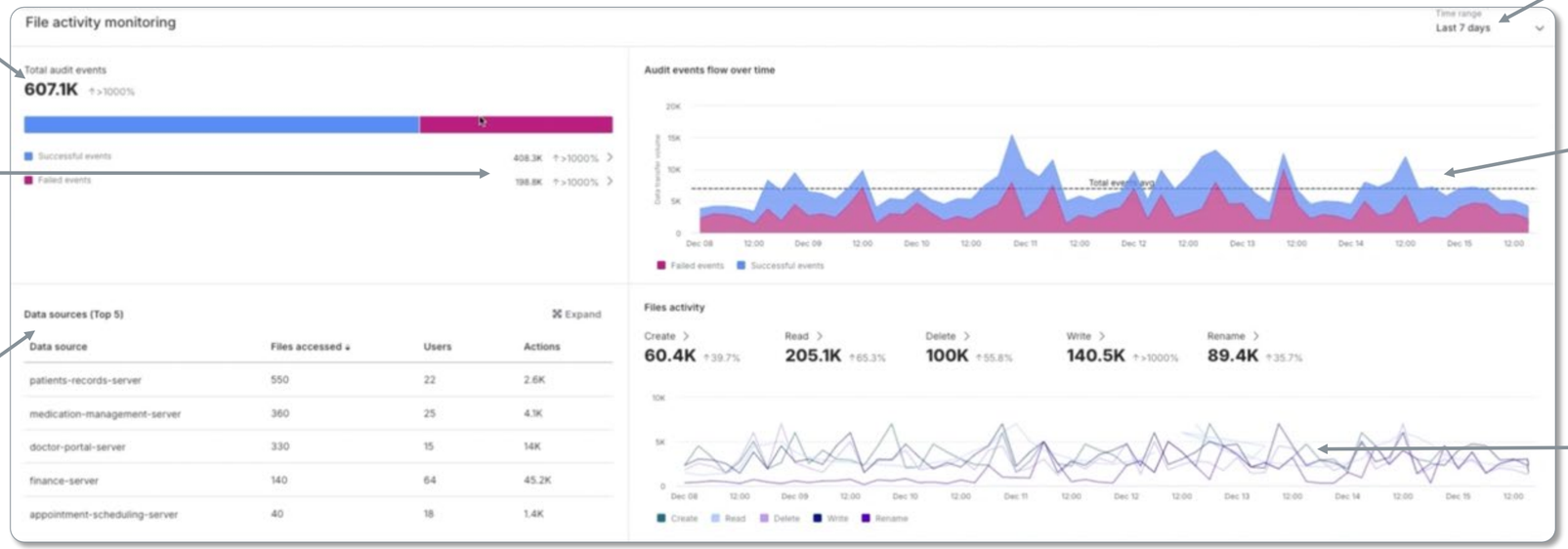
Answering Auditors Questions

“Show me all attempts to access sensitive data in your files”

607K file audit events in the last 7 days

408K successful file events, and 199K failed file events (i.e., user was denied access)

Events filtered by most accessed file source



Time range set to the last week

Successful and failed audit events over time

File activity (create, read, delete, write, rename) over time

Answering Auditors Questions

“Show me all files that fall under GDPR regulations”

Filter all files that have been classified as being subject to GDRP regulations

Drill-down into file records to discover if they are sensitive and/or encrypted

`{“Is_Sensitive”:true,”Profile:[“GDPR”]}`

`{“Is_CTE_encrypted”:true…}`

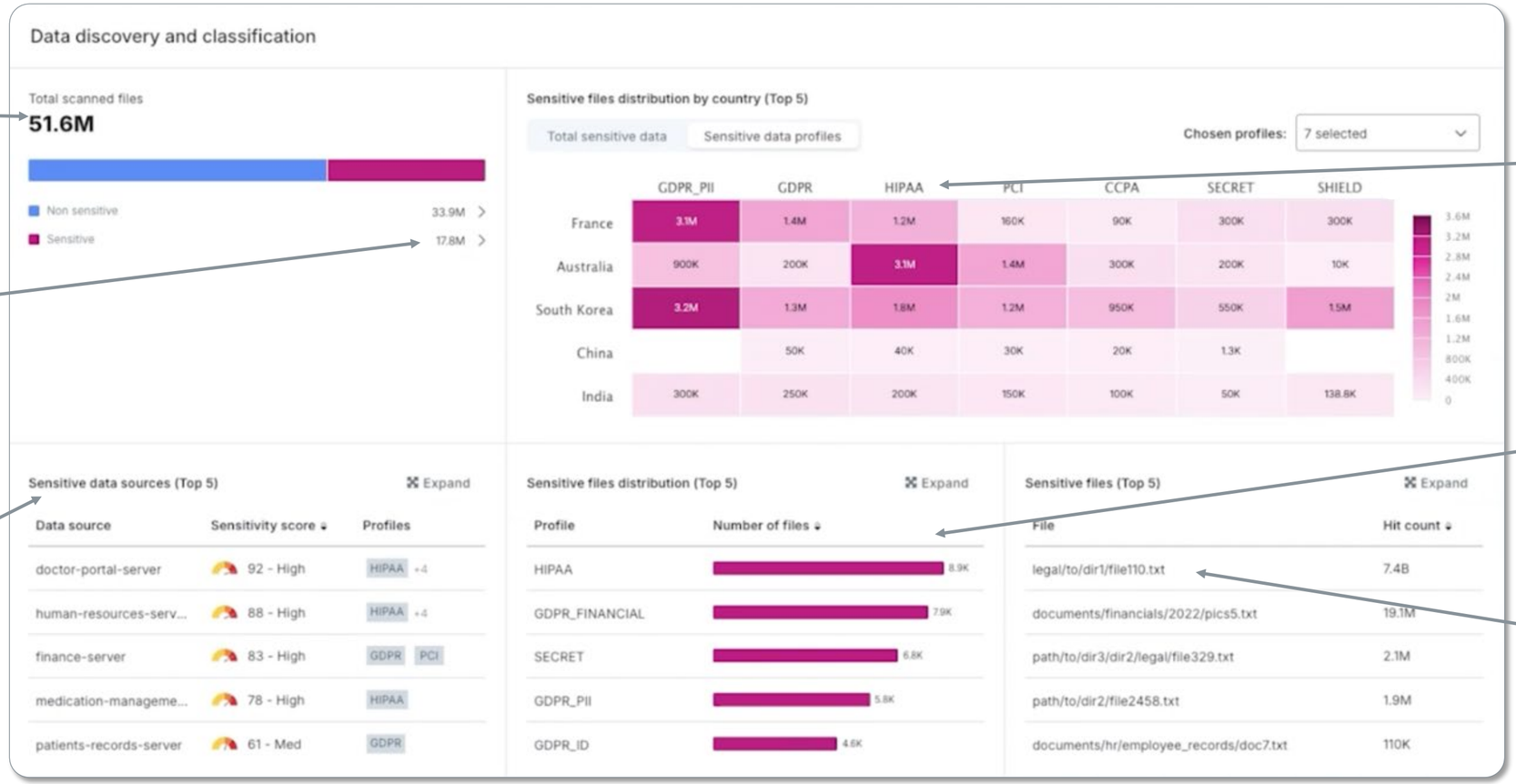
Answering Auditors Questions

“Where are your sensitive HIPAA files physically located?”

52M total files scanned

18M files found with sensitive data

Top five sensitive file data sources



Heat map visual of sensitive data types by geographic location

Distribution of sensitive data by classification

Most accessed sensitive files

GenAI Data Security Assistant

- Based on GenAI and LLM
- Assists in gathering information and insights on the audit data for compliance and security use cases
- Simplifies reports and dashboards creation
- Streamlines compliance and security tasks

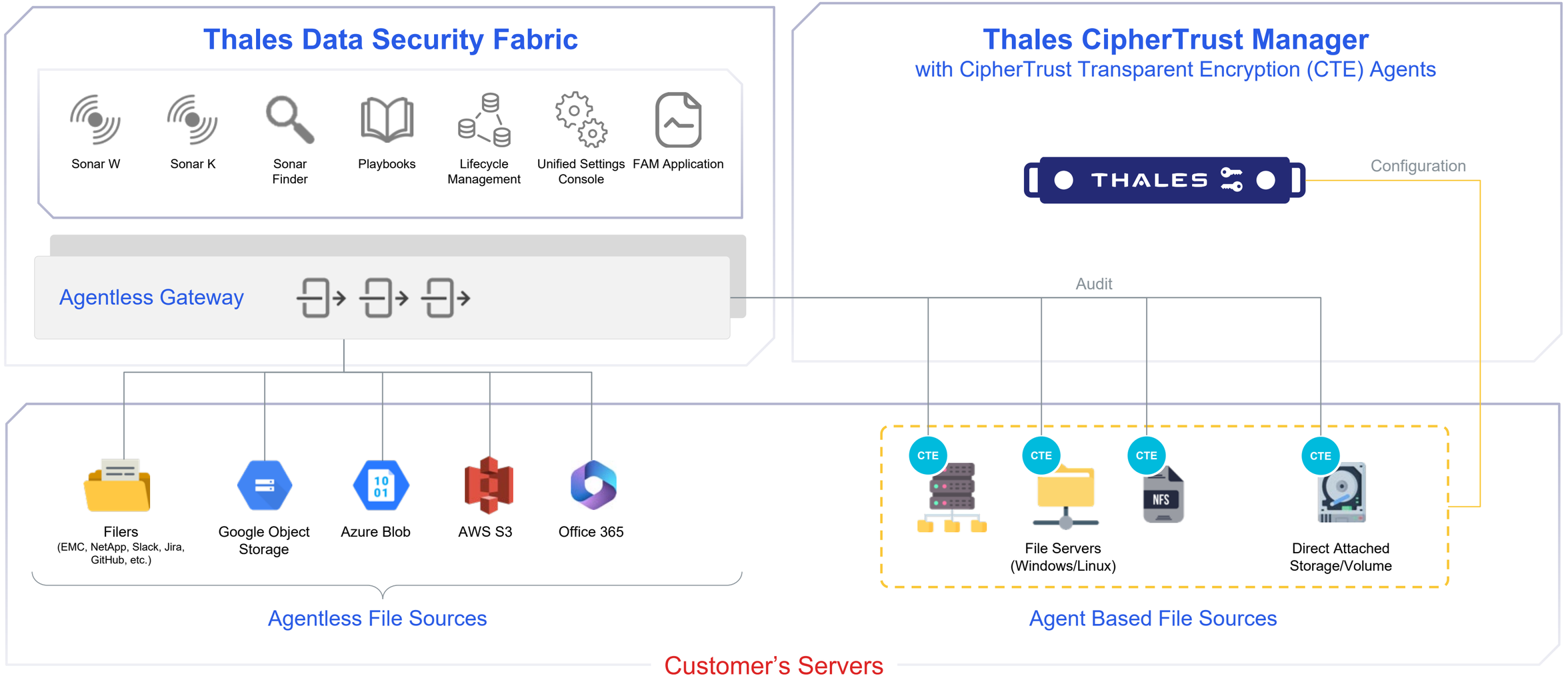
Ask questions like…

- Can you list all policy violations?
- Who are the users responsible for the violations?
- What specific policy violations were caused by Shiri?
- What is the file on which the violation occurred?

…with follow-up actions

- Save to report
- Drill down to the data warehouse for more slicing and dicing
- Get ideas of follow up questions

Files Monitoring High-Level Design



Thank you

www.thalesgroup.com