

# File Activity Monitoring (FAM) - Overview

**MICHAEL GORELIK**  
Senior Product Manager

[www.thalesgroup.com](http://www.thalesgroup.com)



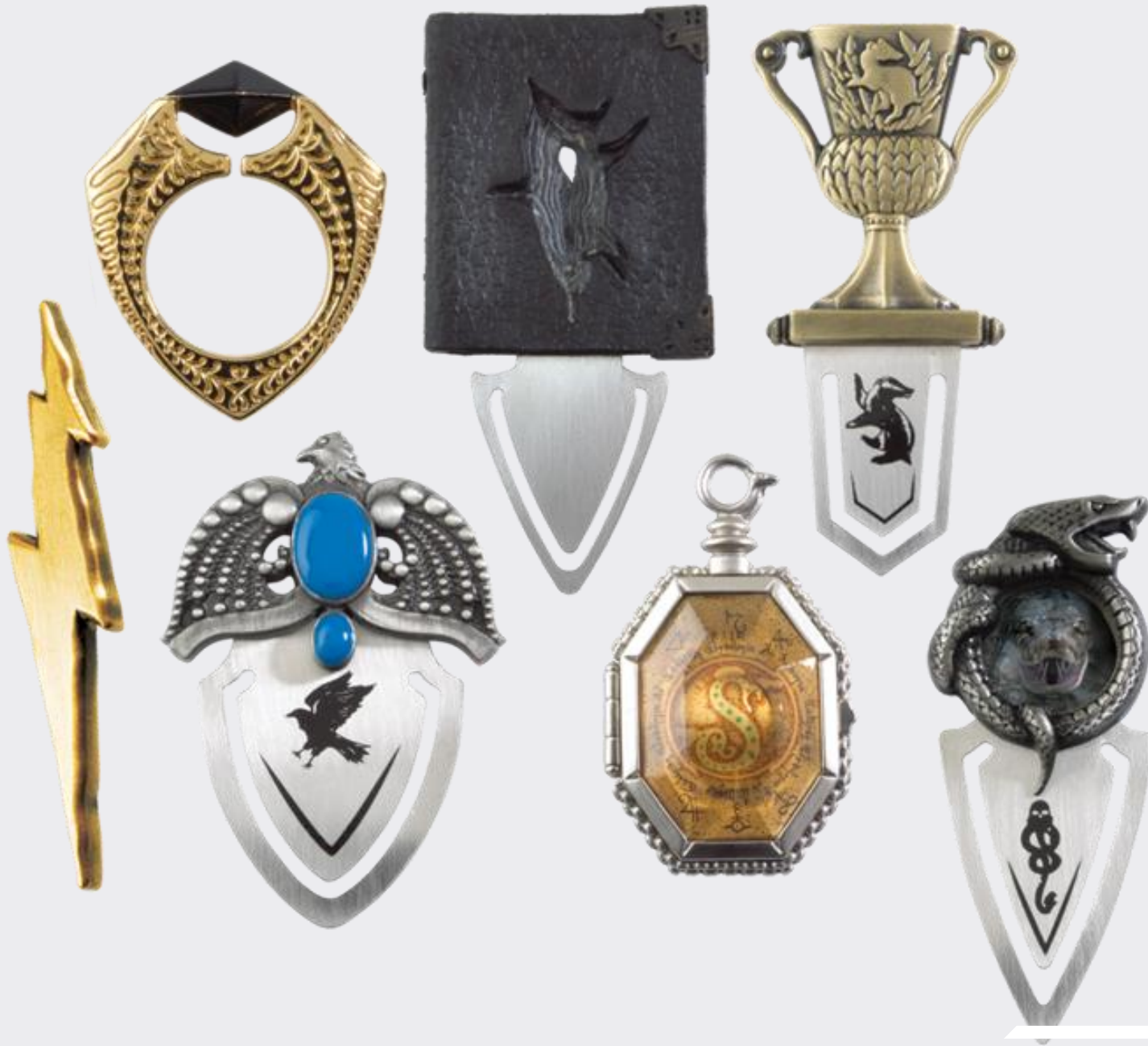
# Disclaimer

This presentation is being provided for **INFORMATIONAL PURPOSES ONLY**. The information provided represents Imperva's expectations as of the date the presentation was prepared. Imperva undertakes no obligation to update or revise this information. The information should not be construed as a commitment to deliver any specific upgrade or feature or functionality.

Imperva may change the contents of the presentation in its sole discretion at any time. You should not rely on the anticipated timelines or potential upgrades, features, or functionality described in the presentation when making a decision to purchase products from Imperva.



HE WHO MUST  
NOT BE  
NAMED !

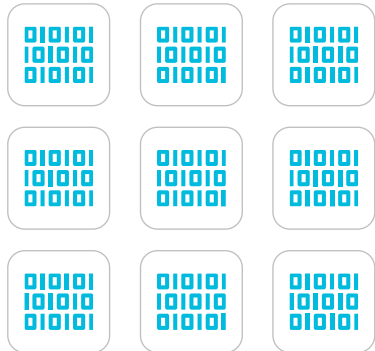




# Not All Data is Created Equal

## Types of Data

### Structured



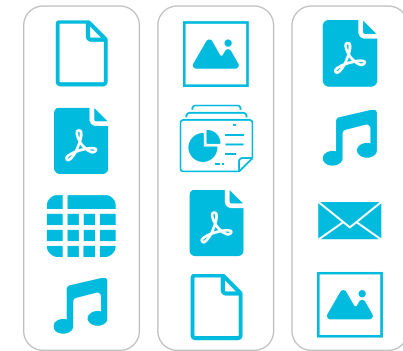
Organized in fixed fields and formats, typically stored in relational databases (e.g., spreadsheets, SQL tables)

### 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)



# Rapid Growth Rate of Unstructured Data



**Unstructured data is growing at a rate of 55–65% per year**

The rapid growth of unstructured data—often containing sensitive or regulated content—poses major security challenges, as its lack of structure hinders traditional tools from effectively identifying and protecting it.



# Michael Gorelik

Senior Product Manager





## Auditor pays a visit...

- DATALAND is a global Healthcare Organization
- 10K employees
- 5,000 customers
- Web customer facing applications
- Doctor's patient management systems and more

# Compliance Management Use Case

Comply with GDPR

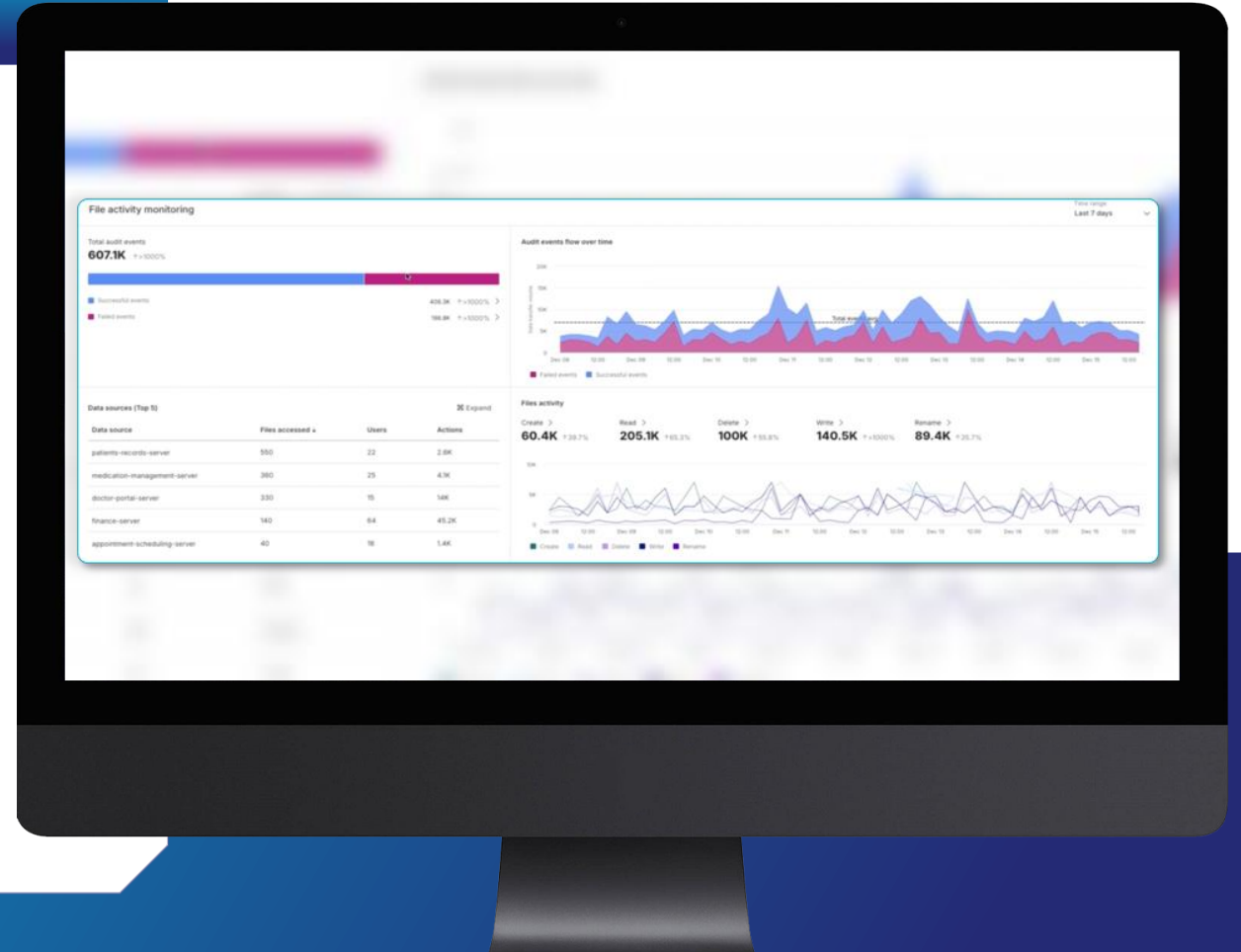
## Use Case: Demonstrate compliance proof to the auditor

An auditor requests evidence that the organization has been auditing access to sensitive GDPR-regulated data over the past five years

The compliance manager uses the FAM dashboard to present audit monitoring statistics, including the number of files monitored over a given period, the types of operations performed, and a breakdown of successful vs. failed access attempts by users

From the FAM dashboard, the compliance manager drills into the reporting platform, filters for GDPR-classified data accessed within the last five years, and generates a report or dashboard tailored to the auditor's request

**Using Thales FAM, the organization can demonstrate GDPR compliance—in minutes**





You have  
been  
breached!!  
Suspicious  
sensitive files  
access



# Why Customers Choose Imperva



## Malicious

Current or former employees, third parties, or partners may misuse their access to steal intellectual property or company data for fraud, sabotage, espionage, revenge, or blackmail.

**Key Traits:** Revenge, financial gain, ideology.

**Example:** Edward Snowden NSA leak (2013), Boeing documents leakage



## Careless

Employees lacking security awareness often expose confidential data due to failure to follow security protocols.

**Key Traits:** Unintentional, often due to lack of training or awareness.

**Example:** Capital One Breach (2019) – Firewall misconfig



## Compromised

Threat actors steal employee credentials, pose as authorized users, and exfiltrate sensitive data, often without the employees' knowledge.

**Key Traits:** Unwitting participant in external attacks. Often exploited by manipulation

**Example:** Twitter Phone Spear-Phishing Attack (2020), SolarWinds supply chain (2020)



# Coverage & Timeline

**Use Case:** Investigating suspicious file access patterns

During a routine dashboard review, the SOC engineer notices an unusual spike in activity

A Microsoft 365 SharePoint Online data source, which typically sees around 100 daily access events, has suddenly recorded 100,000 access events in a single day

To investigate, the engineer opens the Thales FAM Data Security Assistant and begins querying the anomaly using natural language

**Armed with this information—retrieved effortlessly via the Data Security Assistant—the SOC engineer can quickly assess whether the behavior is legitimate (e.g., a planned data migration or review) or a potential insider threat that warrants immediate response.**

**“Who normally accesses the Microsoft 365 SharePoint Online data source?”**

The assistant returns a list of six users:

- Shiri
- Maya
- Steve
- Bill
- Mor
- Tyson

**“How many files did each user access each day over the past week?”**

The assistant reveals that all users, except Shiri, accessed a consistent number of files each day. However, Shiri accessed an abnormally high number of files today.

**“Show me the list of files Shiri accessed today, along with their sensitivity and classification profile.”**

The assistant provides a detailed breakdown, including whether each file is marked as sensitive and how it's classified (e.g., PII, HIPAA, confidential IP)

# You have been breached: Reported Suspicious Activity by Mariam Harris





# Sensitive Un-authorized Data Access

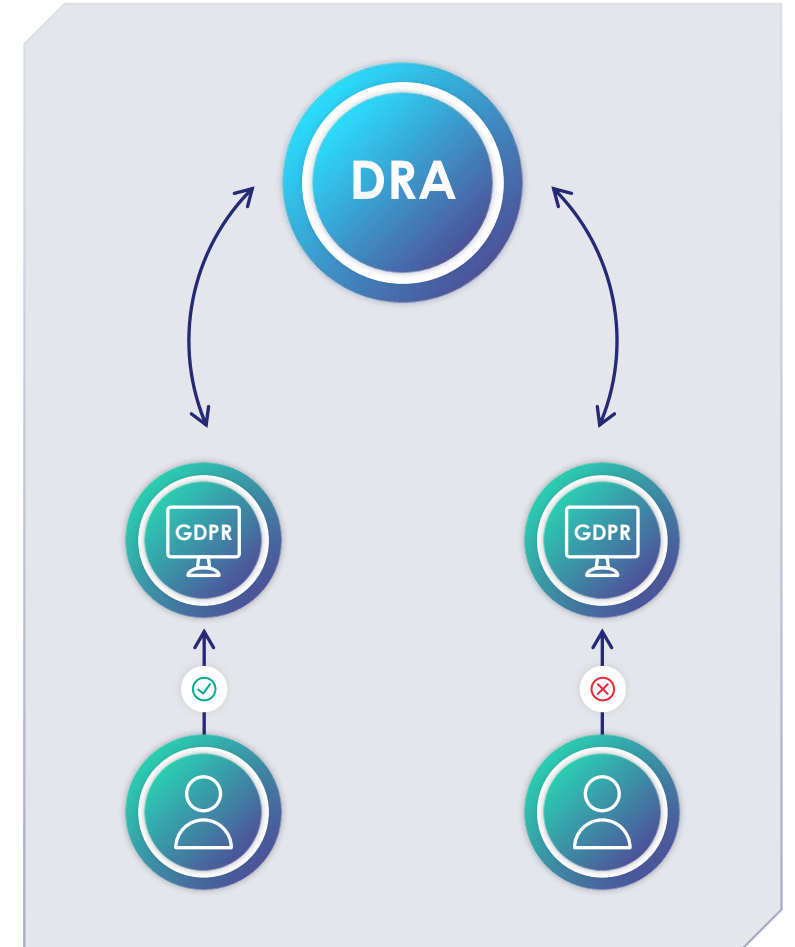
## Use Case: Uncover unauthorized access to GDPR sensitive data

Mariam, an employee of the organization, reads GDPR sensitive data from one Windows local storage

Mariam is a contractor that shouldn't access GDPR sensitive data

Using a playbook, Mariam's activity can be blocked on the data source, until the permissions of Mariam are properly updated

**Using Thales DRA monitoring potential data breach was caught, put proper controls in place, and saved the organization's sensitive data from being exposed**





# Behavioural Incidents with a broad context

What

Why

Who

Context

Critical 97

Suspicious Database Command Execution

☆

Event Time: Jan 28, 2022 7:41:00 PM | Status: Open | ID: 1307

Close incident

Create Allow List

Interactive (non-application) user 'tim cooper' executed the command 'Create Assembly' that is highly suspicious in nature and has never been executed by this user on the database on '10.51.45.114' in the past

[Learn how to investigate this type of incident](#)

Comment

▼

What influenced the severity of this incident

Source Details

tim cooper (Support EMEA)  
Senior Customer Support

Host: win7x-tim.c-desk

IP Address: 10.38.26.108

Source Application: microsoft sql server management studio - query

User Endpoint

Interactive Tool

Destination Details

MsSql

Host: eu-customers-05

Dest IP: 10.51.45.114

DB User: svc\_gen

DB Name: db\_gen13

Service Account

▼ Show details

Incident Details

Typical Behavior

RELATED ISSUES (1)

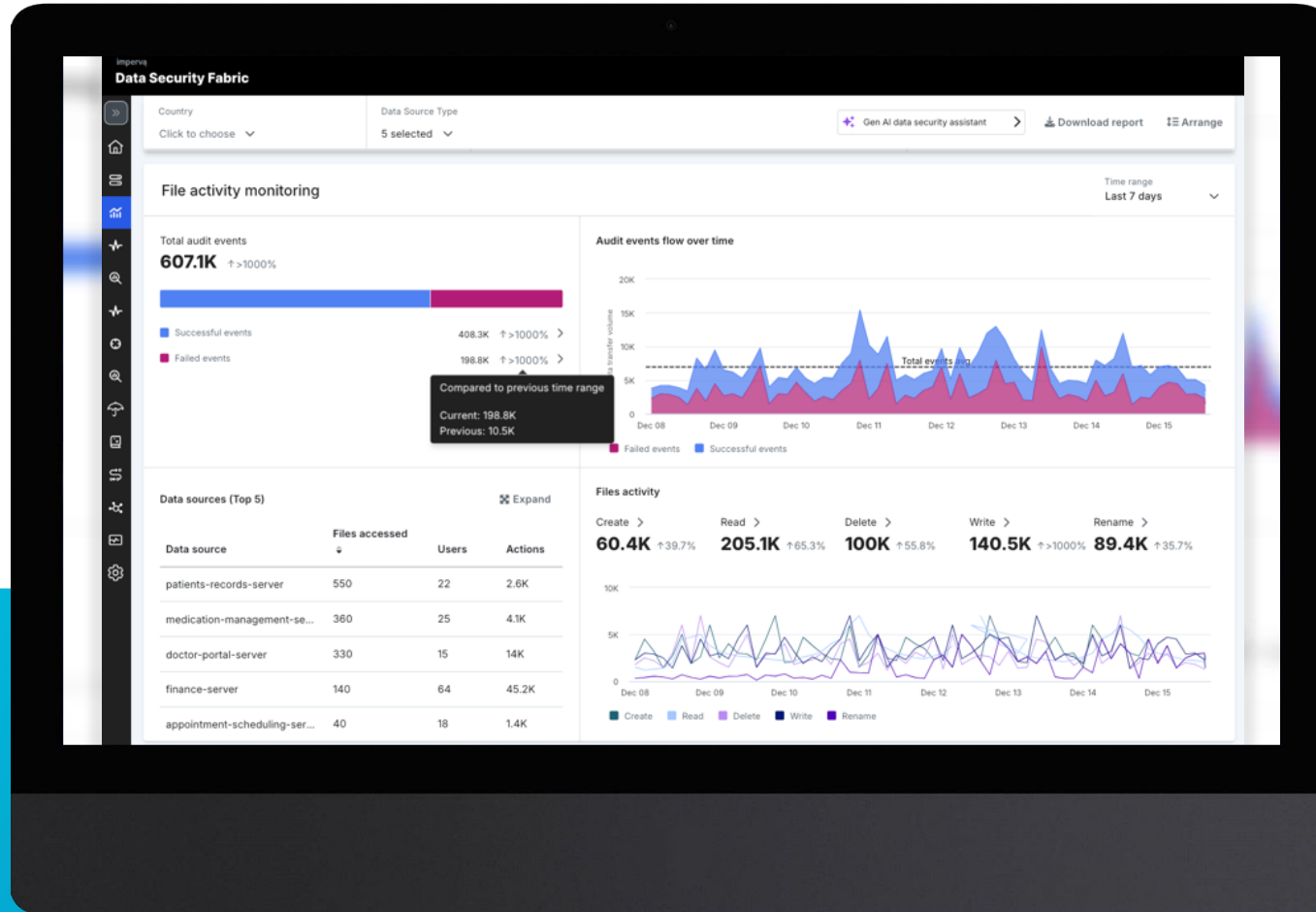
Suspicious Database Commands Executed Multiple Times by a Single User  
User 'tim cooper' performed multiple database commands on multiple databases

Where



# Unstructured Monitoring FAM Offering – GA Released in Q2 2025

Delivering Immediate Data Security Value to your Organization



**Discover** and **classify** sensitive data

Automatically **monitor accesses**

Manage **compliance**

**Enrich audit** with sensitive information

**Enrich audit** with encrypted information

Simple & Intuitive **UX**

**Gen AI** powered data security assistant to streamline workflows

# Data Risk Intelligence (DRI)

## POSTURE INDICATORS



Vulnerabilities



User Permissions Misconfigurations



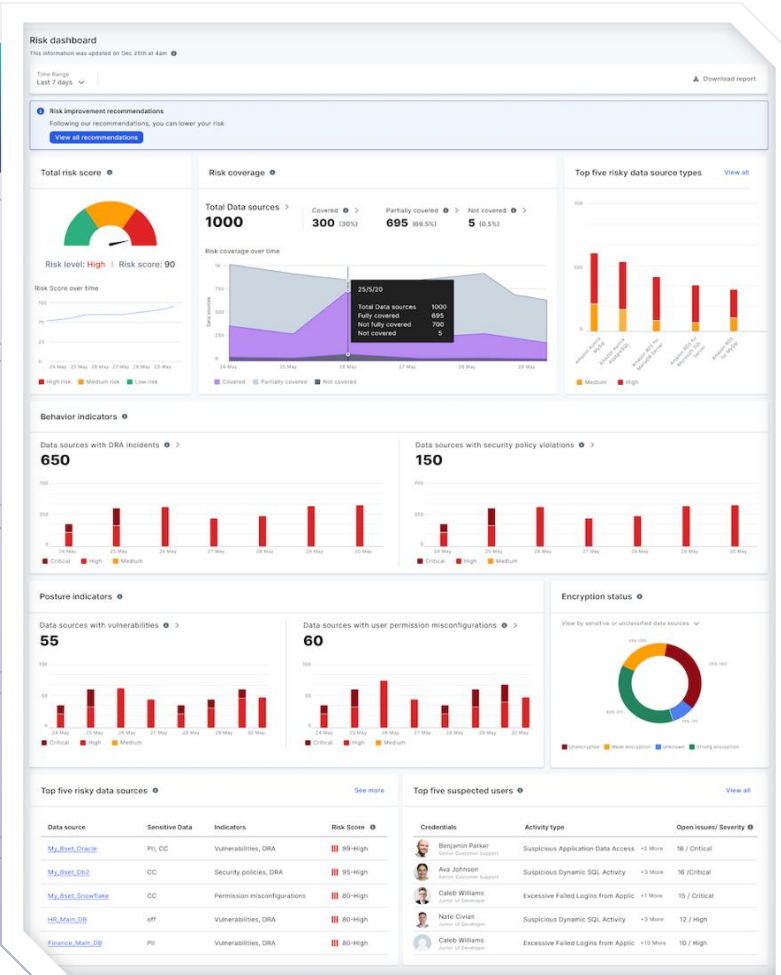
Coverage



Sensitive Data



Encryption



## BEHAVIORAL INDICATORS

Active Attacks on Databases



Suspicious Scans



Suspicious Logins



Suspicious Command Execution



Suspicious DB Access Scenarios





# Data and all paths to it



**Compliance  
Management**



**Data  
Visibility**



**Threat Investigations  
& Forensics Analysis**



# Thank you

[www.thalesgroup.com](http://www.thalesgroup.com)



# Agenda

## Key use cases

## Roadmap



**Why FAM?**



**Architecture  
& data flows**



**Live demo**

# Not All Data is Created Equal

## Types of Data

### Structured



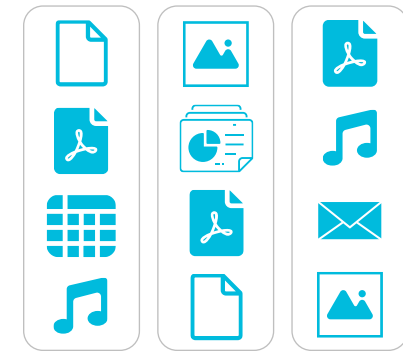
Organized in fixed fields and formats, typically stored in relational databases (e.g., spreadsheets, SQL tables)

### 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)



# POLL QUESTION:1

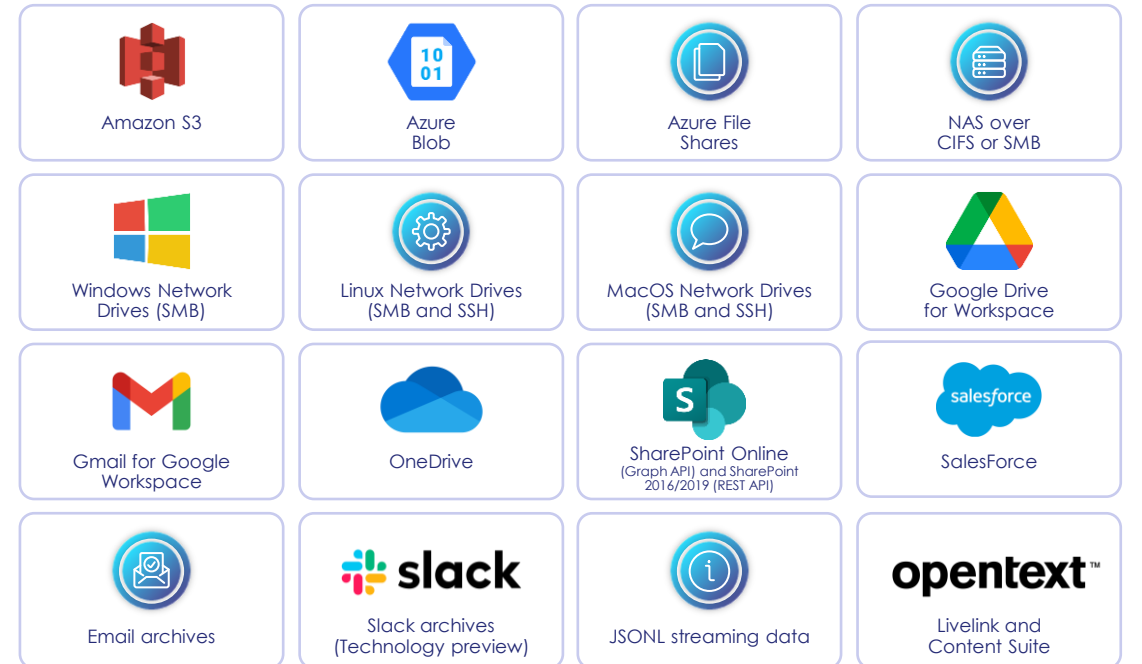
# Data Security is Required for All Data Types

While structured data powers most enterprise applications and transactional systems, unstructured data makes up most of the data volume across all organizations

## Structured Data Types



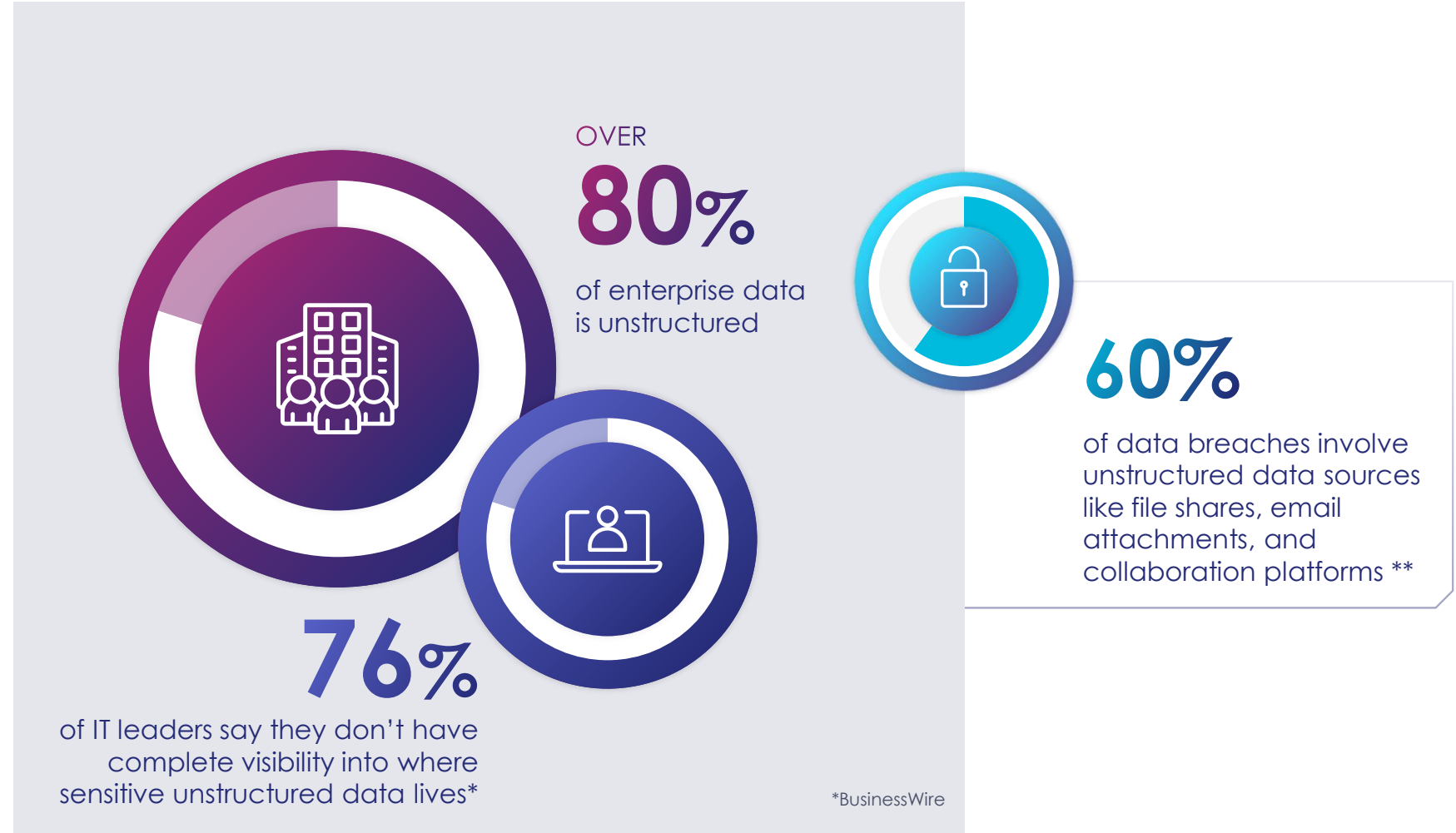
## Unstructured Data Types





# The Importance of Monitoring Unstructured Data

\* BusinessWire | \*\*Ponemon Institute



# You Can't Protect What You Can't See

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





# Rapid Growth Rate of Unstructured Data



**Unstructured data is growing at a rate of 55–65% per year**

The rapid growth of unstructured data—often containing sensitive or regulated content—poses major security challenges, as its lack of structure hinders traditional tools from effectively identifying and protecting it.



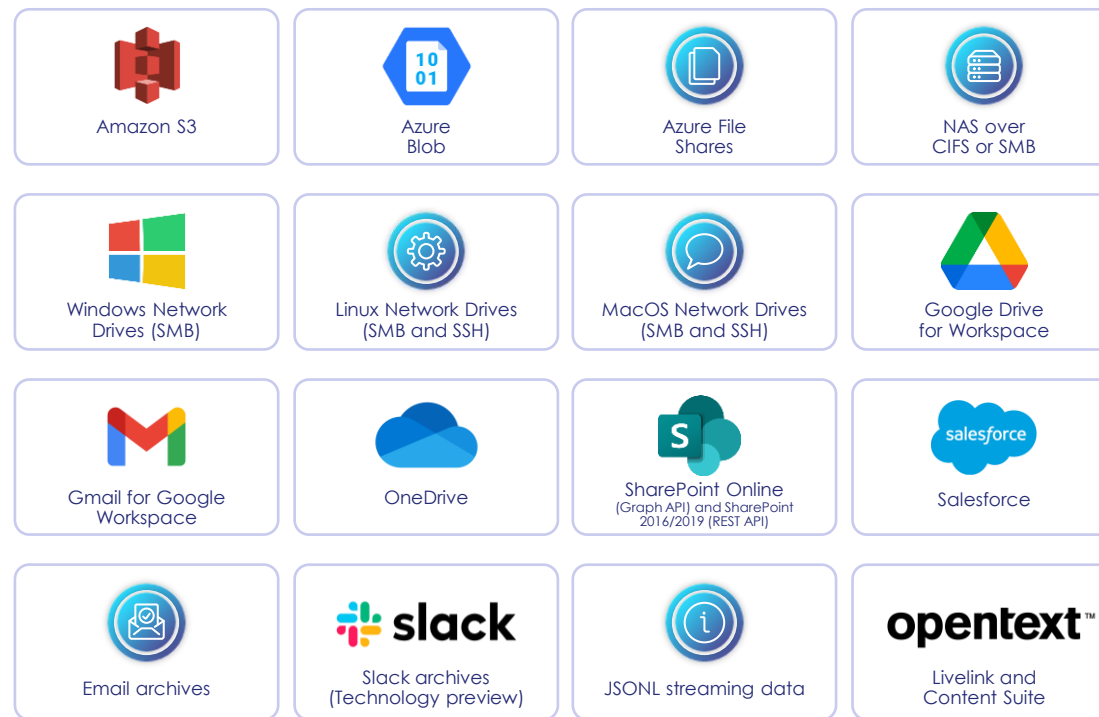
# Extending Data Activity Monitoring to Unstructured Data

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

## Structured Data Activity Monitoring

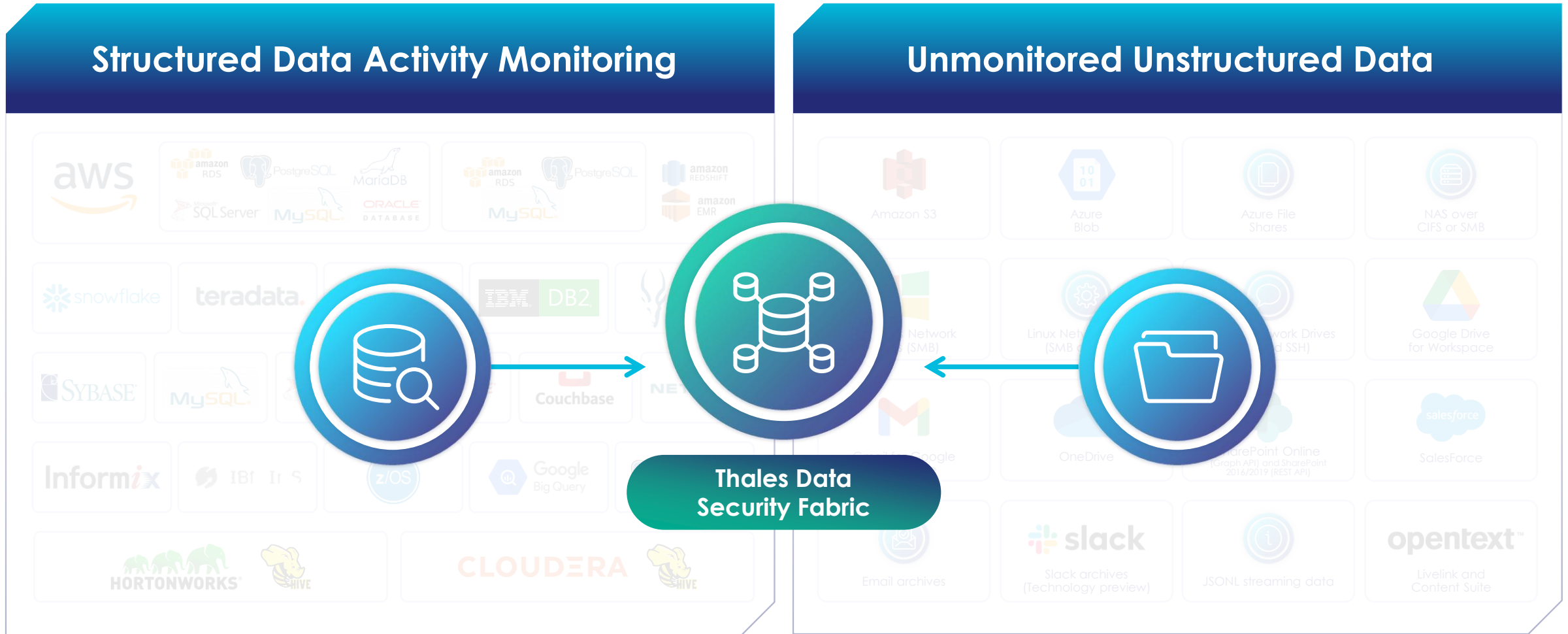


## Unmonitored Unstructured Data



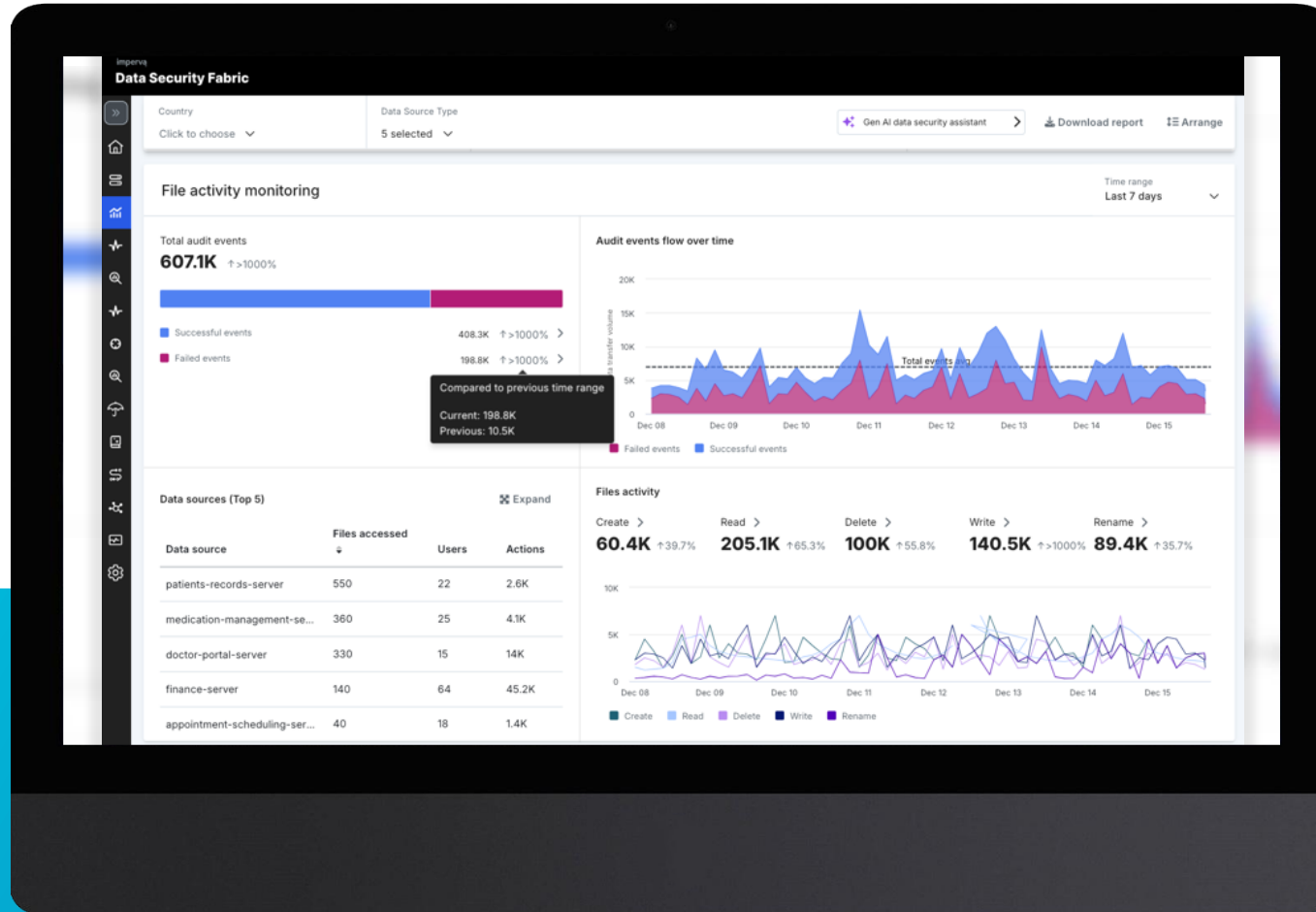
# Extending Data Activity Monitoring to Unstructured Data

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



# FAM Offering – GA Released in Q2 2025

Delivering Immediate Data Security Value to your Organization



**Discover** and **classify** sensitive data

Automatically **monitor accesses**

Manage **compliance**

**Enrich audit** with sensitive information

**Enrich audit** with encrypted information

Simple & Intuitive **UX**

**Gen AI** powered data security assistant to streamline workflows



# GenAI Data Security Assistant

Based on  
GenAI and LLM

Assists in gathering information  
& insights on the audit data for  
compliance & 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

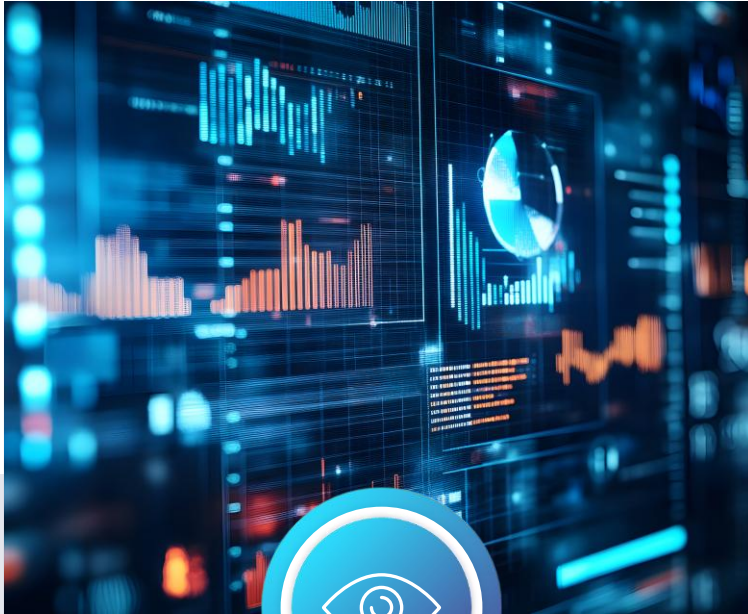


Get ideas  
of follow up  
questions

# Example Use Cases



## Compliance Management



## Data Visibility



## Threat Investigations & Forensics Analysis

# Compliance Management Use Case

Comply with GDPR

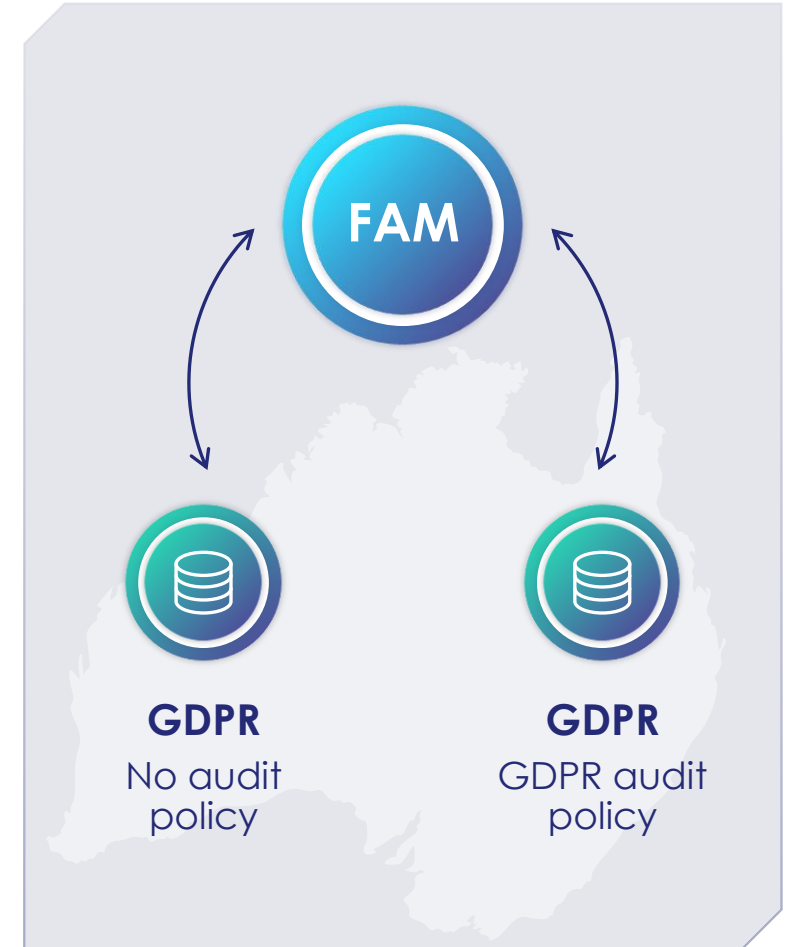
## Use Case: Discovering and auditing GDPR sensitive data

Following a data classification scan, the compliance manager discovers that a Microsoft OneDrive in Australia contains GDPR sensitive data

From the FAM data source inventory, the compliance manager easily sees that this data source doesn't audit the file activity monitoring of the GDPR sensitive data, as required by the auditor

The compliance manager configures the GDPR audit policy to make sure GDPR sensitive data is fully monitored in the organization

**Using Thales FAM, the compliance manager uncovers GDPR sensitive data and makes sure it is audited**





# Compliance Management Use Case

Comply with GDPR

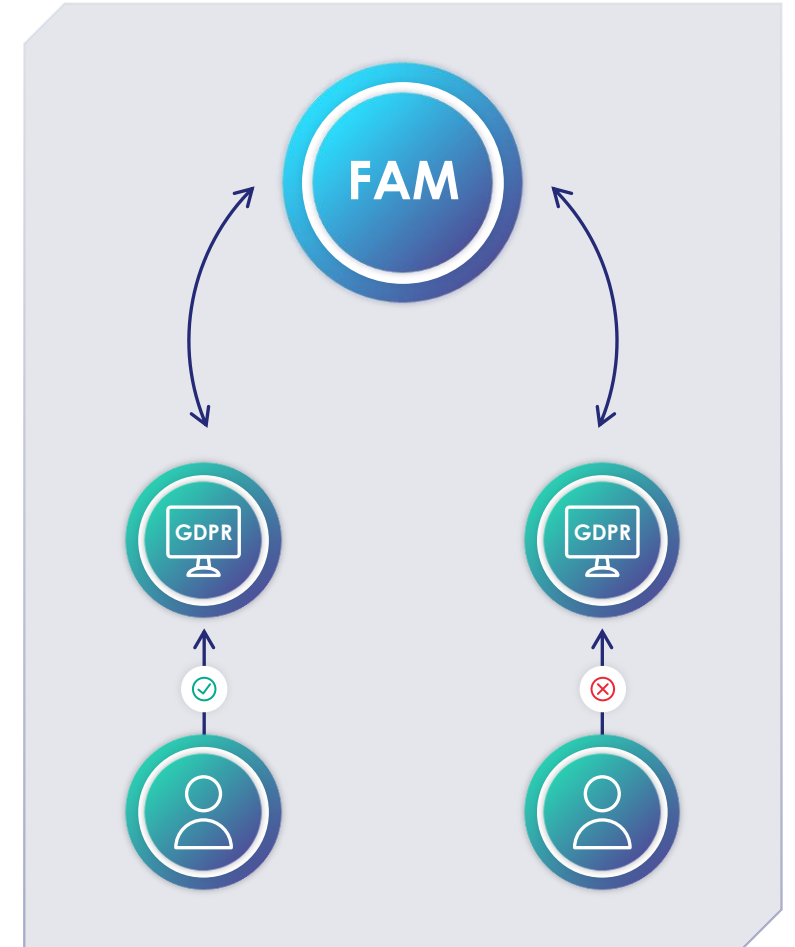
## Use Case: Uncover unauthorized access to GDPR sensitive data

Michael, an employee of the organization, reads GDPR sensitive data from one Windows local storage

Michael is a contractor that shouldn't access GDPR sensitive data

Using a playbook, Michael's activity can be blocked on the data source, until the permissions of Michael are properly updated

**Using Thales FAM activity monitoring & DDC, the compliance manager caught this GDPR violation, put proper controls in place, and saved the organization from being fined by regulators**



# Compliance Management Use Case

Comply with GDPR

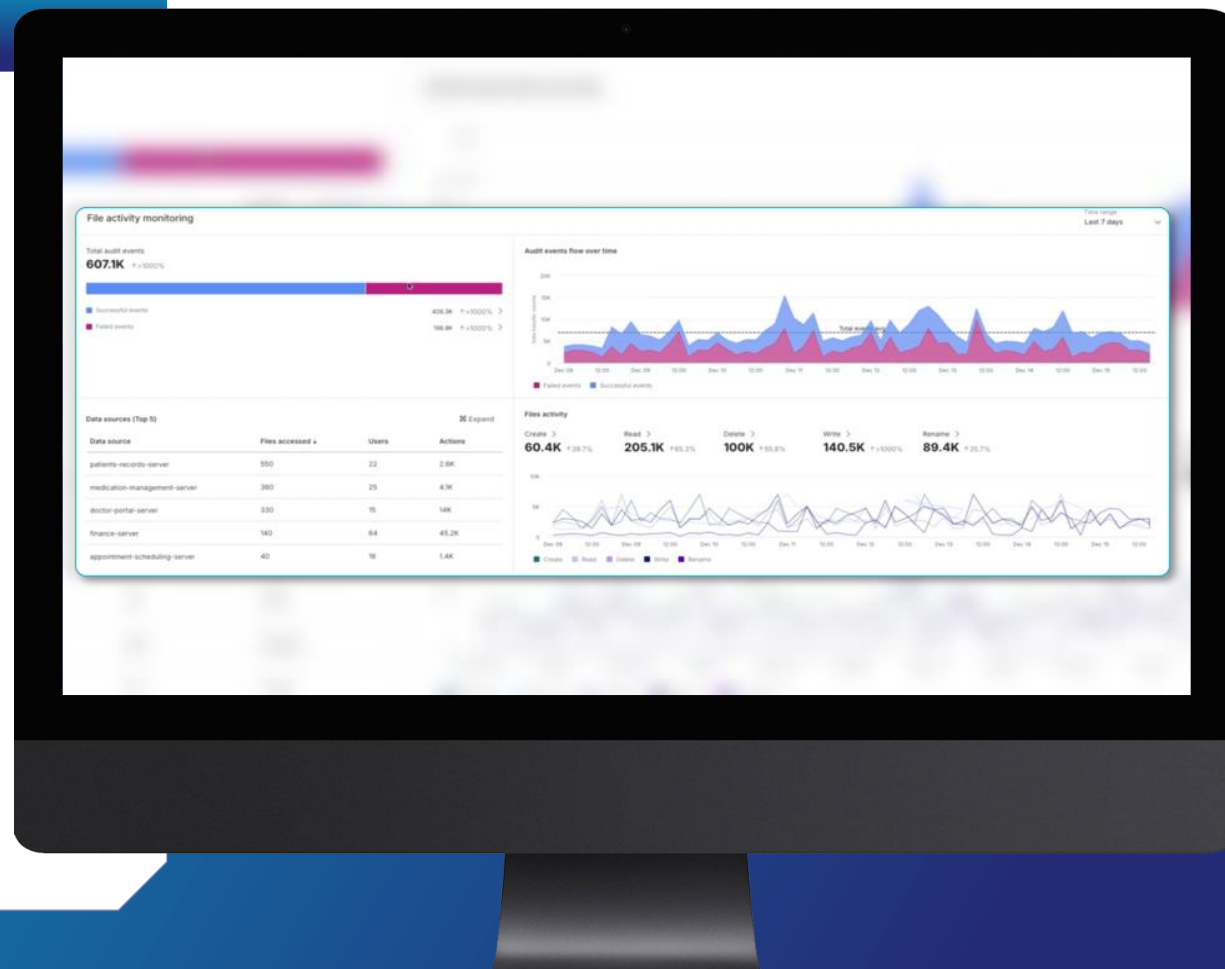
## Use Case: Demonstrate compliance proof to the auditor

An auditor requests evidence that the organization has been auditing access to sensitive GDPR-regulated data over the past five years

The compliance manager uses the FAM dashboard to present audit monitoring statistics, including the number of files monitored over a given period, the types of operations performed, and a breakdown of successful vs. failed access attempts by users

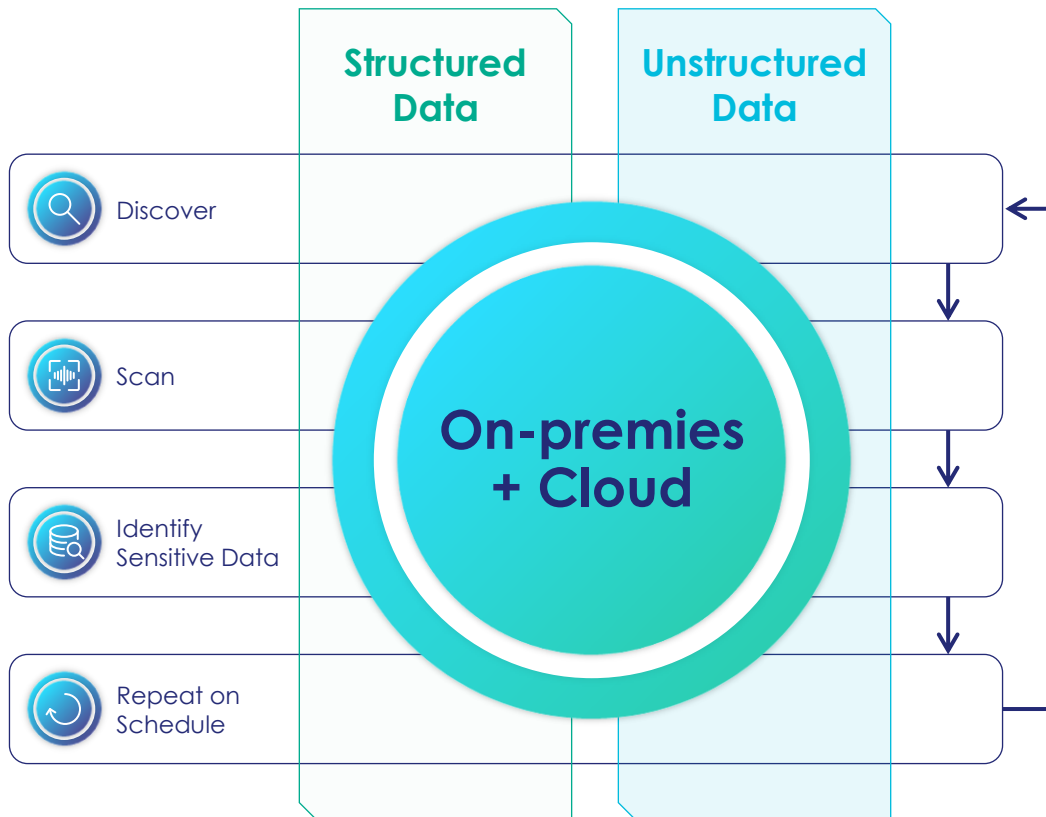
From the FAM dashboard, the compliance manager drills into the reporting platform, filters for GDPR-classified data accessed within the last five years, and generates a report or dashboard tailored to the auditor's request

**Using Thales FAM, the organization can demonstrate GDPR compliance—in minutes**



# Full Visibility of Data Use Case

Know exactly where all HIPAA data is located



## Use Case: Ensuring full visibility of HIPAA data

In the FAM dashboard, a data security engineer can view high-level statistics and insights on the data scanned by Data Discovery and Classification (DDC) across the organization

- The number of scanned files identified as sensitive
- Which data sources contain the highest concentration of sensitive data
- The most prevalent classification profiles
- The geographic distribution of sensitive data by classification type

If a significant amount of HIPAA-regulated data is in Spain, the data security engineer can drill down from the FAM dashboard into the Data Source Inventory to verify that all sources containing HIPAA data are actively monitored

If any source is not being monitored, it can be added with a single click

**Using Thales FAM, the data security engineer gains full visibility into the location of HIPAA-sensitive data, ensuring it is continuously audited for both compliance and security purposes**





## Identify What Data Is Encrypted... and What Data Isn't Encrypted

Unstructured data often holds sensitive information in vulnerable locations like file shares and cloud storage. Encrypting it is essential to prevent unauthorized access or data breaches.

**Thales File Activity Monitoring** tracks encryption status to help identify unprotected files, enforce security policies, and maintain compliance with data protection regulations.

# Coverage & Timeline

**Use Case:** Investigating suspicious file access patterns

During a routine dashboard review, the SOC engineer notices an unusual spike in activity

A Microsoft 365 SharePoint Online data source, which typically sees around 100 daily access events, has suddenly recorded 100,000 access events in a single day

To investigate, the engineer opens the Thales FAM Data Security Assistant and begins querying the anomaly using natural language

**Armed with this information—retrieved effortlessly via the Data Security Assistant—the SOC engineer can quickly assess whether the behavior is legitimate (e.g., a planned data migration or review) or a potential insider threat that warrants immediate response.**

**“Who normally accesses the Microsoft 365 SharePoint Online data source?”**

The assistant returns a list of six users:

- Shiri
- Maya
- Steve
- Bill
- Mor
- Tyson
















**“How many files did each user access each day over the past week?”**

The assistant reveals that all users, except Shiri, accessed a consistent number of files each day. However, Shiri accessed an abnormally high number of files today.

**“Show me the list of files Shiri accessed today, along with their sensitivity and classification profile.”**

The assistant provides a detailed breakdown, including whether each file is marked as sensitive and how it's classified (e.g., PII, HIPAA, confidential IP)

# Coverage & Timeline

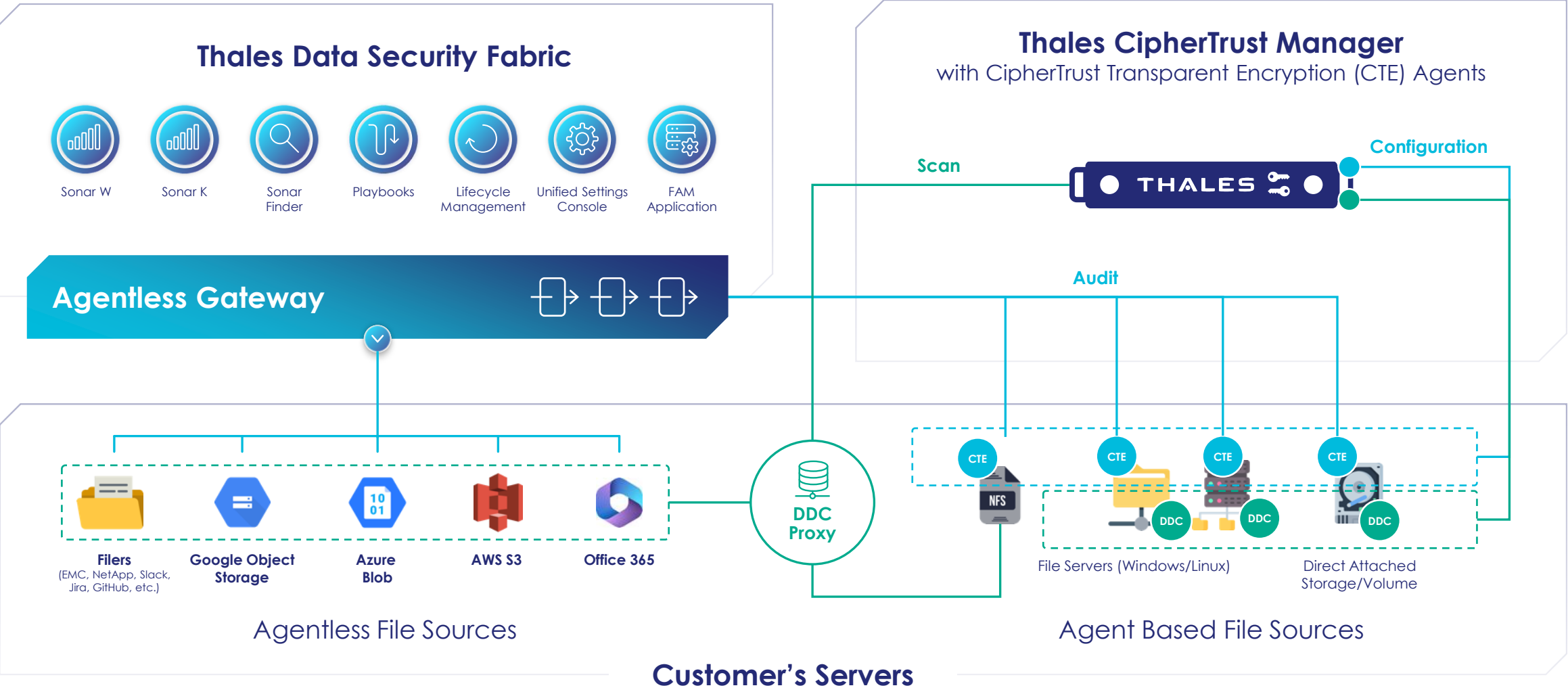
	Q2 2025	Q3 2025	Q4 2025	2026
<div>  <div> Agent Monitoring </div> </div>	<div>  Local storage Windows </div> <div>  Local storage Linux </div> <div>  Network storage NFS Share </div> <div>  Network storage SMB/CIFS Share </div>			
<div>  <div> Agentless Monitoring </div> </div>	<div>  Microsoft 365 One Drive </div> <div>  Microsoft 365 SharePoint on-line </div> <div>  Microsoft 365 Exchange on-line </div>	<div>  Google Drive </div>	<div>  AWS S3 </div>	<div>  Microsoft Teams </div> <div>  Microsoft Azure blobs </div> <div>  Salesforce </div> <div>  Confluence </div>



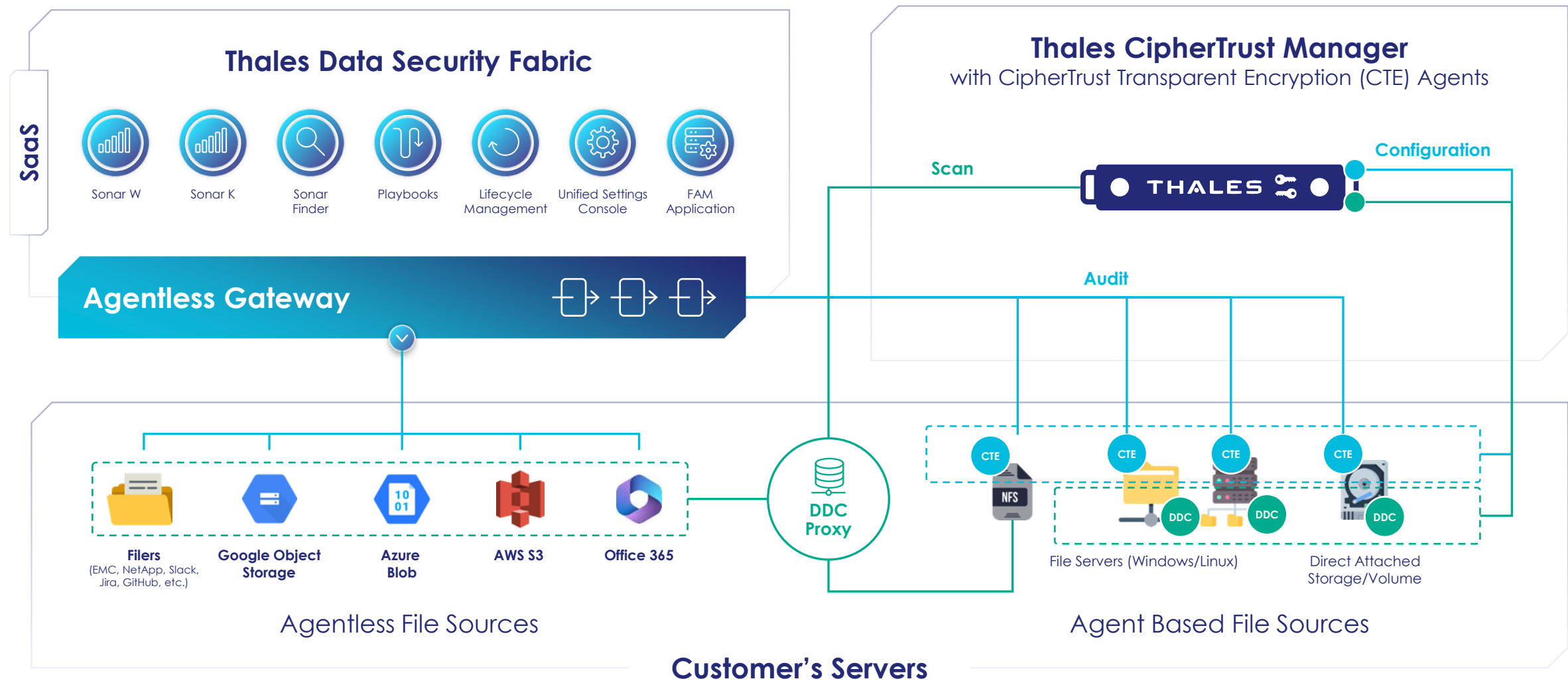


# POLL QUESTION:2

# FAM High-Level Design



# FAM SaaS – Roadmap







# POLL QUESTION:3

# Feature Roadmap

## Q2 2025 – FAM GA



File Activity  
Monitoring



Uncovering  
Sensitive Data

## 2026 and beyond



File Entitlement  
Management



Proactive Threat  
Detection



Threat  
Response



## File Activity Monitoring Video

Seeing is believing!





# QUESTIONS?



# Thank you

[www.thalesgroup.com](http://www.thalesgroup.com)