THALES
Building a future we can all trust

Thales Trusted Cyber Technologies

Ryan Hodges
Rich Johnson
Joe Bedard

Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies: Who We Are

Trusted, U.S. Provider of Cybersecurity Solutions Dedicated to the U.S. Federal Government

Corporate Snapshot

- Business Area of Thales Defense & Security Inc.
- President: Lloyd Mitchell
- Headquarters: Abingdon, MD
- Maintain required U.S. Federal Government approvals and certifications to develop, support and sell products to government clients
  - Proxy Agreement with DCSA for Foreign Ownership, Control and Influence (FOCI)
  - National Security Agreement with the Committee on Foreign Investment in the United States (CFIUS).
- Trusted U.S. Source of Supply of Key Technologies for the Federal Government
- Provide U.S. based support for all products developed and sold through Thales Trusted Cyber Technologies

U.S. Support | Cleared Employees| U.S. Manufacturing

Development

Design core solutions for U.S. Federal agencies with code maintained & compiled by Thales TCT

Commercial to Type 1 development capabilities
All R&D is onshore with only U.S. citizens (75%+ cleared)

We mitigate the risk associated with procuring solutions developed outside of the U.S.

Manufacturing

Provide core solutions that have a U.S. supply chain lifecycle

Rigid supply chain risk mitigation process including a Vendor Approval Process prohibiting the use of tainted or counterfeit components

Trusted/controlled distribution, delivery, and warehousing

Sales

Maintain all government approvals and certifications of products required by U.S. Federal agencies

All customer information maintained exclusively by Thales TCT for both core and resale product sales

All U.S. citizen sales team

Support

All Technical and Sales support is onshore with only U.S. citizens

Fully cleared support Levels 1-3

Web, email and phone support

24x7x365 support available

On-site services available

Federally-focused Solutions to Mitigate Risk

Zero Trust

Cloud Security

Data Protection

PKI Security

Network Encryption

Identity & Access Mgmt

Application Security

Quantum

Edge Security

Ransomware Prevention

Robotic Process Automation

AI Security

Security Where You Need It, Delivered On Your Terms

Protect anything

- Big data
- Intellectual Property
- Financial data
- Enterprise data
- Identities of things
- Payments & digital transactions

Protect anywhere

- Applications
- Data centers
- Containers
- Networks
- Virtual
- Clouds

Delivered any way

- On-premises hardware or software
- Hybrid cloud & on-premises
- As a service

Integrating with Existing IT Infrastructure

Certificate Services (PKI)

EJBCA PKI by PrimeKey, Information Security Corporation, Microsoft, HID, axway, AppViewX, VENAFI, ENTRUST, redhat, IBM, digicert, neXus

Identity & Access MGMT

UiPath, blueprism, Ping Identity, ORACLE, IBM, RSA, HID, versasec, XTEC, SailPoint

Web Firewall/Gateway

paloalto networks, IRON, Microsoft, BROADCOM, FORTINET, f5, Ping Identity

Cloud Services

aws, IBM, McAfee Together is power., CipherCloud, Microsoft Azure, BROADCOM

Card MGMT Issuance

HID, THALES, Microsoft, ORACLE, ENTRUST, intercede

DB/File Encryption

protegrity, Microsoft, ORACLE, NetLib Security, CLOUDERA

Key Management (HSM)

CERTES NETWORKS, IBM

Rights Management

BROADCOM, Microsoft, TITUS, GigaTrust

Password Protection

SSH.COM, CYBERARK, BeyondTrust, HashiCorp

Web Services

IBM, ORACLE, redhat, APACHE SOFTWARE FOUNDATION

Robotic Process Automation

UiPath, blueprism

Code Signing

ENTRUST, Microsoft, BROADCOM

Digital Signatures

Adobe, Microsoft, EJBCA PKI by PrimeKey, ENTRUST

DNSSEC

debian, Infoblox

Data Storage, Big Data Key MGMT

PURESTORAGE, mongoDB, IBM DB2, NUTANIX, NetApp, vmware READY vSAN, Hewlett Packard Enterprise, DELL EMC, ctera, PANASAS

TDE Key MGMT

ORACLE EXADATA, Microsoft SQL Server, ORACLE

Cloud Key MGMT

Azure, Office 365, Google Cloud, salesforce, aws

Home-grown apps, web servers, CAs

Microsoft, APACHE, HashiCorp, ORACLE, NGINX

THALES
Building a future we can all trust

Data Security Fabric

Protecting data and all paths to it

Thales Trusted Cyber Technologies

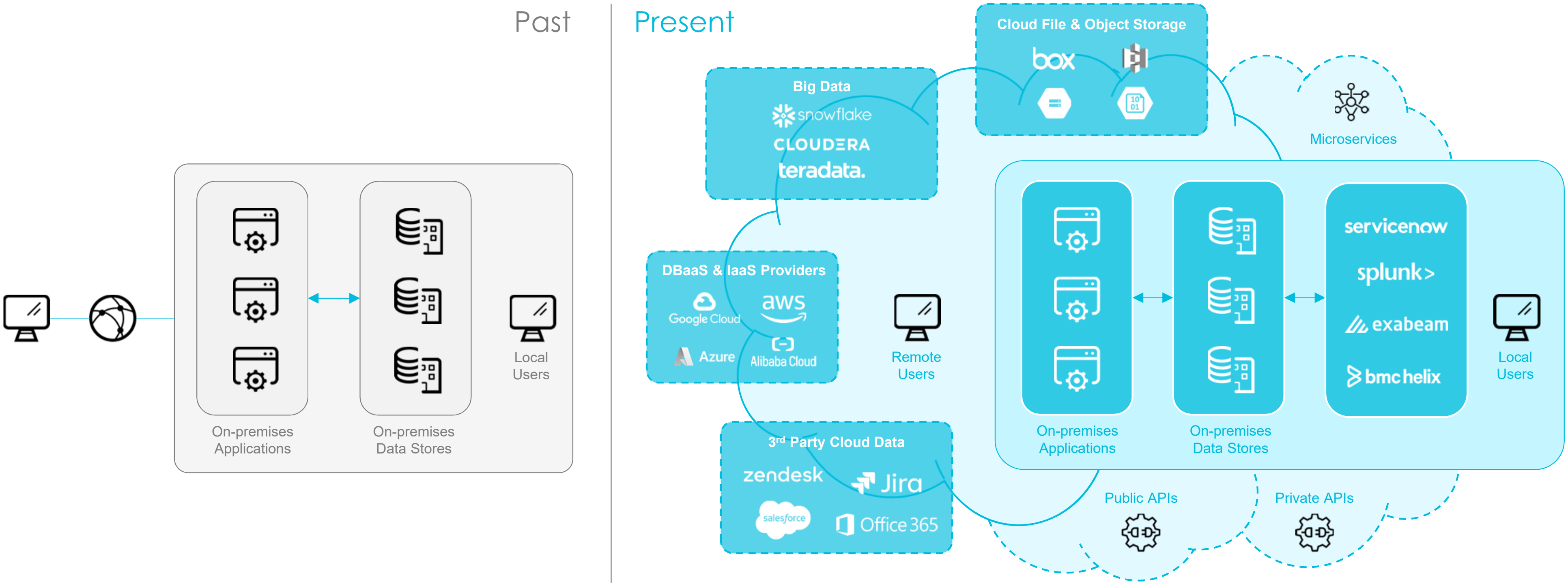
Agenda

- Introduction
- Define the Data Security Problem
- Demo how DSF solves the problem
- Unique Features of Data Security Fabric
- Demonstration
- Questions

Evolution of data workloads

Distributed & cloud technologies are powerful but tend to create management complexity

- Organizations have data workloads beyond relational databases: non-relational, data lakes, business intelligence apps, AI models, etc.
- Organizations are undergoing modernization efforts (e.g., DevOps, microservices, multicloud)
- CISOs must protect a broader digital surface area, which has more attack vectors and risks



Data Security Questions

Along with benefits, new technologies come with security challenges & needs

Key use cases driving business needs

We have a **data inventory** problem. Where is my sensitive data? How do I get visibility?

I have both data **compliance & security needs**; how can I simplify solving for both?

Who is accessing my data in these disparate locations?

How can I get the most value from my data source logs to **understand our risk?**

Are my databases configured securely?
Is data encrypted?

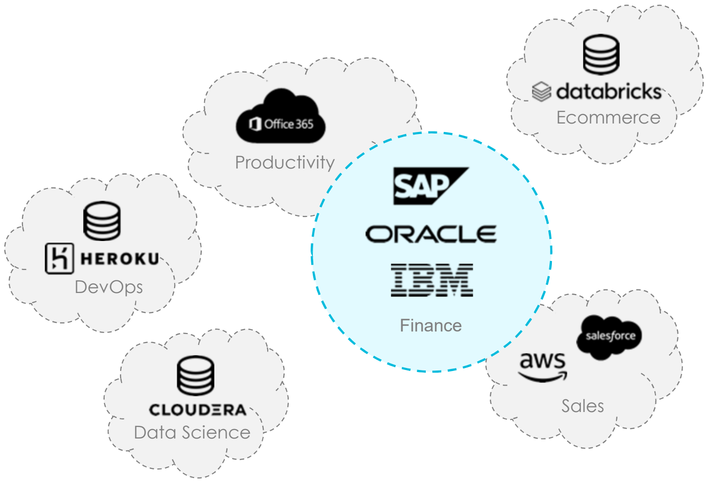
How can I get an actionable view of my **monitored data?**

Evolving technologies driving new use cases

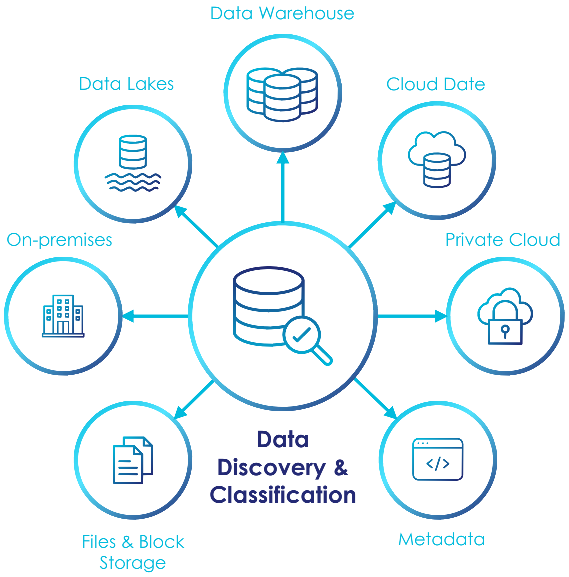
- Artificial Intelligence & Machine Learning
- Microservices
- 3rd Party Cloud Data
- DBaaS & IaaS Providers
- Cloud File and Object Storage
- Public APIs

We have a data inventory problem. Where is my sensitive data? How do I get visibility?

More-and-more users and apps on connected, yet siloed, systems make it hard to discover sensitive data and have oversight or manage access across data sources



Thales automatically discovers your data stores across on-premises, hybrid, and multicloud environments to help you protect and manage your sensitive data



- **Autodiscover:** Across AWS, Azure, GCP, OCI, Alibaba, etc. & on-premises
- **Classification:** Pinpoint and categorize sensitive data across all platforms
- **Tracking & unified view:** What, Why, Who, When, Where monitoring, risk analysis, & rapid response

Who is accessing our data and what are they doing with it?

Database Activiy Monitoring

```
select SCN, TO_CHAR(CAST(EVENT_TIMESTAMP_UTC AS
TIMESTAMP), '**0') as "TIMESTAMP", ADDITIONAL_INFO,
AUDIT_TYPE, SESSIONID, OS_USERNAME as "CLIENT
USER", USERHOST, TERMINAL as "CLIENT TERMINAL",
CLIENT_PROGRAM_NAME, AUTHENTICATION_TYPE,
DBUSERNAME, STATEMENT_ID, ENTRY_ID, ACTION_NAME
as ACTION, RETURN_CODE as RETURNCODE,
OS_PROCESS, OBJECT_SCHEMA, OBJECT_NAME as
OBJ$NAME, DBID, SQL_TEXT, APPLICATION_CONTEXTS,
CLIENT_IDENTIFIER, DBLINK_INFO, INSTANCE_ID,
PROXY_SESSIONID, SQL_BINDS,
SYSTEM_PRIVILEGE_USED, CLIENT_PROGRAM_NAME,
UNIFIED_AUDIT_POLICIES, XS_SESSIONID,
XS_USER_NAME, TRANSACTION_ID, NEW_SCHEMA,
NEW_NAME, ROLE, SYS_CONTEXT('**1','**2') as
DATABASE_NAME from UNIFIED_AUDIT_TRAIL WHERE
'**3'='**3' AND EVENT_TIMESTAMP_UTC > CAST('**4' AS
TIMESTAMP) AND EVENT_TIMESTAMP_UTC <= CAST('**5' AS
TIMESTAMP)
```

- Limited database security expertise
- Each database has own security controls
- Logs do not give visibility into sensitive data
- Severity of the threat is unknown
- Too many alerts to process
- Too many tools to manage
- Operational frustrations (translation: what do we do with all the information we are getting?)

Thousands to millions of events like these daily

Data Security Compliance within the DoD and Civilian Departments

Along with benefits, new technologies come with security challenges & needs

Key use cases driving business needs

Revolve around requirements as enumerated in an Authorization to Operate (ATO)

Assessment of security control implementation from relevant controls selected from NIST SP 800-53

- Access Controls (AC)
- Audit and Accountability (AU)
- Security Assessment and Authorization (SC)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Privacy Reporting (PM)

Zero Trust Architecture Directives

- **Data Pillar**
- **Visibility & Analytics**
- **Automation & Orchestration**

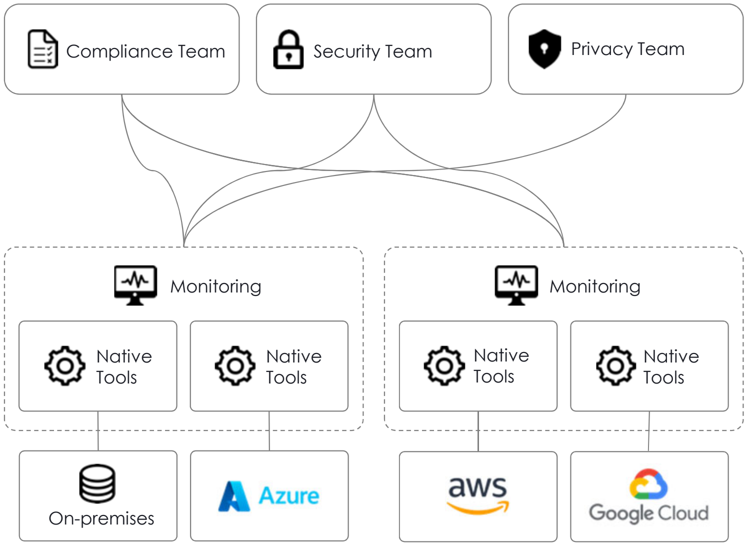
DISA STIG requirements for databases

- **Hardening requirements**
- **Auditing requirements**

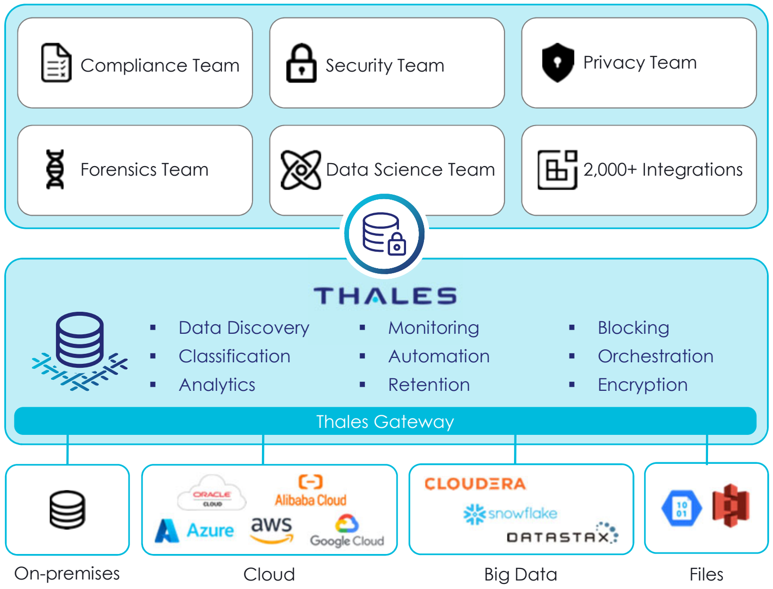
•Successful and unsuccessful attempts to access, modify, and delete categories (classification) of information
•Successful and unsuccessful attempts to access, modify and delete security objects
•Enforcement of access restrictions associate with changes to configuration
•Successful and unsuccessful attempts to add, modify and delete privileges/permissions
•Logins and logouts
•Unsuccessful logins
•Concurrent logins by same user from different workstations
•Unsuccessful access to objects
•All direct access (outside of a frontend application such as a web application that it supports)

How can I get an actionable view of my monitored data?

Log files deliver a high volume of rich usage data at a high velocity; need to bridge and unify data from diverse sources & systems with better and faster visibility for insights



- Thales offers unified visibility, encryption, control, automation, and insights across the entire data estate - delivering comprehensive and centralized management via a single service or dashboard
- Enable previously siloed teams secure access to data stores to unlock new business innovations and insights



Data Security's value goes far beyond Compliance

Supports a broad range of business needs across the organization

Safely Accelerate
Business Transformation
CISO/CIO

How can I protect my data and ensure compliance across multiple clouds?

OTHER BUSINESS NEEDS

- How do I embrace new technologies to help transform my businesses?
- How do I protect my data as I move apps and services to the cloud for agility and speed?
- How can I reduce my CAPEX while using the cloud to to quickly scale?

Drive
Data Security
Security & IT Professionals

I have both data security & compliance needs; how can I simplify solving for both?

OTHER BUSINESS NEEDS

- How do I protect data from external attacks, e.g., ransomware, SQL Injection, malware, etc.?
- How do I detect and mitigate insider threats, e.g., misuse, compromised credentials, etc.?
- How do I prevent social engineering attacks and vulnerability exploits?
- How do I gain visibility of all data traffic, access, digital assets, and data stores?
- Can you help me apply Zero Trust principles to my organization?

Understand & Manage
Risk
Internal Audit & Executives

How can I get the most value from my data source logs to understand our risk?

OTHER BUSINESS NEEDS

- How do I reduce organizational risk associated with sensitive data?
- How can I proactively assess my risk posture including my vulnerabilities?
- How can I orchestrate and automate risk management?

Enable
Analytics & Insights
IT, Security & SOC Engineers

How can I get an actionable view of my monitored data estate?

OTHER BUSINESS NEEDS

- How do I consolidate alerts & normalize insights?
- How do I shorten SOC's critical incident detection and response times?
- How can I accelerate risk resolution for business users?

Ensure
Compliance
Executives & Compliance

I have both data compliance & security needs; how can I simplify solving for both?

OTHER BUSINESS NEEDS

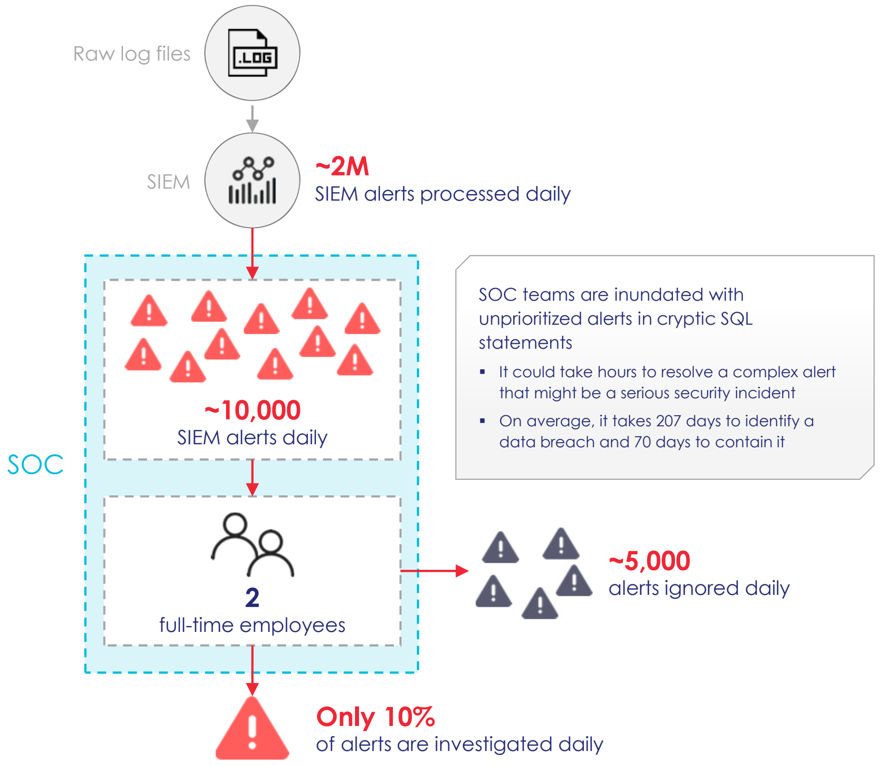
- Can you help me avoid fines & penalties with audit trails & compliance reports?
- How can I comply with global regs & privacy laws: SOX, PCI, NYDFS, HIPAA, SOC 2, GDPR, CPRA, etc., and pass my audits?
- How can I comply with industry standards like COBIT, ISO/IEC 38500, & ISO/TC 215?
- How do I consolidate compliance efforts for all data types and data stores?
- Can you help me with my cybersecurity insurance?

Sensitive Data
Discovery & Classification
Technical LOB staff

OTHER BUSINESS NEEDS

- How do I discover ungoverned data repositories?
- How do I classify data types for compliance and audits?

How can I get the most value from my data source logs (database audit) to understand our risk?



Raw log files

SIEM

~2M
SIEM alerts processed daily

SOC

~10,000
SIEM alerts daily

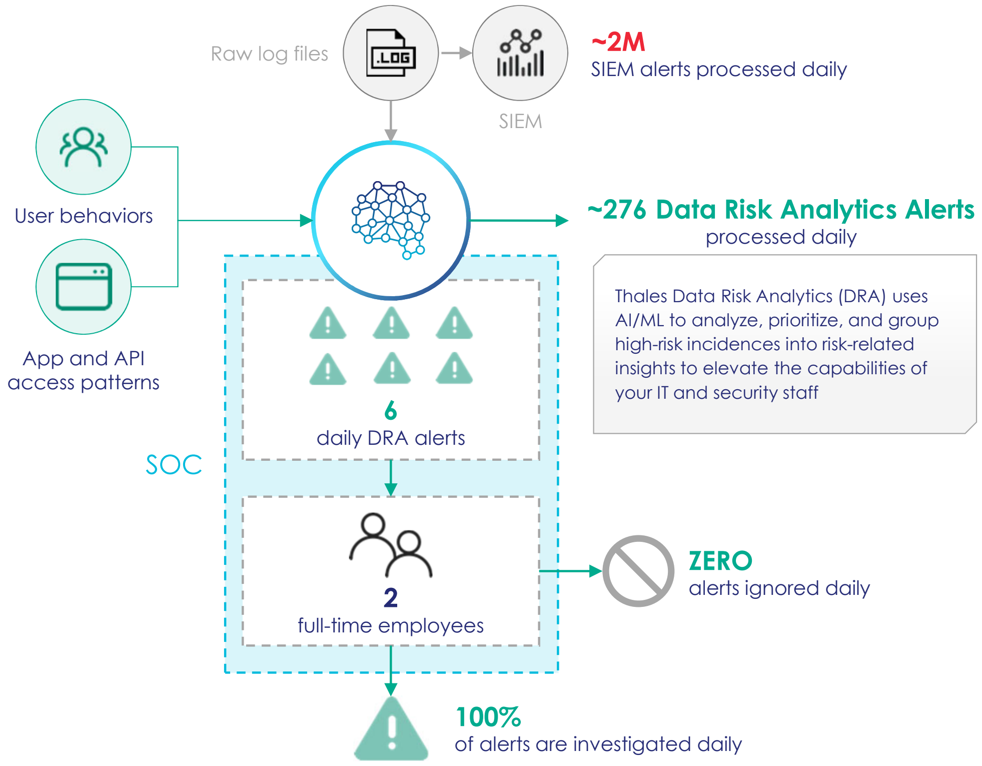
SOC teams are inundated with unprioritized alerts in cryptic SQL statements

- It could take hours to resolve a complex alert that might be a serious security incident
- On average, it takes 207 days to identify a data breach and 70 days to contain it

2
full-time employees

~5,000
alerts ignored daily

Only 10%
of alerts are investigated daily



Raw log files

SIEM

~2M
SIEM alerts processed daily

User behaviors

App and API access patterns

~276 Data Risk Analytics Alerts
processed daily

Thales 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

SOC

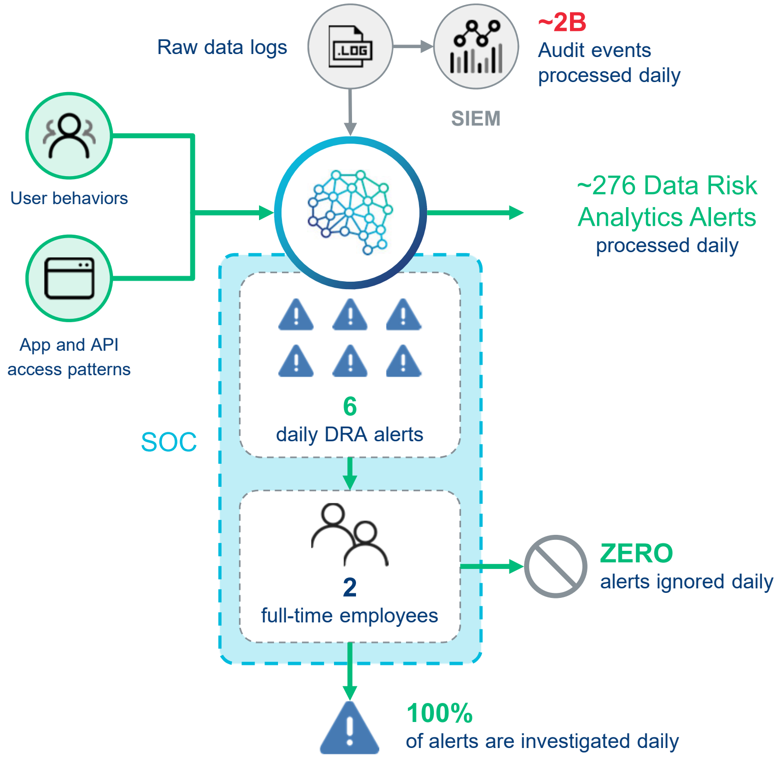
6
daily DRA alerts

2
full-time employees

ZERO
alerts ignored daily

100%
of alerts are investigated daily

Imperva Data Risk Analytics (DRA) Protects your Data

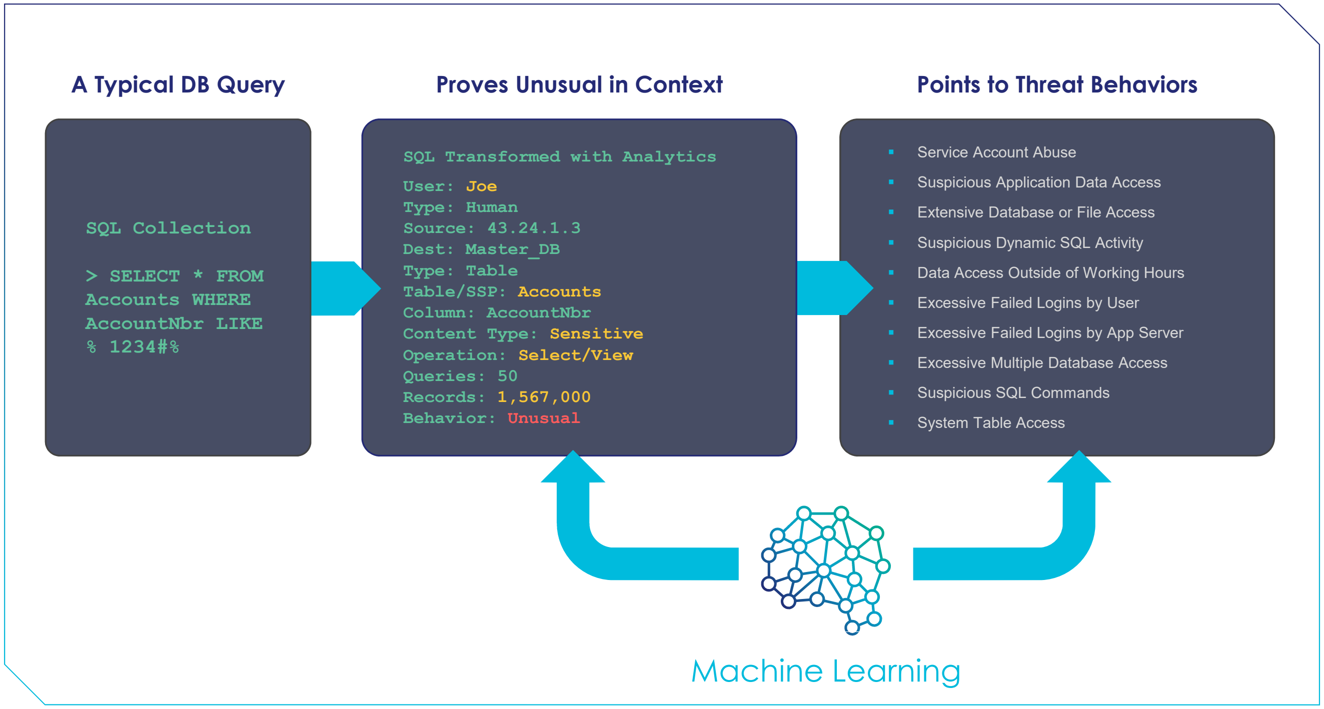

Raw data logs
.LOG
~2B
Audit events processed daily
SIEM
User behaviors
App and API access patterns
~276 Data Risk Analytics Alerts processed daily
SOC
6
daily DRA alerts
2
full-time employees
ZERO
alerts ignored daily
100%
of alerts are investigated daily

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

Leveraging decades of data domain threat research

- Continuous insider and external threat research
- Modeling, building, and testing of anomalous and bad behavior detection with machine learning algorithms
- Seamless translation of database languages into plain English for effortless usage
- Translates Structured Query Language (SQL) to security events that are actionable for the Security Operations Center



A Typical DB Query

```
SQL Collection

> SELECT * FROM
Accounts WHERE
AccountNbr LIKE
% 1234#%
```

Proves Unusual in Context

```
SQL Transformed with Analytics
User: Joe
Type: Human
Source: 43.24.1.3
Dest: Master_DB
Type: Table
Table/SSP: Accounts
Column: AccountNbr
Content Type: Sensitive
Operation: Select/View
Queries: 50
Records: 1,567,000
Behavior: Unusual
```

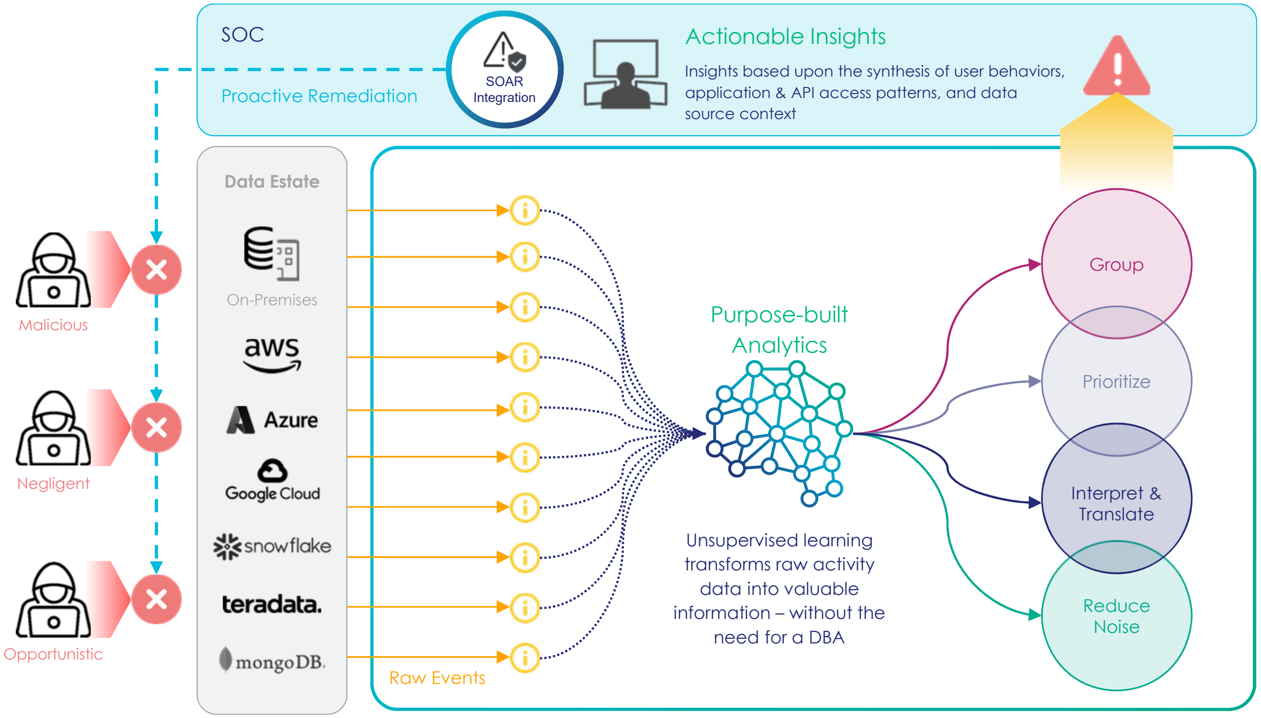
Points to Threat Behaviors

- Service Account Abuse
- Suspicious Application Data Access
- Extensive Database or File Access
- Suspicious Dynamic SQL Activity
- Data Access Outside of Working Hours
- Excessive Failed Logins by User
- Excessive Failed Logins by App Server
- Excessive Multiple Database Access
- Suspicious SQL Commands
- System Table Access

Machine Learning

Data Risk Analytics elevates the security capabilities of IT

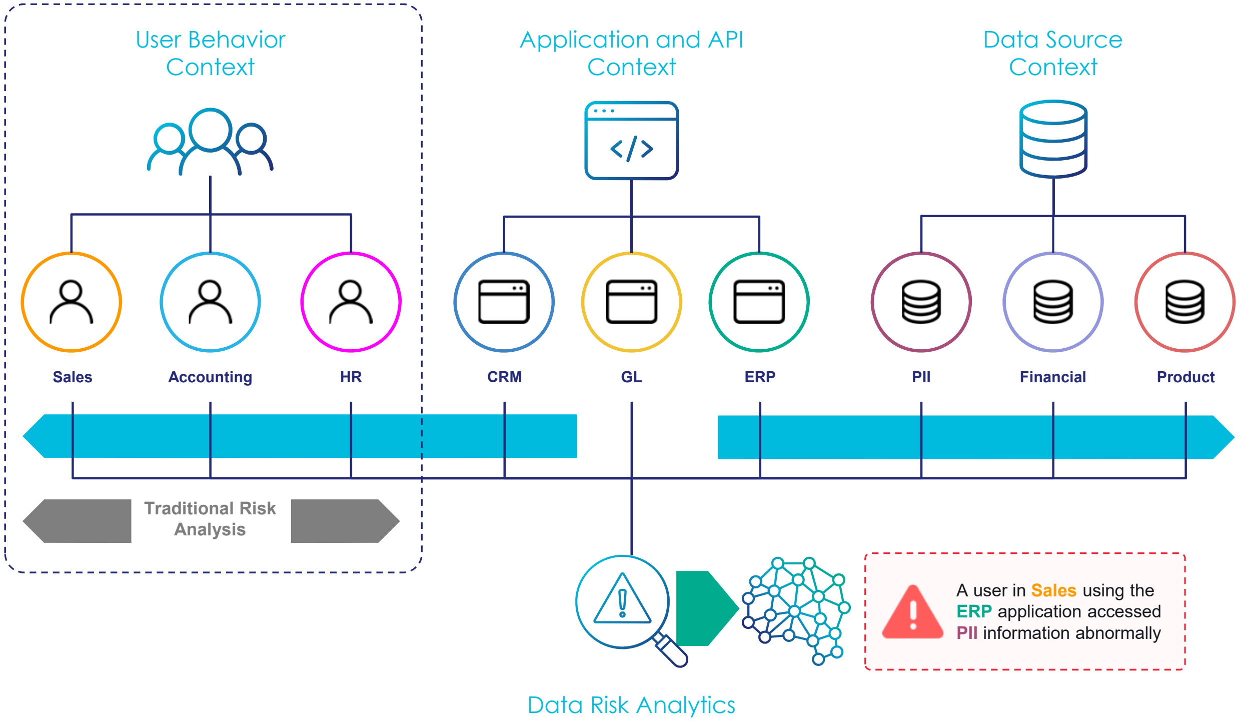
DRA can be the home page for data security in your SOC



DSF Coverage:

- **File servers:** Windows file shares, NFS (Network file system) NAS (Network attached storage), SharePoint
- **AWS:** Amazon Elastic File System (EFS), Amazon Elastic Block Store (EBS), Amazon FSx for Lustre, Amazon FSx for NetApp ONTAP, Amazon Storage Gateway, Amazon FSx for Windows File Server
- **Azure:** Azure Disk Storage, Azure Files, Azure NetApp Files, Azure Elastic SAN
- **GCP:** Google Filestore, Google Persistent Disk
- **Microsoft:** SharePoint online, Microsoft 365, OneDrive

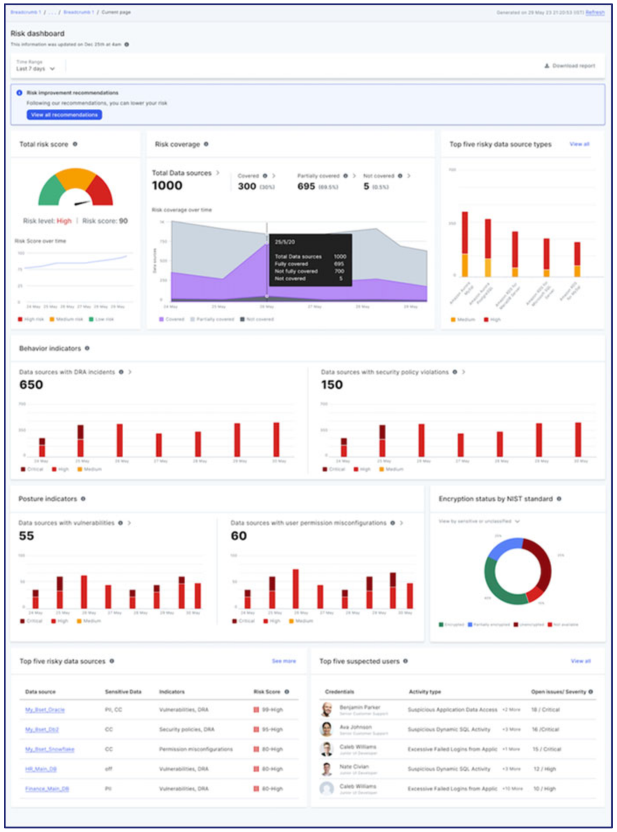
Prioritize and group high-risk incidents to elevate team skills



A user in Sales using the ERP application accessed PII information abnormally

- **No configuration needed**
  Unsupervised learning transforms raw activity data into valuable information – without the need for a DBA
- **Fully automated**
  Events are prioritized based on best practices defined using pre-built or custom models – without the need for a data scientist
- **Unique triangulation**
  Insights based upon the synthesis of user behaviors, application & API access patterns, and data source context

Data Risk Intelligence Application



Risk dashboard

This information was updated on Dec 25th at 4am

Risk improvement recommendations

Following our recommendations, you can lower your risk

Total risk score

Risk coverage

Total Data sources 1000 | Covered 300 (30%) | Partially covered 695 (69.5%) | Not covered 5 (0.5%)

25/5/20

Total Data sources	1000
Fully covered	695
Not fully covered	700
Not covered	5

Top five risky data source types

Behavior indicators

Data sources with DRA incidents 650

Data sources with security policy violations 150

Posture indicators

Data sources with vulnerabilities 55

Data sources with user permission misconfigurations 60

Encryption status by NIST standard

Top five risky data sources

Data source	Sensitive Data	Indicators	Risk Score
My_Bset_Oracle	PII, CC	Vulnerabilities, DRA	99-High
My_Bset_Db2	CC	Security policies, DRA	95-High
My_Bset_Snowflake	CC	Permission misconfigurations	80-High
HR_Main_DB	off	Vulnerabilities, DRA	80-High
Finance_Main_DB	PII	Vulnerabilities, DRA	80-High

Top five suspected users

Credentials	Activity type		Open issues/ Severity
Benjamin Parker	Suspicious Application Data Access	+2 More	18 / Critical
Ava Johnson	Suspicious Dynamic SQL Activity	+3 More	16 /Critical
Caleb Williams	Excessive Failed Logins from Applic	+1 More	15 / Critical
Nate Civian	Suspicious Dynamic SQL Activity	+3 More	12 / High
Caleb Williams	Excessive Failed Logins from Applic	+10 More	10 / High

Value Proposition (Beta - Q2, Q3 2024; GA - Q42024)

- **Goal 1: Provide executives with a clear understanding of their organization's data risk coverage**
- **Goal 2: Empowering data security experts to quickly prioritize, understand, and respond to data risk alerts**
- **Goal 3: Prioritize specific indicators and data sources in risk score**

Customer Benefits

- **Reduce TCO: achieve the highest return on investment in data security**
  - Actionable and prioritized insights that ease the day-to-day work
  - Need fewer security resources to protect the organization's data, as Imperva DSF bridges the knowledge gap
- **Shorten data risk management cycles: via automated prioritization and mitigation**

Modernizing data security

The evolution of risk management

Orgaizations get stuck here

Data Management

Streamline data collection to elevate operational focus from collection to **consumption**.

Ingest, consolidate and store any data feed

Agents or agentless

high value data to **empower new use cases** and users.

Unified enterprise view

Contextual enrichment

Self-service reporting

Interpretation

Exploit **extensible analytics** to distill data and decision trees into **manageable information.**

SOC/Splunk optimization

Complex correlations

Flexible UEBA engines

Operationalize

Leverage automation to transform manual efforts into **efficient business processes.**

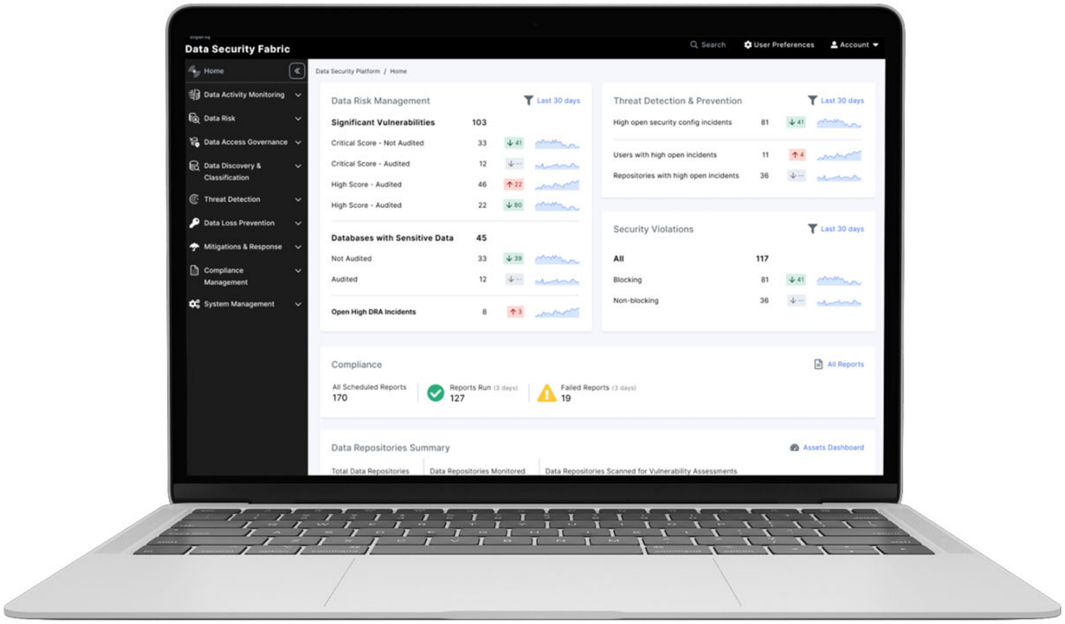
Cross-silo workflows

Enterprise integrations

Integrated SOAR

And never quite reap the value of their efforts

DSF unifies visibility, control, workflow automation, and insights



Data Risk Management — Last 30 days

Significant Vulnerabilities	103		
Critical Score - Not Audited	33	↓ 41	
Critical Score - Audited	12	↓ --	
High Score - Audited	46	↑ 22	
High Score - Audited	22	↓ 80	
Databases with Sensitive Data	45		
Not Audited	33	↓ 39	
Audited	12	↓ --	
Open High DRA Incidents	8	↑ 3	

Threat Detection & Prevention — Last 30 days

High open security config incidents	81	↓ 41
Users with high open incidents	11	↑ 4
Repositories with high open incidents	36	↓ --

Security Violations — Last 30 days

All	117	
Blocking	81	↓ 41
Non-blocking	36	↓ --

Compliance — All Reports

All Scheduled Reports 170 | ✓ Reports Run (3 days) 127 | ⚠ Failed Reports (3 days) 19

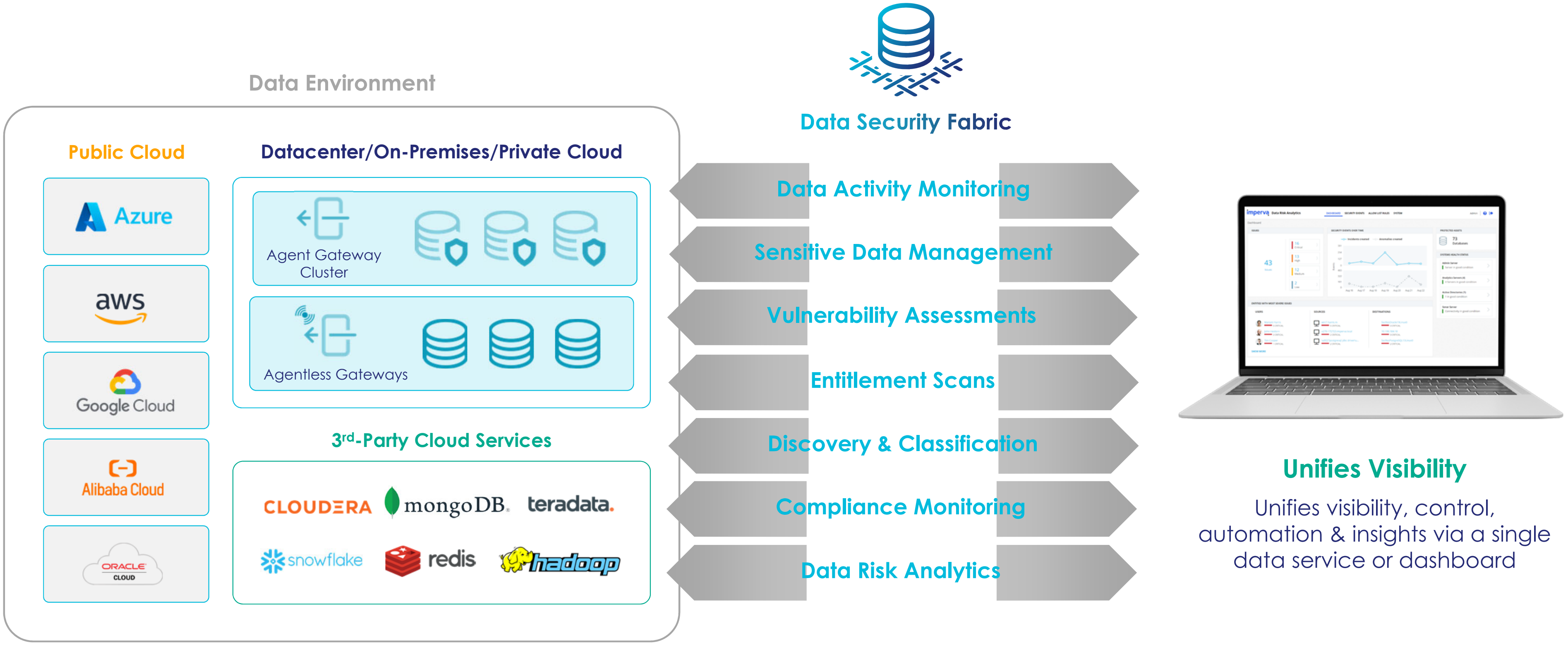
Data Repositories Summary — Assets Dashboard

Total Data Repositories | Data Repositories Monitored | Data Repositories Scanned for Vulnerability Assessments

- Protect data by understanding and controlling access by users, processes, and apps within a single service view
- Gain full enterprise visibility of multicloud and hybrid threats, risk and activity across the entire data environment
- Detect anomalous and bad behavior with Machine Learning algorithms

Actionable insights automation

Imperva DSF provides a streamlined views that help customers automate their audit and security risk response and compliance processes



Unifies Visibility

Unifies visibility, control, automation & insights via a single data service or dashboard

THALES
Building a future we can all trust

Questions?

Ryan Hodges
443-910-1245
ryan.hodges@thalestct.com