imperva

Imperva Data Security

European Union Network and Information Systems Directive (NIS2)

Mohamed Lallouch
Data Security Specialist
Mohamed@lallouch@Imperva.com

EU Network & Information Systems Directive (NIS2)

- NIS2 revises the EU's Network and Information Systems Directive originally adopted in 2016.

- Its purpose is to enhance cybersecurity capabilities for organizations' network and information systems in response to increased cyberattacks.

- NIS2 expands the original NIS Directive to now cover more **industry sectors**, with additional **risk-management measures** and incident **reporting obligations**. It also provides for stronger **enforcement**.

- As an EU Directive adopted in January 2023, all 27 EU member states must implement the NIS2 Directive into their national laws by October 2024.

Source: European Commission

Summary of NIS2 Key changes from NIS1 include:

1: EXPANDED SCOPE

NIS2 extends its reach to a greater number of sectors, considering them essential or critical. This expansion encompasses more organizations, such as essential service providers, digital service providers, and other vital sectors.

2: MORE STRINGENT SECURITY REQUIREMENTS

The directive enforces stricter cybersecurity measures. These requirements involve risk management practices, technical and organisational measures, incident response and recovery plans, employee training, and frequent updates and patching.

3: INCIDENT REPORTING

NIS2 requires organizations to report significant cybersecurity incidents more efficiently, using a standardised format and a shortened reporting timeframe of 24 hours, as opposed to the previous 72-hour window under the initial NIS Directive.

4: ENFORCEMENT THROUGH PENALTIES

The NIS2 Directive imposes more severe penalties for non-compliance, including increased financial penalties (up to 10 million euros or 2% of an organisation's global annual turnover, whichever is higher) and potential legal repercussions

NIS2 Scope

Industry Sectors

Essential

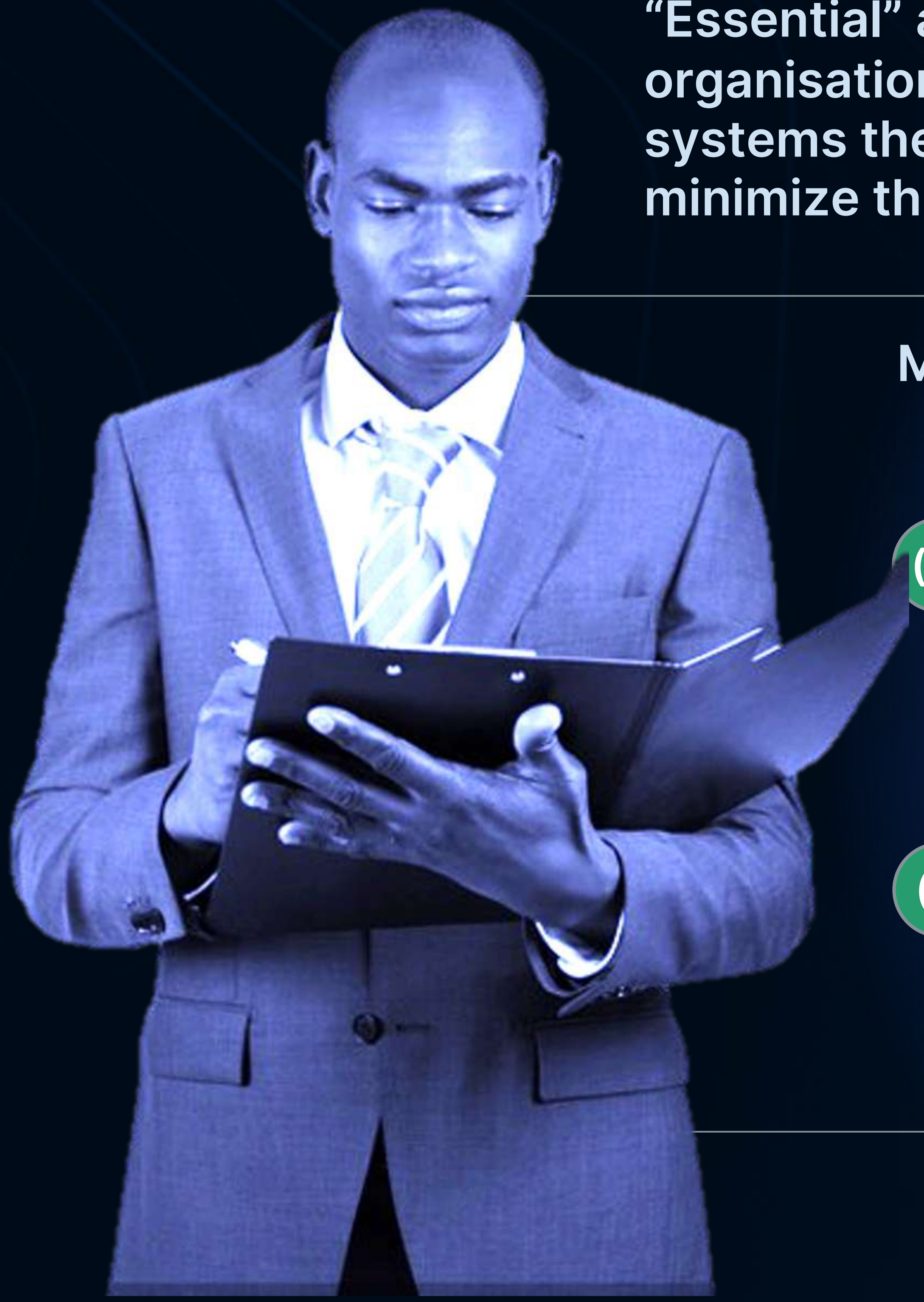
- NIS Healthcare
- NIS Transport
- NIS Digital Infrastructure
- NIS Water Supply
- NIS Banking
- NIS Financial Market Infra.
- NIS Energy
- New: NIS2 Digital Service Providers
- New: NIS2 Waste Management
- New: NIS2 Pharma. & Labs.
- New: NIS2 Space
- New: NIS2 Public Admin.

Important

- New: NIS2 Public Comms. Providers
- New: NIS2 Chemicals
- New: NIS2 Food Produces, & Distributors
- New: NIS2 Critical Device Manufacturers
- New: NIS2 Social Networks, Online Marketplaces
- New: NIS2 Post, Courier Services

NIS2 Scope

Cybersecurity risk-management measures (Article 21)



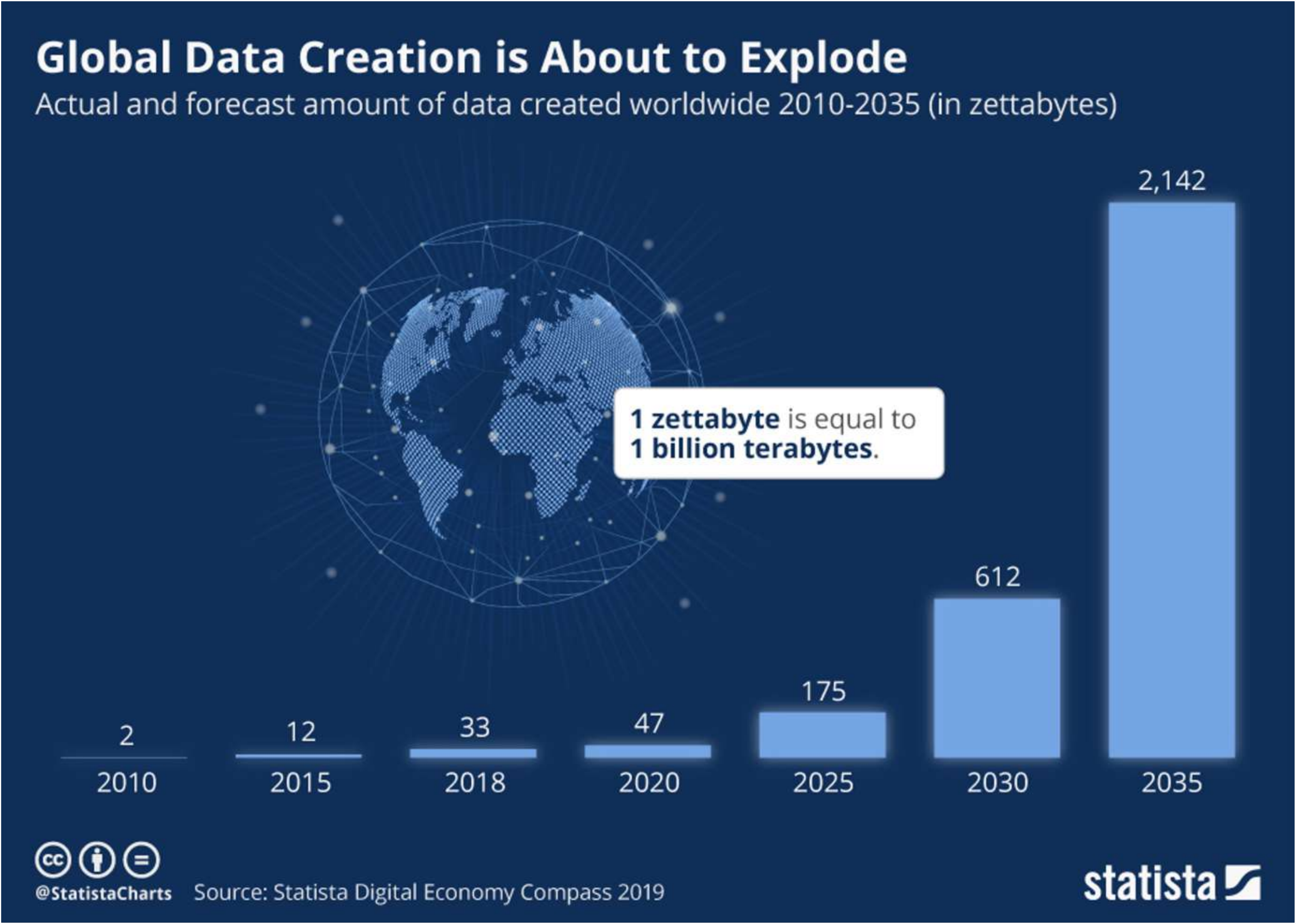
“Essential” and “Important” entities must take appropriate technical, operational and organisational measures to manage risks posed to the security of the network and information systems they use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on their users.

MEASURES FOCUS ON

- (a) Risk Analysis
- (b) Incident Handling
- (c) Business Continuity
- (d) Supply Chain Security
- (e) Security for Network & IT Systems
- (f) Effectiveness of cyber risk management
- (g) Cyber hygiene & cyber Security training
- (h) Cryptography & encryption
- (i) Human resources security
- (j) Multi-factor authentication

NIS2 Scope

Reporting obligations (Article 23)



Global Data Creation is About to Explode

Actual and forecast amount of data created worldwide 2010-2035 (in zettabytes)

1 zettabyte is equal to **1 billion terabytes**.

@StatistaCharts Source: Statista Digital Economy Compass 2019

statista

SHORTENED REPORTING TIMEFRAME

NIS2 requires organizations to report significant cybersecurity incidents more efficiently, using a standardized format.

NOTIFICATION

CSIRT and service recipients must be notified within the defined timeframes.

Within 24 Hours
Provide an 'early warning' that a significant cybersecurity incident is suspected.

Within 72 Hours
Provide an 'initial assessment' with key details about the incident.

Within 72 Hours
Provide a 'final report' that describes the incident, cause, and mitigation efforts.

NIS2 Scope:

Enforcement (Articles 32, 33, 34)

	Essential Entities	Essential Entities
Penalties	***Fines of EUR 10,000,000*** or of a maximum of at least 2% of total worldwide annual turnover	***Fines of EUR 7,000,000*** or of a maximum of at least 1.4% of total worldwide annual turnover
Supervision	■ Must comply with supervision requirement ■ The supervising entity (competent authorities) have the right to enforce specific measure ■ If the entity does not comply within the given deadline the competent authority has the power to suspend managerial responsibility at the CEO or legal representative level	■ Action will be taken if authorities receive evidence and order the entity to carry out specific actions based on audits, and other requirements.

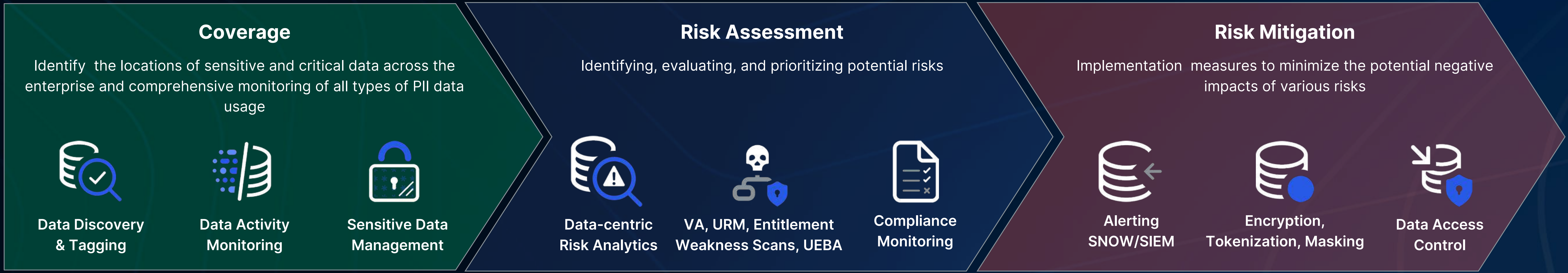
Imperva as Part of Your Overall Cybersecurity Strategy to Support NIS2

Key NIS2 requirements: How Imperva can help

NIS2 obligation category	Articles	How Imperva can help	Services & Deliverables
Risk analysis and information system security policies	21.2(a), (h)(e),(f) Point 125	Identifying the current state of compliance, documenting gaps, and providing a path to full compliance is a critical first step using Imperva's Professional Services team including the industry's largest vulnerability handling and disclosure on databases.	Data Risk Analytics Professional Services Partner Services Vulnerability Management + Zero Trust
Incident handling	21.2(b)	Connecting existing systems through the Imperva Data Security Fabric (DSF) eliminates manual errors and speeds incident handling by opening and updating ServiceNow tickets on all incidents related to NIS2.	Ticketing System Integration Professional Services Partner Services
Business continuity and crisis management	21.2(c)	Implementing preventive measures to predict and avoid crisis situations means that crisis management can be optimized with fewer incidents	Professional Services Partner Services Artificial intelligence
Supply Chain security	21.2(d) Point 90	Monitoring and alerting on anomalies can detect and prevent unwanted activities from disrupting supply chain activities.	Data Activity Monitoring User Rights Management Discovery and Classification
Security in network and information systems	21.2(e), (f) Point 98	Data-centric security, regardless of structured, unstructured, on-prem, or cloud means simple sensors can provide security and compliance across the broadest data environment.	Monitoring Agents and Agentless Data Risk Analytics Blocking Real-time alerting Zero Trust
Testing and auditing	21.2(g)	Comprehensive reports and dashboards that highlight data activity and provide documented evidence of audit and test environments helping in training and cyber hygiene.	Professional Services Partner Services Reports and Portals
Use of cryptography and encryption	21.2(h) Point 51	Encryption, obfuscation, anonymization, tokenization, and masking can be used to protect the privacy and security of regulated data.	Technology Alliance Program
Incident Reporting	21.2(b)	Automatic opening of ServiceNow tickets means reporting is streamlined, documented, and simplified.	Ticketing System Integration Workflows and Integration

Technology Architecture

Data Security Fabric covers important NIS2 risk-management requirements



Coverage

Identify the locations of sensitive and critical data across the enterprise and comprehensive monitoring of all types of PII data usage

- Data Discovery & Tagging
- Data Activity Monitoring
- Sensitive Data Management

Risk Assessment

Identifying, evaluating, and prioritizing potential risks

- Data-centric Risk Analytics
- VA, URM, Entitlement Weakness Scans, UEBA
- Compliance Monitoring

Risk Mitigation

Implementation measures to minimize the potential negative impacts of various risks

- Alerting SNOW/SIEM
- Encryption, Tokenization, Masking
- Data Access Control

Imperva’s unique capabilities for NIS2 Risk Management and Reporting

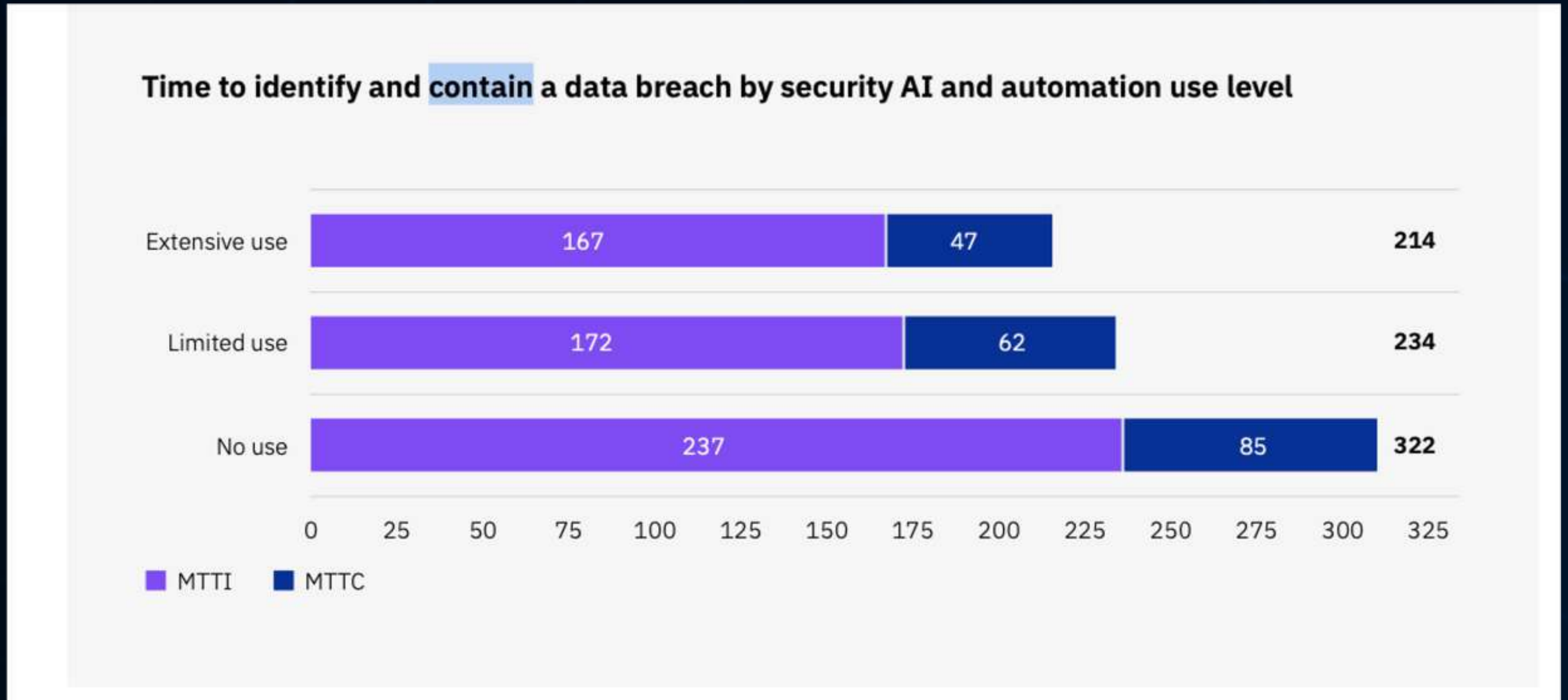
Data Security, Anywhere: protects essential entities’ critical workloads and ensures compliance in NIS2-regulated industries across hybrid and multi cloud environments at any scale, including through digital transformation.

Future-proofed Fabric: maximizes ROI through business capabilities that meet a broad range of NIS2 needs, seamlessly integrating with features and products from our Technology Alliance Program.

Data Security, Unleashed: elevates the security and compliance capabilities of IT and security staff by providing automation and filtering that accelerate entities’ paths to compliance.

Why Current Technologies May Not be Enough…

Extensive use of security AI and Automation can reduce the mean time to contain a breach to 30 days; It still takes up to 47 days to identify the breach. (*Ponemon*)



Time to identify and contain a data breach by security AI and automation use level

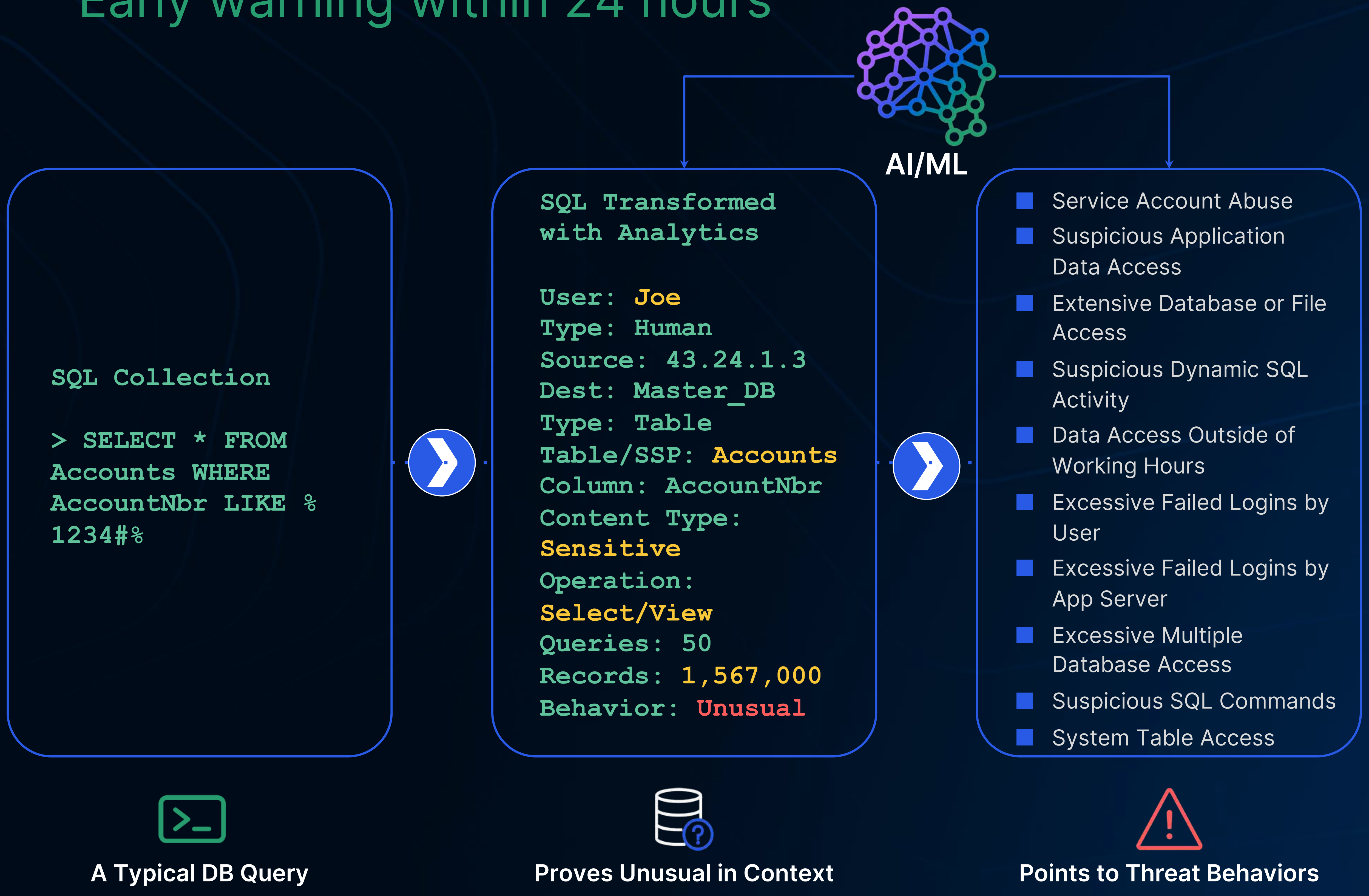
Figure 42. Measured in days

Are these okay for me to comply with?

- **Extensive Use of SIEM/SOAR**
  It can help monitor movement in infrastructure but cannot interpret and understand SQL and NoSQL languages. Imperva can preprocess this understanding for more than 30 languages.
- **Segregation of Duties using PAM and IAM**
  Access Management and a Zero Trust strategy are not effective in near real-time if someone authorized has taken malicious actions on data purposely or accidentally. Imperva can monitor data access and disclose any potential effective Data Breach with the query context.
- **DLP solutions**
  Blocking data sent to a personal domain won't show the data source, what was stolen, and where; it does not help compliance with NIS2 Art 23.

How Imperva Reduces Incident Reporting Time

Early warning within 24 hours



SQL Collection

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

A Typical DB Query

```
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
```

Proves Unusual in Context

- 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

Points to Threat Behaviors

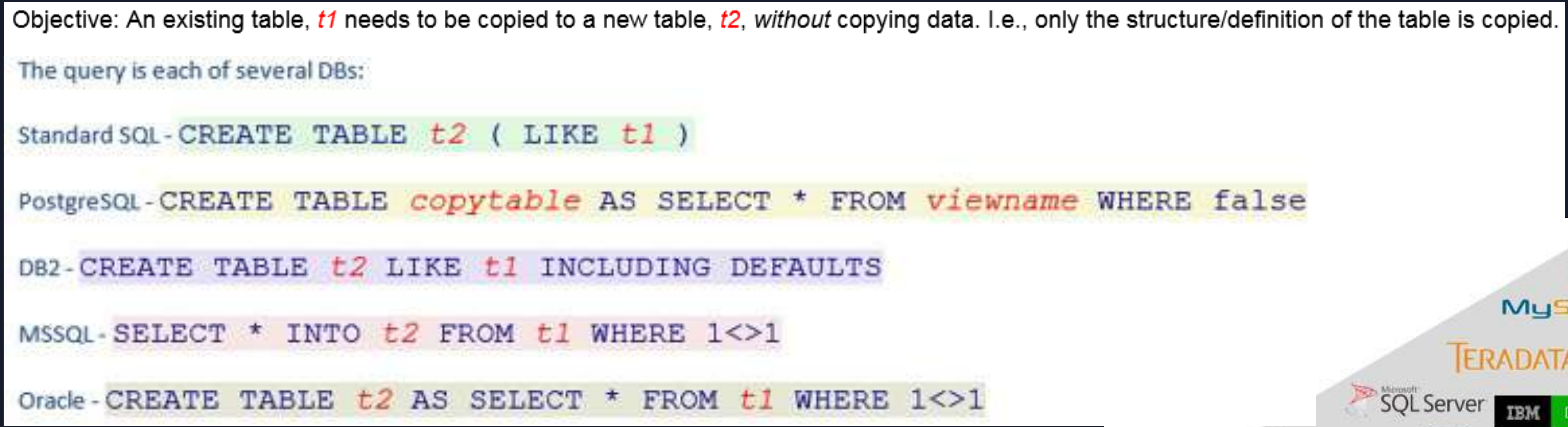
Imperva Data Risk Analytics (DBA)

- **Anticipates an impending attack by identifying event sequences that align with recognized attack patterns.**
- **Seamlessly translates database languages into plain English for effortless usage.**
- **Translates Structured Query Language (SQL) to actionable security events for the Security Operations Center.**

What is a "deep" understanding of data?

Take SQL for example.

Each DB provider speaks a different SQL language
Imperva "speaks" 30 different SQL languages
5 examples of the same operation:



Objective: An existing table, *t1* needs to be copied to a new table, *t2*, *without* copying data. I.e., only the structure/definition of the table is copied.

The query is each of several DBs:

Standard SQL - `CREATE TABLE t2 ( LIKE t1 )`

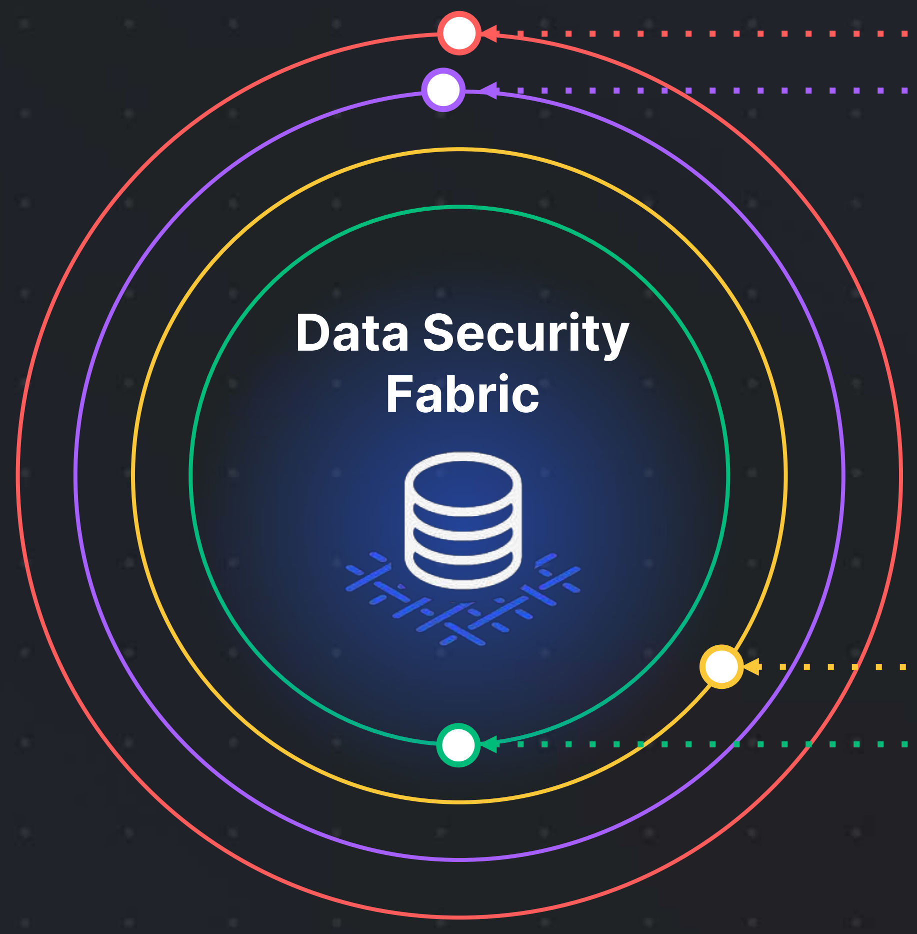
PostgreSQL - `CREATE TABLE copytable AS SELECT * FROM viewname WHERE false`

DB2 - `CREATE TABLE t2 LIKE t1 INCLUDING DEFAULTS`

MSSQL - `SELECT * INTO t2 FROM t1 WHERE 1<>1`

Oracle - `CREATE TABLE t2 AS SELECT * FROM t1 WHERE 1<>1`

The Inside-Out Strategy for Data Security



2. Audit & Report

- Centralized governance
- Compliance reporting
- Sign-off management
- Automated escalations
- Secure audit repository
- Data mining for forensics
- Long-term retention (years)
- Self-service reporting

1. Discover & Classify

- Discover all databases, applications, and clients
- Classify sensitive and PII data, structured and unstructured
- Group data for policy enforcement
- Continuously scan and update catalogs

4. Monitor & Enforce

- 100% visibility for cloud and on-prem
- Policy-based actions
- Anomaly detection
- Real-time prevention
- Granular access controls
- Call playbooks and workflows

3. Assess & Harden

- Assess vulnerabilities
- Mitigate configuration risks
- Behavioral assessment
- Risk dashboards
- Correlate user activity with data usage
- Change control reconciliation

Did they take anything?
Did they change anything?
Did they break anything?
How much data did they access?

Did they access any sensitive data?
Should they access this data?
What about their peers?
Is this more data than they normally access?

Answering the right questions and more

Recommendations

1 Identify, assess and address your risks.

2 Evaluate your security posture.

3 Take steps to safeguard privileged access.

4 Strengthen your ransomware defense

5 Move to a Zero Trust network.

6 Use cryptography and encryption.

7 Formalise your incident response plan.

8 Create a proactive security culture.

Asking Better Questions

Questions for the Security and Risk Teams

Questions data collecting organizations should be asking themselves

- **Where** specifically, is your **private** data located?
  - Could it be someplace else?
- **Who** is accessing your data?
  - Apps, APIs, and people?
- **What** data did they access and how much?
  - What happens if you can't answer this?
- **Should** they have access to your data?
  - Is this normal for them?
- **Where** does your organization have the **fewest controls?**
  - Data space, end point, or network?
- Which users have **access** to your data, **but do not use it**?
  - How do you know about dormant users?
  - What tracks the last access or use of a data privilege?
- Who is **responsible** if data is **lost**?
  - Whose phone rings first post-breach?
  - Do they have the answers and tools for incident response?
- Who is **responsible** for **monitoring** that data?
  - How do find a data issue without monitoring for it?

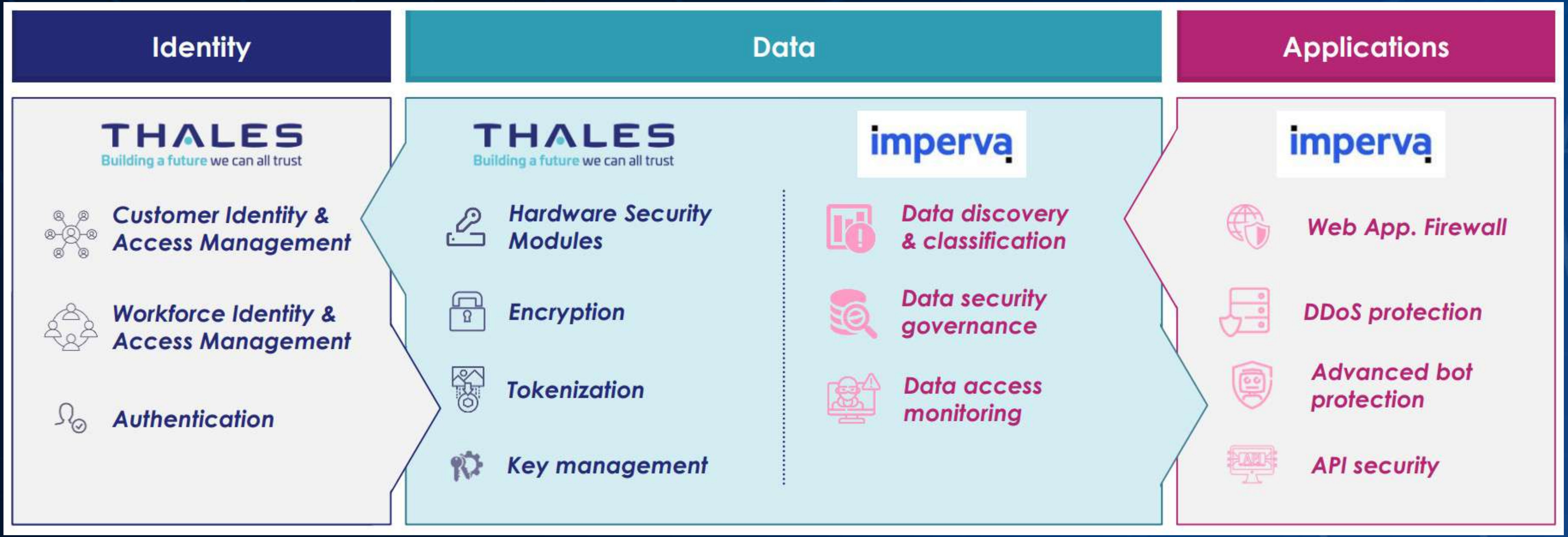
Cyber audit requirements growing in detail

Better question depth during a cyber security regulatory audits

- Record all user logins and failures
- Material changes are made to the data
- Report all new users added
- Discover all data stores and classify all data
- Encryption of data at rest and transit
- De-identification of non-production data
- How many incidents per day created for review?
- Which tools generate the most incidents?

- Monitor and secure all access to PII
- Detect unusual interesting behavior
- Access role for each user and last time used
- Hygiene of orphan and unused data users (disable unused accounts >365)
- Demonstrate long-term log retention - 1-7 years

Thales + Imperva – Strong synergies



Identity

THALES
Building a future we can all trust

- Customer Identity & Access Management
- Workforce Identity & Access Management
- Authentication

Data

THALES
Building a future we can all trust

- Hardware Security Modules
- Encryption
- Tokenization
- Key management

imperva

- Data discovery & classification
- Data security governance
- Data access monitoring

Applications

imperva

- Web App. Firewall
- DDoS protection
- Advanced bot protection
- API security

Next Steps

Imperva and Thales provide thought leadership, best practices, and technical assistance throughout the NIS2 lifecycle, from initial design and planning through incident response.

SCHEDULE A COMPLIMENTARY RISK ASSESSMENT

Imperva expert team will help you evaluate your application and data protection systems and practices to assess your threat and risk profile as you prepare for NIS2.

RUN OUR FREE SNAPSHOT TOOL

A Cloud Data Security Posture Management Assessment that is quick and easy-to-use for Amazon RDS DBs.

CONTACT US

Or your local Partner for more information on how we can assist you to get ready for NIS2.

Thank you

Mohamed Lallouch
Data Security Specialist
Mohamed@lallouch@Imperva.com