Why Data Security is important and role of DLP in it?

Krishna Murari Vijay

- Expertise in the design and deployment of IAM and cybersecurity solutions.
- Talks about Identity solutions.
- Talks about data security.
- Enthusiastic and eager to engage in conversations with peeople.

DATA

Do you understand the data?
Do you know what is the data in your organization?
Do you know why it is important to secure your data?

See what's happening around the world?

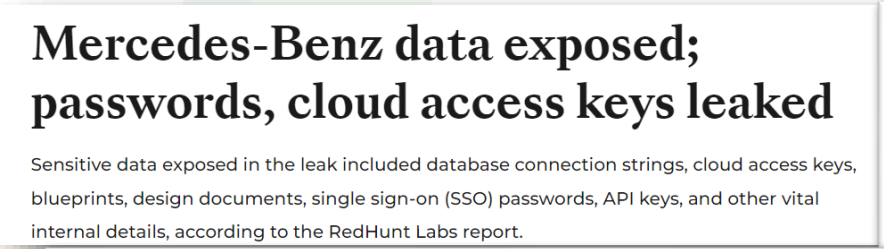
Year: 2022
Incident: A software engineer's corporate laptop was compromised, allowing the unauthorized threat actor to gain access to a cloud-based development environment and steal source code, technical information, and certain LastPass internal system secrets.

Data Accessed:

- On-demand, cloud-based **development and source code repositories** – this included 14 of 200 software repositories.
- **Internal scripts** from the repositories – these contained LastPass secrets and certificates.
- **Internal documentation** – technical information that described how the development environment operated.

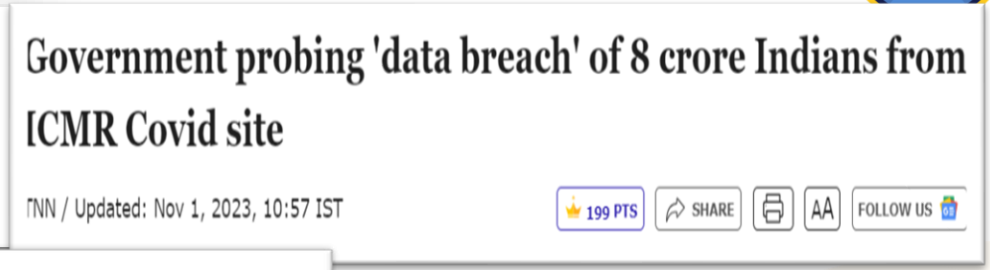
Source: https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/

See what's happening around the world?



Mercedes-Benz data exposed; passwords, cloud access keys leaked

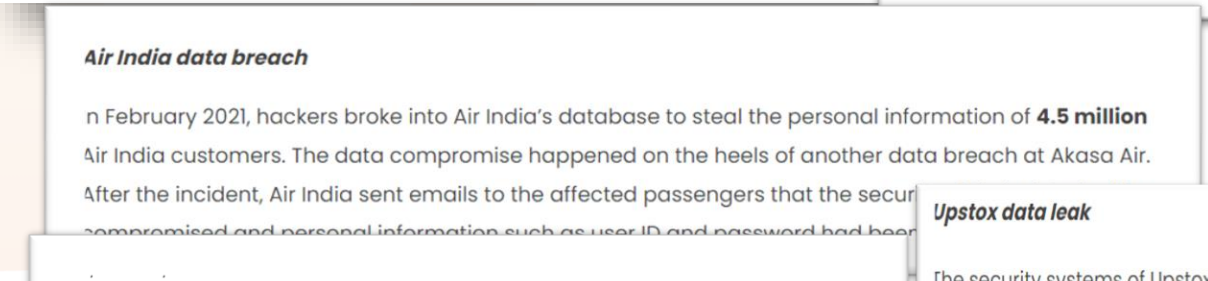
Sensitive data exposed in the leak included database connection strings, cloud access keys, blueprints, design documents, single sign-on (SSO) passwords, API keys, and other vital internal details, according to the RedHunt Labs report.



Government probing 'data breach' of 8 crore Indians from ICMR Covid site

TNN / Updated: Nov 1, 2023, 10:57 IST

199 PTS SHARE AA FOLLOW US



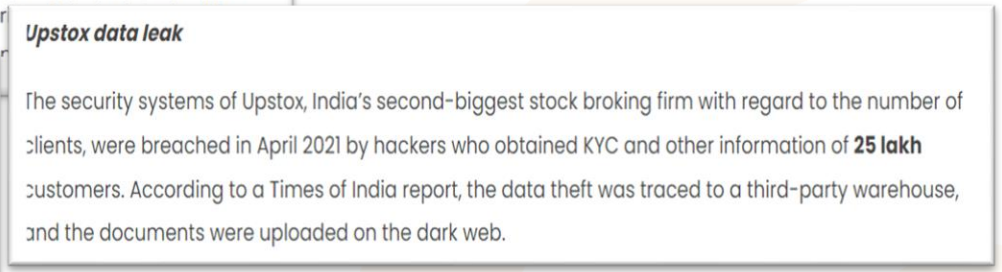
Air India data breach

n February 2021, hackers broke into Air India's database to steal the personal information of **4.5 million** Air India customers. The data compromise happened on the heels of another data breach at Akasa Air. After the incident, Air India sent emails to the affected passengers that the secur

Okta says hackers stole data for all customer support users in cyber breach

Reuters

Aa



Upstox data leak

The security systems of Upstox, India's second-biggest stock broking firm with regard to the number of clients, were breached in April 2021 by hackers who obtained KYC and other information of **25 lakh** customers. According to a Times of India report, the data theft was traced to a third-party warehouse, and the documents were uploaded on the dark web.

Source: https://ciso.economictimes.indiatimes.com/news/data-breaches/mercedes-benz-data-exposed-passwords-cloud-access-keys-leaked/107418268
https://etinsights.et-edge.com/top-7-data-breach-incidents-in-india/

What is Data?

Data refers to raw facts, figures, and statistics that are collected, stored, and processed by computers. Data can take different forms, including text, numbers, images, audio, and video. There are two main types of data:

Structured Data

- Organized and formatted in a specific way.
- Typically stored in databases using tables like SQL database, spreadsheets and CSV files.

Unstructured Data

- No Predefined data model
- Examples: text documents, images, audio, video files.
- More challenging to analyze compared to structured data.

miniOrange

Data Classification

Classification is the process of arranging the data in groups or classes according to their resemblance.

Data classification is the process of categorizing the data that is scattered throughout your network, endpoints or servers, shareable drive, or it many be in the database. So, data in an organization is basically dispersed everywhere.

A DLP strategy without a robust classification framework or mechanism in place is bound to fail.

miniOrange

Need of Data Classification

- Data Protection
- Risk Management
- Data Lifecycle Management
- Compliance and Regulatory Requirement

GDPR | HIPPA | PCI DSS | ISO 27001

miniOrange

Types of Data Classification

Content-Based
Data Classification

Context-Based
Data Classification

miniOrange

Data Classification is a continuous process…

Data Discovery

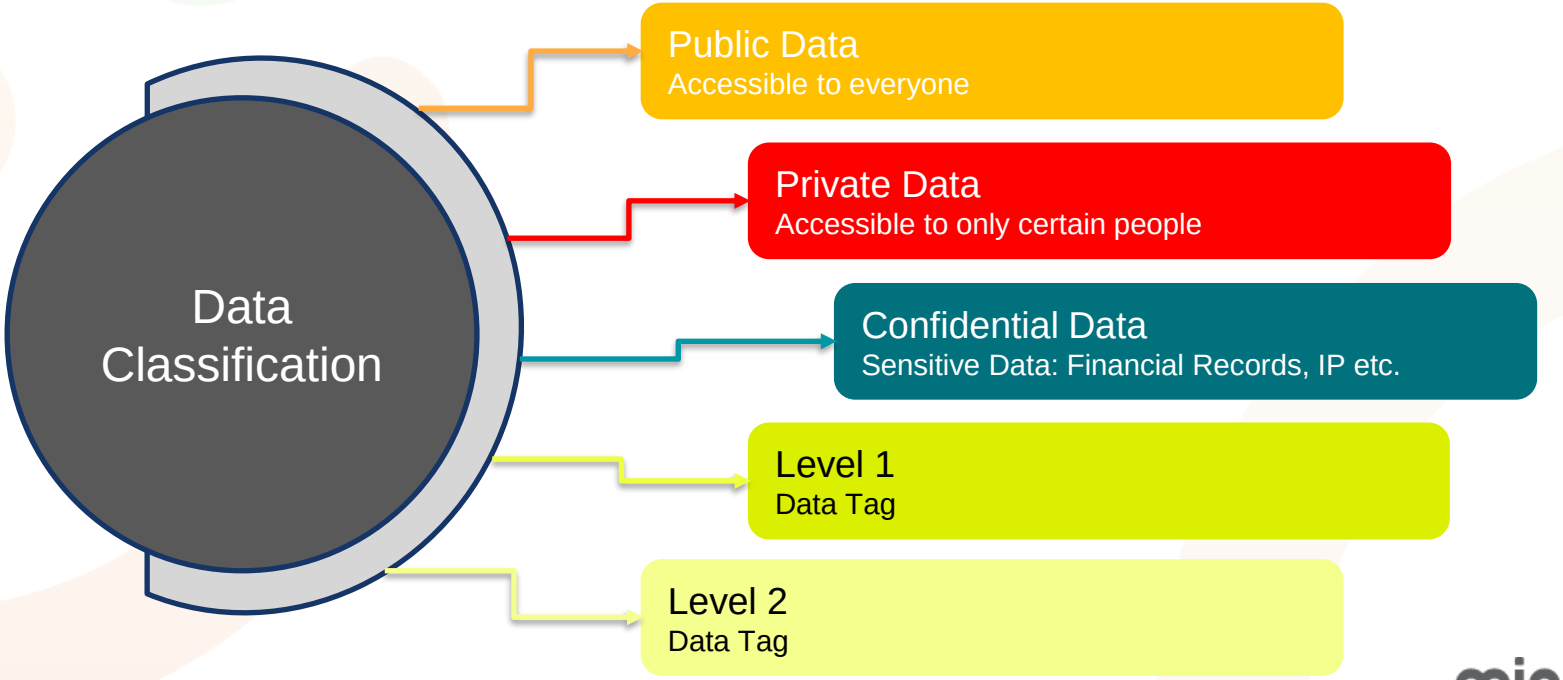
It is the process of identifying and locating the data assets within an organization’s infrastructure.

- Identity data for classification
- Data Storage
- Data Access
- Data Transportation

miniOrange

Data Tagging

It is the process of adding descriptive labels or tags to the data assets that has been identified during the data discovery.



Implementing DLP

Data Classification

Data Discovery

Data Tagging

Data Loss Prevention

miniOrange

DLP Objective

WHY	Define the reasons for implementing the DLP	Threats, Regulations etc.
WHAT	Define the type and form of data in scope for DLP	PII, PHIs, Contracts, Docs etc.
WHERE	Define the type of locations in scope for DLP	File Servers, Cloud, Application, DB etc.
WHEN	Define the time DLP will be needed	Immediately as data is created, duration etc.

miniOrange

DLP Scope

Define the exact location of data in scope for DLP	File Server Names/IP, App Name, Cloud Providers etc.
Define the infrastructure diagram in scope for DLP	System and Network Diagrams
Define the data flow in scope for DLP	Business & Operation Logic, Data Flow diagrams etc.

miniOrange

Three States of Data

AT REST	IN USE	IN TRANSIT
Where data is stored	When data is created & consumed	When data is transmitted
Local Disk	Document Read	Data Sent in Email
File Server	Document Modify	Data saved to cloud
Cloud Storage	Document Deletion	Data Sent to Server
Removable Media	Database Query	Data Sent to Removable Media

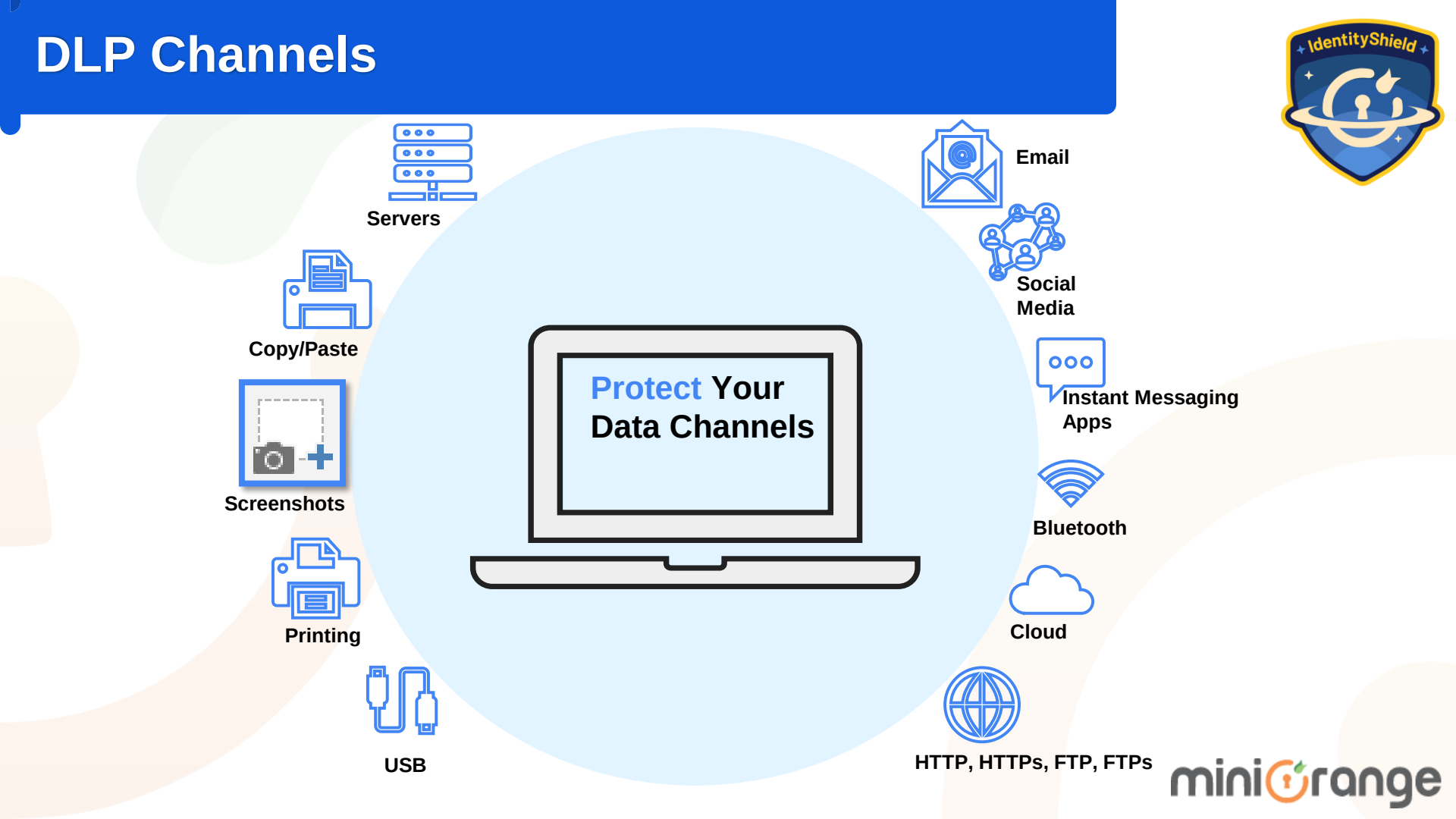
miniOrange

DLP Models

- The **data in use** at endpoints can be leaked via
  - USB
  - Email
  - Web mails
  - HTTP/HTTPs
  - IM
  - FTP
  - Other channels
- The **data in transit** can be leaked via
  - SMTP
  - FTP
  - HTTP/HTTPs
  - Other Channels
- The **data at rest** could
  - Reside at wrong place
  - Be accessed by wrong person
  - Be owned by wrong person

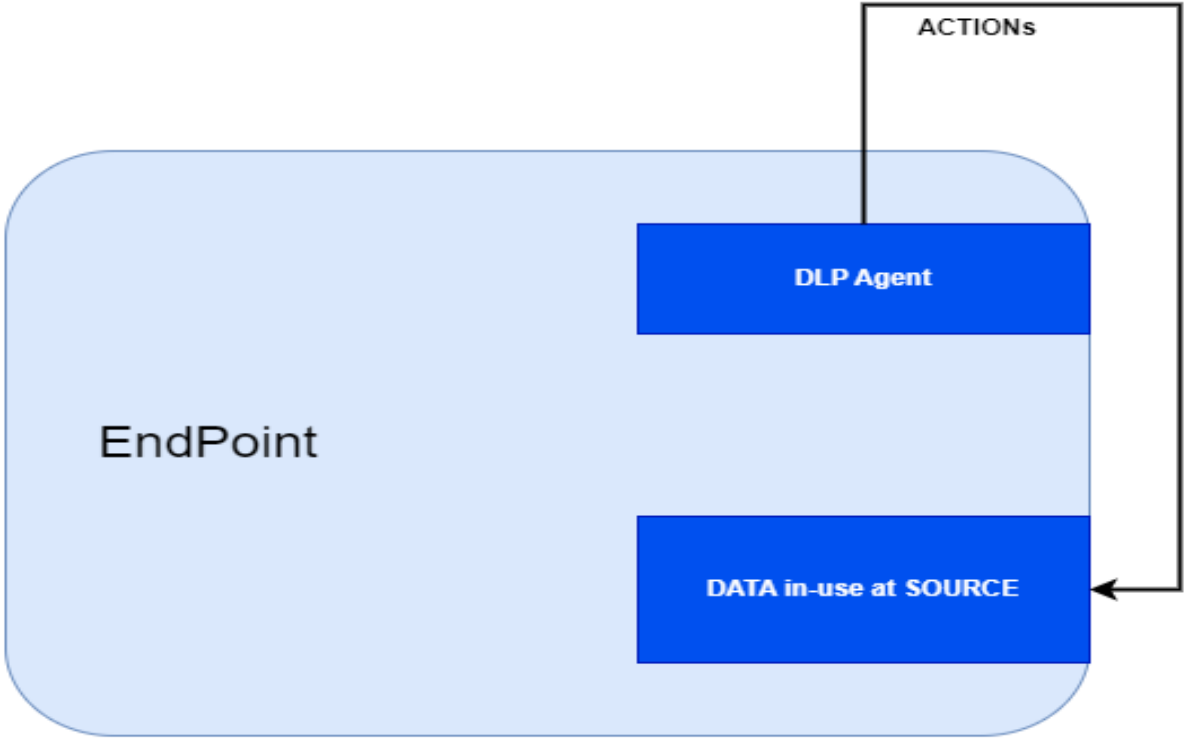
miniOrange

DLP Channels



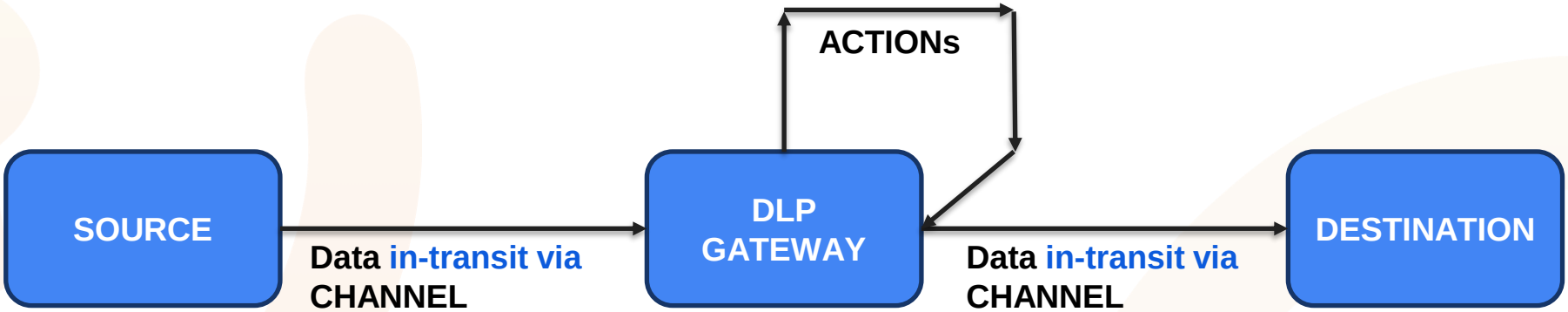
Data-In-Use: Technical View

- Preventing unauthorized use of data



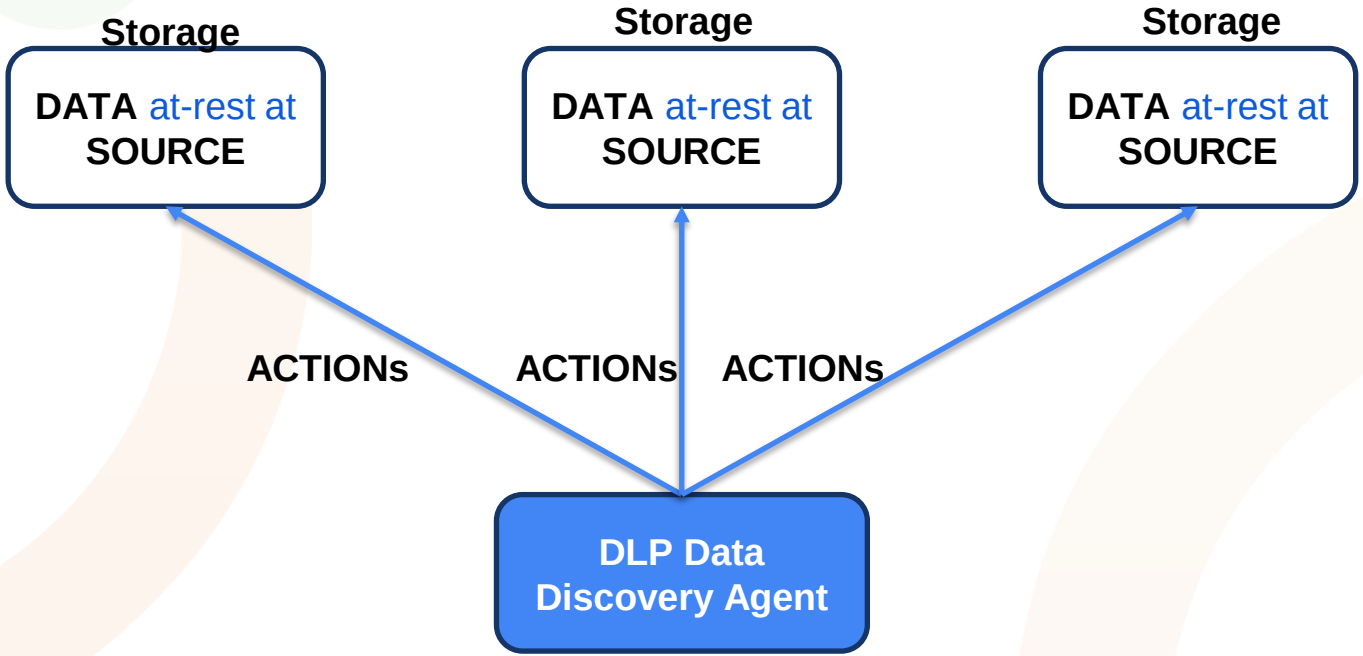
Data-In-Transit: Technical View

- Monitoring and Controlling the transfer of data



Data-At-Rest: Technical View

- Preventing unauthorized access to stored data



DLP Rules

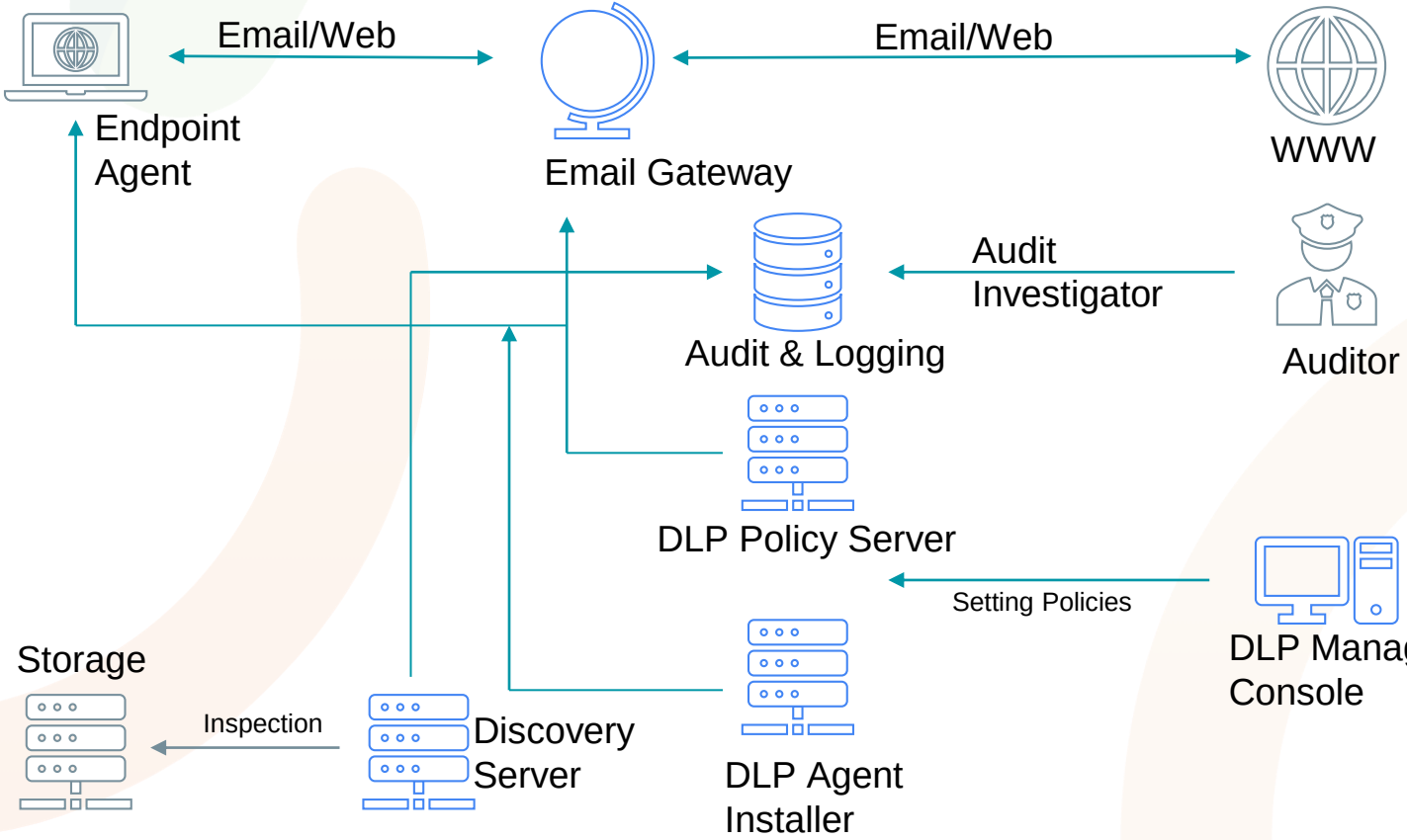
Content-based Rules	Contextual Rules	Action-based Rules	Threshold-based Rules	User-based Rules
• Predefined Patterns • Keywords • Regular Expression • Data Fingerprints	• User Roles • Locations • Devices • Sensitivity of the data	• Blocking • Encrypting • Quarantining • Alerting • Logging	• Setting the limit for acceptable behavior • Usage patterns	• User identities • Roles • Privileges • Group membership

miniOrange

DLP Components

- DLP Management Console
- DLP Endpoint Installer
- DLP Policy Server
- DLP Email Gateway
- Data Discovery Agent

DLP Basic Architecture



DLP Best Practices

- Identify and Classify your data according to your business needs.
- Use Encryption to protect your confidential data.
- Enable Access Controls
- Monitor Data Access
- Conduct Regular Security Audits
- Educate and Train your Employees
- Implement Incident Response Procedure

miniOrange

Thank You

Scan this QR Code and share your valuable feedback.

Krishna Murari Vijay
krishna@xecurify.com