Product Brief

Imperva Data Security Fabric

Unstructured Data Discover and Classify

thalestct.com

THALES
Building a future we can all trust

THALES

Unstructured data is everywhere

In many organizations, unstructured data in the form of email, files from office productivity suites, PDF documents and various other application files is the majority of their data. Organizations have very little insight into what most of those files contain or what risk exposure they hold. Many threats from insider mishaps, malicious actors, cyber-attacks, ransomware and other sources are always lurking in enterprise environments with files spread across on-premises and cloud data repositories.

Gaining visibility and creating a framework to profile the data is a business imperative for data governance, compliance, security and privacy. For a large organization, the data volume can be overwhelming, and automated tools are needed to help sort it out. Imperva Data Security Fabric (DSF) Unstructured Data Discover and Classify provides the capabilities to automate data search, discovery, and classification of unstructured data at an enterprise scale, so you can find exposed sensitive data and protect it before it is discovered by auditors or hackers.

One data view, enterprise-wide

One challenge of unstructured data auditing and risk management often lies in the complex mix of unstructured data repositories that reside within an organization. Imperva DSF Unstructured Data Discover and Classify can help uncover, identify and classify sensitive information from a wide range of unstructured data sources.

Imperva DSF Unstructured Data Discover and Classify provides visibility into the exact location, volume and context of sensitive data. Driven by machine learning, it allows data owners to find and identify data regardless of cloud or on-premise environment or data source.

Automated, cross-directory searches allow data professionals to do an extensive scan across multiple data repositories simultaneously in seconds, finding the information that is needed for an auditor question, an individual's data lookup, or a data deletion request with maximum accuracy at scan speeds up to 100,000 words per second.

Key Use Cases

Data mapping and risk assessment

Data compliance, security and protection

Dark data discovery and remediation

Data minimization and governance

Access control assessment and risk mitigation

The Imperva DSF Unstructured Data Discover and Classify engine analyzes metadata to determine file owner, data type, data category and other information and presents findings to the Imperva Data Security Fabric Hub for risk and security analysis. DSF can consolidate unstructured as well as structured sensitive data into one enterprise data view, enabling rapid assessments of current access profiles. Administrators will quickly know whether any regulated data types may have over-privileged file entitlements, beyond what is intended or entitled for a user.

Imperva DSF has a built-in workflow manager to help automate remediation workflows should action be required. In addition, it can integrate with other enterprise tools an organization might already be using such as ServiceNow, improving collaboration across governance, compliance, and security teams.

Data compliance and privacy

Depending on your organization's regulatory obligations, one or all of the above capabilities are essential to maintaining data compliance. Many data compliance with privacy regulations revolve around maintaining an accurate inventory of your client, employee, and supplier Personal Data. GDPR specifically requires that retained Personal Data is classified, and provisions in the regulation specify that you must implement "state of the art" security measures to protect it.

Data protection is essential to all compliance regulations that empower regulators to impose non-compliance fines and penalties in the event of data exposure or breach. Imperva DSF Unstructured Data Discover and Classify will help you mitigate non-compliance risk and the potential for data breaches from an unstructured data source. Classifying data by sensitivity categories such as Restricted, Confidential, Internal-only, or regulatory categories such as PII, Personal, HIPAA, and others makes it easier for staff to apply the appropriate compliance and security controls.

Data management and minimization

Efficient data governance team collaboration on retention and deletion is almost impossible without a centralized tool to help manage the process. Imperva DSF Unstructured Data Discover and Classify enables organizations to implement continuous governance processes through regularly scheduled data scans and inventory reporting, simplifying tracking and change management.

The unstructured data reporting features provide governance professionals with information that helps them collaborate on data management projects so they can determine which data files are no longer relevant to the business or identify which files contain a hidden business value. Imperva DSF can leverage the data intelligence from a trusted data catalogue such as Collibra where in use. Obsolete files can be earmarked for deletion which helps the organization reduce IT infrastructure and maintenance costs.

Unstructured data security simplified

Data discovery and classification is a foundational compliance and security process. Imperva DSF automates the process so your governance, compliance and security staff can manage the process for unstructured data enterprise wide. Imperva DSF Unstructured Data Discover and Classify helps oranizations simplify compliance, save time, save money and protect your organization from the risks of data breaches through sensitive data in unstructured data files.

Imperva DSF Unstructured Data Discover and Classify is available as an add-on capability to provide coverage for unstructured data protection into a holistic Imperva Data Security Fabric solution for all enterprise data assets across on-premises, cloud, hybrid and multi-cloud enterprise environments. Additionally, Imperva DSF also provides Data Discover and Classify for structured and semi-structured data types.

Imperva DSF Unstructured Data Discover and Classify is available to the U.S. Federal Government through Thales Trusted Cyber Technologies.

Key Features

Agentless and modular architecture

Exhaustive metadata inspection and analysis

ElasticSearch index for quick reporting (in seconds)

Identifies thousands of unstructured data or file types

Supports dozens of commonly used file repositories including:

- Microsoft Sharepoint
- Microsoft file servers
- CIFS network fileshares
- Office 365 Onedrive
- AWS S3 buckets
- Azure Blobs
- Google Workspace drives
- Unix Mail archives

Benefits

Simplify data compliance and accelerate audits

Discover dark data to unlock value or shine a light on unknown organizational risk exposure

Enforce data entitlements and policy compliance to mitigate data breach risk

Pursue data minimization strategies to lower cost and simplify business processes

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

Contact us - For office location and contact information, please visit thalestct.com/contact-us