FASOO

WWW.FASOO.COM

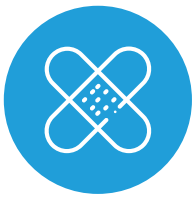
SENSITIVE
UNSTRUCTURED
DATA

Data Visibility for Privacy and Security

Organizations need better visibility into the use and movement of their sensitive data to meet privacy regulations and safeguard content.

The best approach is a self-reporting file method, one that automatically traces, gathers and records all document interactions without reliance on disparate network, application, and device logs.

The same technology that enables self-reporting files is the foundation of a powerful data security approach – a file-centric method. Bridge both privacy and security gaps with a file-centric method that delivers deep data visibility and a strong front-line defense for your sensitive data.



Traditional security and network tools create a patchwork approach to data visibility that is inadequate, impractical, and unsustainable.

You need visibility to know where your data is, who is using it, and how it changes throughout its lifecycle. Discovery and classification tools are a good start to find data and tag it for downstream controls. However, to maintain control, you need deep visibility to track data as it travels, is accessed and transforms into other file types throughout its lifecycle. Cybersecurity and privacy teams are challenged to keep track of sensitive files. A file will

be accessed by multiple systems, applications and devices as users share it internally and with external parties. With over 40 different security and IT operations tools used in a typical business, organizations struggle as they work to accumulate, correlate, and report file interactions.

This challenge grows as data visibility is often obscured when documents travel within the organization or shared externally to the organization and change either through duplication or revisions. Without proper data visibility, you can miss the moment sensitive information is shared, moved to a different location, changed, or deleted.

You must also have visibility into sensitive file interactions for data breach investigations and to comply with privacy regulations. Details must be readily available to support incident response teams; and privacy regulations like GDPR and CCPA compel businesses to report on all data they hold regarding an individual within a specified period or be subject to fine.

KEY INSIGHT:

Faced with millions of files and countless interactions across global networks with thousands of end points, organizations need a new way to track data use and movement.

Visibility gaps widen as three trends stress legacy infrastructure

IT, security and privacy professionals are working to address widening visibility gaps and overcome the risk posed by:

- Exponential growth of unstructured data that includes strategic, operational and intellectual property
- COVID-driven remote workforces suddenly operating outside the corporate perimeter
- Privacy regulations increasingly focused on an individual's rights to control their data used by businesses

Data proliferation is staggering, and unstructured data is rapidly growing, estimated to be 80% of a business's data inventory. Unstructured data is routinely undermanaged and is hard to control and track as users take sensitive files from controlled repositories, store them on laptops, endpoints, and cloud services and share them in collaboration applications both internally and with external parties.

COVID-19 rapidly expanded the remote workforce and dissolved corporate perimeters. Sensitive

data now resides on more unmanaged and shared devices. It travels on insecure networks and is used in unauthorized or non-compliant apps. All this is obscured from corporate oversight.

Privacy regulations have vaulted individual rights to the forefront. Right to be informed; right to be forgotten; and data residency all impose new demands on data visibility, tracing, control and reporting.

KEY INSIGHT:

Regulatory agencies and corporate Governance, Risk and Compliance (GRC) teams increasingly focus on the visibility gap of sensitive unstructured data and the actions of security, compliance and IT professionals to close these gaps.

Self-reporting files use an embedded ID technology to trace and record all interactions

Legacy security and privacy data architecture lack the deep data visibility and persistent tracking needed to meet today's requirements.

Data loss prevention (DLP) and identity and access management (IAM) solutions designed for perimeter security lose track of data migrated to the cloud and when downloaded by remote workers. Privacy and legal e-discovery applications may have file mapping features, but they are siloed, don't track all interactions, and the multiple datasets are disconnected and incomplete.

A unique ID that's embedded and travels with the file enables persistent tracing and self-reporting of interactions throughout the file's lifecycle. By using this method, it:

- Eliminates working with patch-work logs from multiple systems
- Provides a single source of truth for audit and regulatory purposes
- Enables efficient and timely incident and privacy response

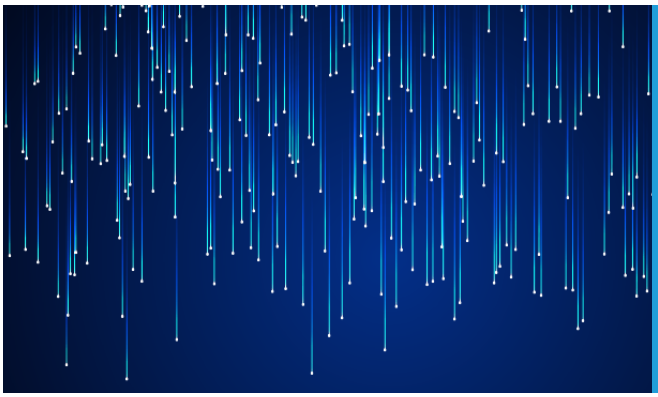
An organization's existing data-centric tools perform better with an embedded ID approach. Discovery scans lack the intelligence to relate file derivatives that are copied or duplicated.

With an embedded ID, derivatives of an original file, whether duplicated or renamed, inherit the parent ID tag and all its security and governance policies.

An embedded ID reduces tool sprawl by negating the need for tracking tools fielded with each security, privacy and legal e-discovery application. All applications benefit from a single source of truth for file tracing and interactions.

KEY INSIGHT:

Using an embedded ID for deeper visibility, tracking and reporting at the file level is the best way to achieve sustainable and auditable processes and better safeguard sensitive data.



Deep Visibility with Embedded File ID

File Derivatives

Data changes throughout its lifecycle: As the original file copied and renamed or saved in a different format.

Discovery scans find sensitive unstructured data but lack: The means in subsequent scans to relate derivatives to a previously scanned file.

Missing derivative traceability compromises: Privacy compliance and increases the organization's threat surface as redundant sensitive data is unnecessarily retained across multiple locations.

With an embedded ID: Derivative files inherit the same file ID as the original, making visibility, security classifications and handling controls consistent across your IT infrastructure.

Individual Data Rights

Tracing of individual information: Requires persistent visibility and reporting in order to comply with modern day privacy regulations.

Responding to Data Subject Access Request ("DSAR") requires: Organizations to find all customer information and report in a specific period of time (e.g., 30 days).

Any file associated with an individual: Must be accounted for throughout its lifecycle.

An embedded ID: Eliminates the time-consuming task of file forensics. It provides a single source of truth that offers current deep data visibility, letting organizations meet today's demanding individual information rights regulations.

Control at 3rd Parties

Businesses lose data visibility: When they share files outside the corporate network with supply-chain vendors, external legal and financial professionals.

Regulators make you responsible to ensure data is appropriately safeguarded: Breaches of your data while in custody of a third-party requires you to report the breach.

Secure and compliant sharing means: You extend the same visibility and controls that exist within your managed networks to any third parties.

An embedded ID provides the same activity tracking as if the files were internal: Enabling additional controls to set a file expiration date and revoke access at any time to third party locations. This feature is a key compliance component to the individual regulatory "rights to be informed and forgotten".

User Behavior Monitoring

Who is accessing your data, how it is being used, and where it is being moved: Are critical inputs for monitoring solutions focusing on detecting data misuse and policy violations.

Data transfers to removable drives and large uploads to cloud services outside of your organization: May be an early warning sign of malicious insider threat intent.

User behavior (UB) analytics are most effective when: Data visibility tools provide a full perspective of user activities across all applications and storage locations.

An embedded ID: Provides the highest granularity of data activity to drive UB analytics leading to earlier detection of insider threats. These data insights cue security methods, such as restricting the copy of data to removable drives.

PRIVACY AND SECURITY TOGETHER

Deep visibility and a protect-first approach to data security. It's been observed that "you can have security without privacy, but you can't have privacy without security." Both are tightly related, and today, it's not an either or choice.

A file-centric method with embedded ID is the best choice for data visibility. The same method enables a protect-first security approach that protects the data itself with encryption and access controls and eliminates redundant and overlapping tools implemented at multiple network and end-points.

Bridge both worlds and close privacy and security gaps with a file-centric method that delivers deep data visibility and a strong front-line defense for your sensitive data.

About Fasoo

Fasoo products span the life-cycle of sensitive unstructured data to discover, classify, protect, monitor, control, track and expire access to content wherever it travels or resides. Our unified solution enables users to securely collaborate internally and externally with sensitive information while consistently meeting corporate governance and regulatory requirements. Our file centric approach using encryption with a unique identifier allows organizations to have more visibility and control over unstructured data without interrupting workflows. We've engaged in this journey with over 1,500 enterprises to field data-centric solutions that proactively protect corporate brand, competitive position and meet increasing regulatory demands.

Sales & Partnership: inquiry@fasoo.com