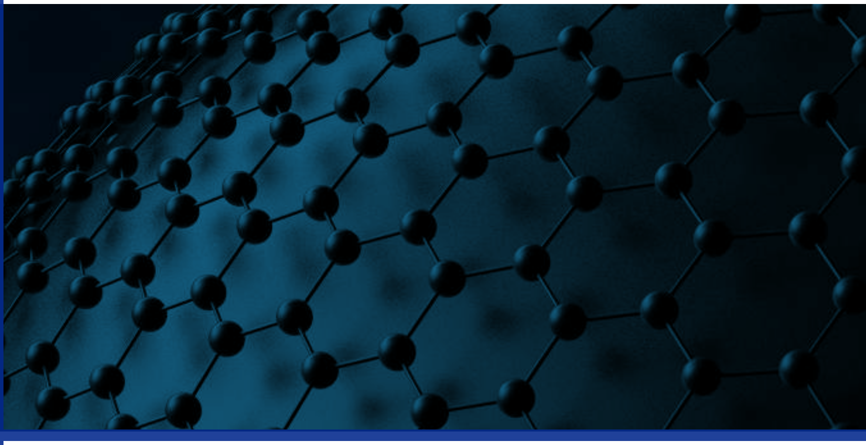
FASOO

WWW.FASOO.COM

SENSITIVE
UNSTRUCTURED
DATA

Protect-First Approach To Data-Centric Security



Three predominant data-centric security methods

There are three predominant methods in the market today to prevent loss and unauthorized access to sensitive unstructured data. Each is different and the best way to compare and contrast the methods is to understand what a vendor's solution looks to defend and the primary data-centric tools used.

METHOD	Data Flow-Centric	Location-Centric	File-Centric
DEFENDS	Data at Ingress/ Egress Points	Folders, File Shares, Disk, Cloud	Files
TOOLS	Data Loss Prevention	Identity & Access Management Behavior Analytics	Persistent Encryption Identity & Access Management

Today, with increasing threats and the consequential impacts of a data breach, more organizations are adopting a file-centric method as the foundation of their data-centric architectures. It's the only method that truly denies unauthorized access to your sensitive data no matter how it flows or the location it resides. This protect-first foundation recognizes that if data isn't properly protected – your entire house crumbles.

A file-centric method works as a frontline defense and can be deployed in combination with other methods to achieve a fortified, cohesive data-centric security architecture. Understanding the key distinctions between the methods helps you navigate vendor engagements and build a protect-first architecture that best fits your needs.

Data Flow-Centric

These solutions defend sensitive data at corporate infrastructure ingress and egress points and use data loss prevention (DLP) tools to stop data leakage. Ingress and egress points include servers, networks, end-points, and cloud services.

The majority of businesses have deployed DLP as point solutions – known as Integrated DLP (e.g., network DLP, email-server DLP, or end-point DLP) while few have scaled to a full enterprise DLP deployment (e.g., a full solution suite across all points).

Data flow-centric characteristics:

DEFENDS:
Prevents data from leaking by intervening with the use or movement of data.

TOOLS:
Content matching that actively looks for regular expressions, defined strings, keywords, patterns or data dictionaries.

Additional tools that can be used include fingerprinting (indexing) and image recognition.

DLP solutions set up rules that specify conditions, actions and exceptions. The tools filter messages and files based on their content and prompt corrective measures. They can simply alert a user that an action may be risky or completely block the action. Examples include alerting when sharing sensitive data through email and restricting the copying of sensitive files onto a USB drive.

Many organizations have implemented email DLP since this is the most obvious ingress/egress point prone to unauthorized exchanges of sensitive data. While there are measured improvements, security and IT administrators still have challenges when implementing and operating DLP solutions, such as:

- Rules are complex and create thousands of initial false alerts.
- Concerns over disrupting user workflows causes administrators to loosen controls and implement few blocking mechanisms.
- Alerts burden administrators and backlogs might take weeks or months to address.

Too often businesses have inappropriate expectations for DLP. It works - but many underestimate the complexities and resources needed to build, tune, and manage policies to fit your environment. You should anticipate iterative refinement of rules and alert resolution.

KEY INSIGHT:

Data flow-centric solutions are good at reducing risk but not a strong, protect-first approach. They don’t defend the data itself, but only how it flows in your organization. Any leakage exposes the data to unauthorized disclosure.

Location-Centric

These solutions defend sensitive data storage locations. They look for gaps and inconsistencies in identity and access management (IAM) and apply user behavior analytics (UBA) to reduce the risk of unauthorized disclosure of sensitive data. Locations include folders, file-shares, disks, and cloud services.

Location-centric characteristics:

DEFENDS:
Folder, file-share or disk from unauthorized access and suspicious usage.

TOOLS:
Analysis of IAM settings and policies to find discrepancies and obsolete controls.

UBA to monitor and detect anomalous events.

Unlike DLP solutions that query and assess content repetitively, location-centric solutions pre-process, classify, and tag sensitive data. These tags flag where sensitive content is located within your IT data architecture and use:

- IAM tools: Find excessive, outdated, or inconsistent user permissions and non-existing passwords, evaluate access controls and authorization processes plus search any Active Directory structures to discover discrepancies.
- UBA tools: Monitor privilege and end user access to detect anomalous behaviors (unusual mailbox activity, large number of failed attempts to access a folder, or excessive downloads of files to a portable storage device).

Location-centric solutions are easier to implement than rules-based data flow-centric solutions because the tools are non-intrusive and use system logs and UBA. Location-centric solutions place priority on data visibility and are superior to many approaches when it comes to privacy compliance, audit and reporting requirements.

However, drawbacks with location-centric solutions include:

- Access IAM and UBA tools are location-specific. Once a file is removed from the location and downloaded to laptops or endpoints, you lose visibility of the data.
- Folder management becomes a challenge at scale as a single terabyte can spread to over 50,000 folders. Keeping access lists current and monitoring user activity across millions of folders is burdensome.
- Like data flow-centric solutions, the alerts place significant demands on administrators' workloads and their ability to respond in a timely manner.

While obfuscation tools are not native to these solutions, some use data encryption while the data resides and is used within a particular location. However, when files are downloaded to endpoints, stored in personal cloud accounts, and shared outside the location - protection, visibility and control is lost.

KEY INSIGHT:

Location-centric solutions use a "least privilege" approach as the foundation for their data protection method – not a "protect-first" approach. Critical gaps arise when data is moved from its original location, and lacking persistent encryption, expose your sensitive unstructured data to a breach.

File-Centric

In contrast to the other methods, persistent encryption and IAM are tied to and travel with the file. This is independent of networks, severs, locations and devices.

File-centric characteristics:

DEFENDS:
Office documents, CAD/CAE files, PDF, plain text, other digital media file types.

TOOLS:
Encryption is persistent, centrally managed and enforced at the file level.

IAM is assigned and enforced at the file level.

The method uses data classification tags to:

- Encrypt the file contents: If exfiltrated, the sensitive data is obfuscated and is of no value to threat actors.
- Restrict file access to only authorized users: Users can be an individual, departments, business unit or defined by role or title.

File-centric solutions were historically used for very specific use cases but today are experiencing a market resurgence. Modern solutions take advantage of the latest in software tools like RESTful APIs and open operating system standards to work transparently across the enterprise. Centralized policies ensure access and protection are consistently applied across all networks, file-shares, devices, end-points and cloud services.

And when it comes to denying access to sensitive content, the file-centric method is by far the best “protect-first” approach. Here’s how leading analyst are advising clients:

- Gartner states that despite extensive DLP coverage there are “gaps in data flows where data can leak” and “the better answer is a strategy focused on securing the data itself.”
- Forrester reports encryption is entering a “Golden Age.” Due to the growing concerns of data theft, privacy and government surveillance, security pros are increasingly using all forms of encryption throughout their digital businesses.
- Gartner claims “Identity” is the new perimeter in a world of distributed Software as a Service (SaaS) and other cloud-based services. Centralized administration and control of access to data must be maintained by the business, not service providers.

Look for file-centric solutions that automate discovery, classification and encryption in a single instantaneous step without user intervention. This improves productivity and consistency in application of policies.

KEY INSIGHT:

File-centric solutions use a “protect-first” approach as the foundation of their data protection method. Persistent access control and encryption remains with the file throughout its life-cycle. Most privacy regulations exempt loss of encrypted files from breach reporting or alternatively, impose significantly reduced penalties.

PROTECT-FIRST, FILE-CENTRIC APPROACH

Organizations struggle to distinguish between data-centric solutions from different vendors as they search for the best way to safeguard their sensitive unstructured data. Data-centric security encompasses a wide range of processes and tools, many with overlapping functions and focused to different end goals. Adding to this confusion has been a flurry of gap-filling point solutions (e.g., CASB, end-point protection) launched to address today’s cloud and mobility adoption.

And despite significant investments in traditional data flow and location-centric methods, data breaches today are at all time highs.

Adopt a protect-first, file-centric method for your data security architecture. Establish this strong frontline defense to deny any unauthorized access to sensitive unstructured data, no matter how it is used, with whom it is shared, or where it is located. Then, use this foundation to integrate other data-centric methods and tools to architect a data security infrastructure that meets your organization’s governance, risk and compliance mandates.

Sales & Partnership: inquiry@fasoo.com

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.