FASOO

WWW.FASOO.COM

SENSITIVE
UNSTRUCTURED
DATA

Streamline and Operationalize Security and Privacy Initiatives

Leading organizations are discovering how a protect first, file-centric approach fortifies data security and enhances data visibility to comply with privacy regulations like GDPR and CCPA. Now, learn how this approach simplifies implementation and operations to fast track your security and privacy initiatives.

Today's Data Loss Prevention (DLP) and data security analytics solutions are challenging to deploy and manage. These solutions repetitively apply complicated rules and analytics at each location where data travels to identify misuse.

Common shortfalls include:

1. Rule-sets and analytics only monitor but don't protect the data itself
2. Responding to alerts, including false-positives, overwhelms security staff
3. Inappropriately applied rules block user workflows
4. Implementation is required at each email, network, endpoint and cloud location

A protect first approach takes a more direct path to safeguarding files that contain sensitive data. At its core is a file-centric technology. A file with sensitive data is discovered, classified and secured the moment it's created. This one time detect and secure method:

- Encrypts and binds identity and access to the file itself for strong protection
- Eliminates continuous monitoring and alert administration
- Uses transparent and seamless protection that doesn't disrupt workflows
- Protects file independent of server, storage or device

By working at the file level, this approach creates a sequence of efficiencies that simplify and streamline data discovery, classification, protection, audit and policy management. When deployed as an integrated platform, the approach delivers a high degree of automation with centralized controls.

Here's how organizations use the protect first approach to keep their security and privacy projects on a fast track.

Discover and Learn
Build informed policy decisions by keeping initial discovery general by looking for file extensions like docx, xlsx, jpg, and dwg to start gaining insights in advance of more complex security and privacy scans.

Prioritize Inventory
Focus on your active data first: that was accessed in the past year, what is it, where is it going, who is accessing it, and how is it being used. This is likely your most valuable and vulnerable inventory.

Classification
Focus on security needs first. Employ a single fundamental - if it's sensitive, secure it. Find and protect the most prevalent and common forms of sensitive content first for quick wins.

Protect, Not Alert
Secure the data itself. Eliminate repetitive content and analytic scans at every sever, cloud service, application, or device. No ensuing alerts to burden security administrators so they can concentrate on more pressing security matters.

Platform Solution
Secure the data itself. Eliminate repetitive content and analytic scans at every sever, cloud service, application, or device. No ensuing alerts to burden security administrators so they can concentrate on more pressing security matters.

Now let's take a more detailed look at how each these activities can keep your project moving.

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

Keep initial discovery simple to gain a first-pass understanding of your data inventory and where security gaps exist

Searching for common file extensions will provide valuable insights into the kind of sensitive information you have and where it is located. The discovery tool searches file shares, desktops, laptops, other endpoints and mapped drives. This snapshot will give you the location of all files, volume of file types you have, who the file owner is, which department it belongs to, and the last date it was accessed.

Use basic insights to formulate priorities

By focusing on the primary goal – to safeguard sensitive unstructured data - you might quickly find that files owned by Human Resources (HR), Research and Development (R&D) or Finance have spread outside their designated file storage locations. If these sensitive files are on employees' laptops, on removable drives or are shared with third parties, the data is at high risk of exposure and should be assessed as an early priority target.

KEY INSIGHT:

Too often projects lose momentum as governance, legal, compliance, IT and security work across multiple departments to gather requirements and develop policies. Overcome inertia and engage with your data inventory to help drive informed policies.

Divide and Conquer

Focus on data that your organization currently generates, accesses and shares. Set older, dated inventory on a separate remediation path. Finally, assess all data for its value, especially "dark" and redundant, obsolete or trivial (ROT) data.

As a general rule, data less than one year old often represents less than 25% of corporate data

Current and active data is typically what matters to your business today and likely the most valuable to threat actors. Target this subset of data first and use the experience to fine tune your

policies. Move this current data onto downstream classification and protection processes first to get sensitive data protected and under control as quickly as possible.

Set dated inventory on a separate path

Consider various remediation paths for older inventory to limit its risk exposure while prioritizing current data. Data discovered in unauthorized locations should immediately be moved to approved file-shares. For departments known to deal with a large amount of sensitive data (e.g., legal, audit, HR), use bulk folder-based or in place encryption methods to protect the data inventory in the interim.

They can't steal what you don't have

As much as 52% of data stored by organization is "dark" data, the value of which is undetermined and 33% is redundant, obsolete or trivial (ROT). Data discovery will surface all files for review and the deep visibility enabled by a file-based method will identify duplicates and file derivatives (i.e., files that are renamed or format has changed). Eliminate ROT immediately and engage data owners to assess dark data.

KEY INSIGHT:

Simply discovering the basic facts about your unstructured data will help you decide on the best path to address and prioritize your data security and privacy requirements.

Classification

Don't get side-tracked by diverse data stakeholder interests

There's a wide range of information governance purposes that impact your data, and security and privacy are just one part. It includes:

- Data categorization (e.g., identifying a sales contract vs. a memo)
- Data attributes (e.g., managing big data warehouses)

Stakeholders will understand the negative impact to their brand and punitive privacy penalties arising from a data breach and why a protect first approach makes sense. Ensure your tool selection can support all stakeholder needs and commit to revisit their requirements after enacting your initial data security and privacy safeguards.

Straightforward security measures makes classification simpler
Classification cues downstream tools to invoke controls. Security that relies on multiple factors to cue controls, like DLP and data analytics, adds complexity to classification.

Keep classification simple. If its sensitive, secure it. This enables you to eliminate complexity and streamline classification efforts.

Quick classification win
Our experience has shown that the majority of sensitive content can be found by searching for the most common sensitive data types using basic and proven filters the 80/20 rule. Like:

- Identification number (like SSN), driver's license, passport information
- Bank account numbers, credit card formats
- Health care codes and terminology
- Patent and trademark numbers

Organizations too often start by scanning volumes of unstructured data using multiple and complex filters to meet a full range of governance requirements. Instead, use proven filters first to find the majority of your sensitive content, keep false-positives to a minimum and then layer on more specific searches.

KEY INSIGHT:

Don't let the classification process turn into an academic exercise. Keep a protect first priority to get your data safeguarded as fast as possible.

Protect, Not Alert

Today's DLP and employee monitoring don't secure the data itself: they monitor data (who has access, where the files are stored, etc.) and alert on misuse but don't secure the sensitive files themselves.

Monitor alert approach overwhelms staff
Security and IT professionals must actively administer and respond to thousands of alerts to implement today's solutions. Complex rules and analytics generate a high percentage of false-

positives and the tools often lack the context to prioritize incidents for administrator actions. Already burdened, security and IT are falling behind and will continue to be less effective as data volumes grow.

A better approach is to automatically secure sensitive data with strong protection from the start and for its lifecycle. There won't be repetitive content, analytics scans or ensuing alerts. Your data is truly protected from a breach and valuable resources are available for more productive purposes.

Protect the file, not the locations

Traditional solutions implement rules and analytics at each location where data may reside or travel. It's become increasingly challenging and complicated to scale these solutions with today's cloud environments, mobile workforces and explosion of endpoint devices.

Rather than struggle to control every network, server, cloud service or endpoint device that interacts with their data, protect the data itself. Eliminate multiple implementations and costly administration.

Platform Approach

A protect first, file-centric approach creates a sequence of efficiencies that simplify and streamlines document security through data discovery, classification, protection, audit and policy management. It uniquely enables a purpose-built, automated data-centric platform that enforces centralized policies across your entire data inventory.

Eliminate complexity and inconsistency

You quickly lose control of sensitive files governed by a patch work of policies spread across networks, cloud services and devices.

Centralize policy management and manage security, access control, and privacy settings all in one platform and enforce actions immediately that updates across your entire sensitive data inventory.

Automate

It's essential that privacy and security measures don't disrupt end user workflows. It must be transparent and seamless with controls applied consistently, in real-time and across the entire enterprise. Automate these processes with a file-centric platform:

- Discovery: don't rely on users to determine data sensitivity. Use continuous scanning to find files with sensitive information the moment they are created.
- Data classification: categorize and tag files with automated tools to apply a consistent set of policies.
- Protect: use classification cues to instantaneously encrypt and apply access and rights controls.

Eliminate tool sprawl and achieve lowest Total Cost of Ownership

Deploying point solutions to close each emerging security and privacy gap, at each location data travels, is inefficient and adds operational complexity.

Consolidate multiple security and privacy tools with a platform that's location-agnostic, efficient to administer and layers seamlessly with current infrastructure.

KEY INSIGHT:

The best path to operationalize data security and privacy is to employ highly automated processes and centralized controls that place the burden on the technology and not the end user.

ACT

Data security and privacy is everyone's responsibility and is essential in today's digital organization. It's key to your brand, reputation and essential to building and keeping customer confidence.

One of the biggest challenges you can face is working with multiple stakeholders and departments is the time it takes to resolve data security and privacy issues. With everyone having an agenda or priority – your initiatives can languish or stall.

Use a protect first, file-centric approach to streamline and operationalize your sensitive data initiatives with:

1. Discover to Learn
2. Divide and Conquer
3. Classification
4. Protect, Not Alert
5. Platform Approach

Sales & Partnership: inquiry@fasoo.com

FASOO

WWW.FASOO.COM

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 comprehensive 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

1,500+
Organizations globally deployed Fasoo solutions enterprise-wide

Millions
of users on our platform

70%+
Of employees with security consulting or engineering backgrounds

US HEADQUARTERS: 7315 Wisconsin Avenue,Suite 420, Bethesda, MD 20814