A COMPREHENSIVE APPROACH TO FILE SECURITY AND COMPLIANCE

FORTIFY| COMPLY |SIMPLIFY

FASOO

DIGITAL TRANSFORMATION HAS SCATTERED SENSITIVE FILES FAR BEYOND THE CORPORATE PERIMETER.

Despite significant investments in tools like data loss prevention and user behavior analytics, security and privacy gaps proliferate and data breaches continue to accelerate.

OVERVIEW

Organizations struggle to find the right approach to secure and control sensitive files. Selecting data-centric tools and processes gets even more complicated since many of them have overlapping functions, strengths, and weaknesses. Then add on the flurry of gap-filling point solutions (e.g. CASB, end-point protection) that flooded the market to address cloud and mobility issues; it's no surprise that security, risk and IT teams are overwhelmed.

This brief introduces a comprehensive approach to file security and privacy compliance. Fasoo's powerful file-centric, protect first platform overcomes the limitations of current data loss prevention and analytic solutions to fortify security, enhance privacy compliance, and simplify operations.

The platform:

- Secures the file itself rather than point solutions for every network, file share, cloud service, or endpoint device where it may travel.
- Automatically applies layered protection that travels with the sensitive file by encrypting, controlling user access, and has the option to restrict file usage (e.g., view, edit, save, print).
- Enables a self-reporting file method for the lifecycle of the file to meet audit and privacy requirements like GDPR and CCPA.
- Instantaneously discovers, classifies, and protects sensitive files as created without user involvement or disruption to workflows.
- Consistently applies and enforces centralized policies across the entire data inventory whether

FORTIFY

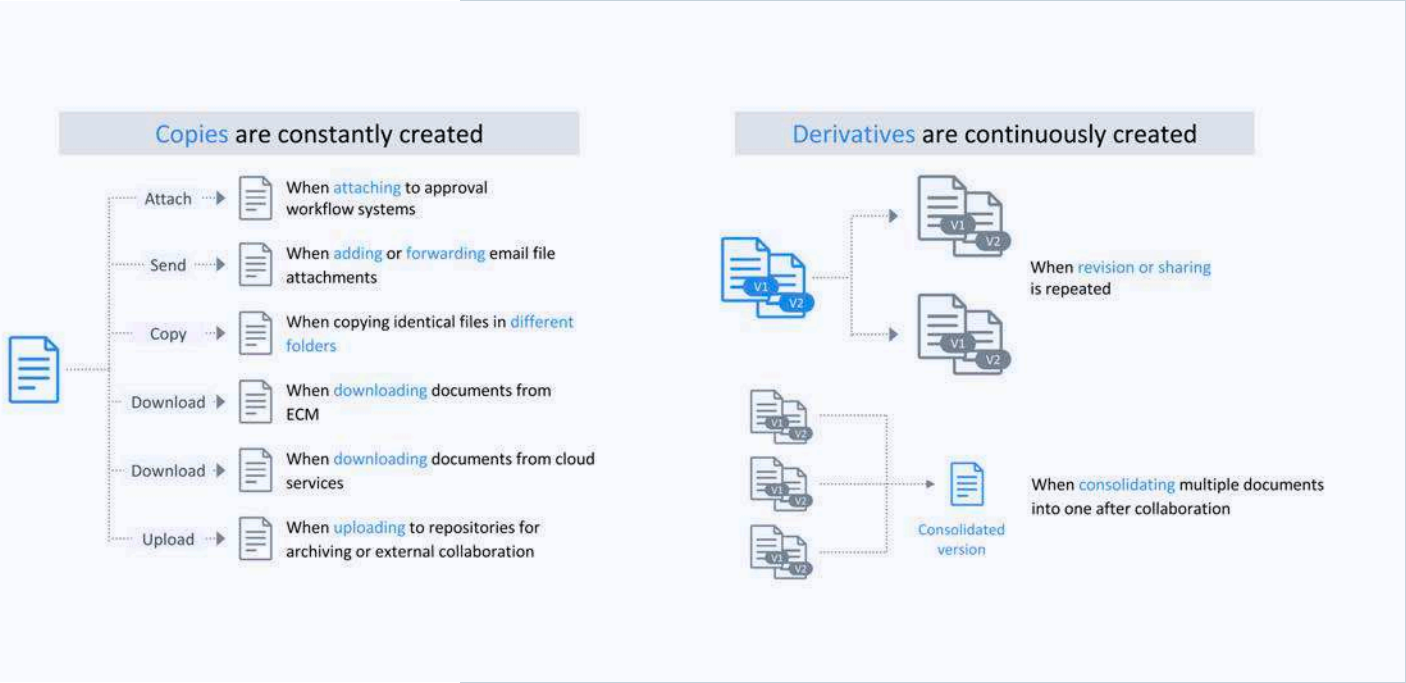
COMPLY

SIMPLIFY

Pioneered by Fasoo, a leading data security and compliance software company, its file-centric, protect first platform is deployed with over 1,500 customers with millions of user worldwide. The platform unifies data discovery, classification, security, reporting and secure collaboration to deliver the highest degree of file security and compliance available in the market today.

AN EXPANDING THREAT SURFACE

Think how many times a day you either create, edit, or share files on different devices as you move from home to mobile to the office. Often using multiple cloud services, collaboration applications and likely downloading and saving files... now multiply that by every employee in your company.



GROWTH OF UNSTRUCTURED DATA

80%

of all business's data inventory is unstructured data

That's a tremendous number of files, often created and used without security or compliance in mind.

Data proliferation is staggering. And unstructured data growth leads the way representing some 80% of business's data inventory. Sensitive and regulated data inside unstructured data formats (word, spreadsheets, presentations, CAD/CAE files) is particularly challenging and creates significant issues for data security, privacy and governance.

Sensitive unstructured files are routinely undermanaged. They represent an expanding threat surface that exposes your organization to data breaches and the resulting consequences.

DRAWBACKS IN CURRENT APPROACHES

Two predominant data security approaches in the market today are data loss protection (DLP) and user behavior analytics (UBA). While using different methods, both share the same challenges in protecting sensitive files that leaves gaps in protection and privacy.

These solutions have failed to keep pace with digital transformation where sensitive files travel and are accessed outside of corporate repositories. They are challenging to scale and leave gaps where sensitive files are exposed to unauthorized access.

It's because they monitor locations, devices and your users, but don't protect the file itself. The approaches worked when perimeters were well-defined and corporate configured desktops were the primary endpoints. But BYOD, mobile, WFH, and cloud services have transformed the digital workplace.

TODAY'S SITUATION

1. An impractical chase to protect each perimeter, user and device where data travels
2. A monitor-alert approach that leaves sensitive files unprotected and staff overwhelmed
3. Inability to enforce consistent controls across hybrid and multi-cloud environments
4. Reliance on disparate systems and device logs to comply with privacy reporting

GAPS LIKE THESE ARE WHY LEADING ORGANIZATIONS TURN TO FASOO'S FILE-CENTRIC PLATFORM

INSIDER THREATS | COMPLIANCE | ALERT RESPONSE

1 WORK FROM HOME-INSIDER THREATS

And now add another new place to chase data – the home office – where DLP and UBA are playing catch up in the race to safeguard sensitive files from insider threats.

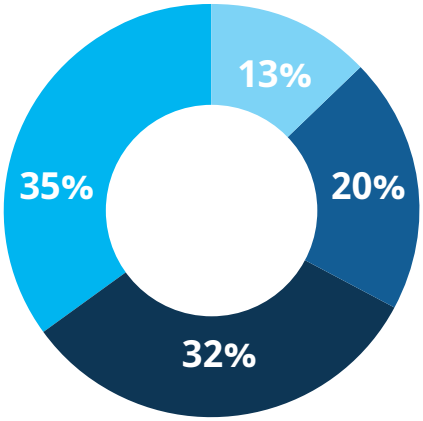
HOW ARE TODAY'S DLP AND UBA SOLUTIONS PERFORMING WHEN IT COMES TO INSIDER THREATS? Not good. Some reports indicate that as high as 90% of insider threats go undetected.

And for those that are detected, The Ponemon Institute 2020 Cost of Insider Threats Global Report found it takes weeks if not months to contain.

DLP wasn't designed for insider threats. While UBA is, its challenged in detecting all events as data moves in and out of organizations and visibility is lost. And neither can stop the most discrete and damaging case – insider threats - when an authorized user with malicious intent downloads, copies, or prints sensitive files.

Enhanced security methods like encryption and granular file controls that restrict actions for data in use (e.g., view, copy, screenshot, print) are needed to stop insider threats.

It's why encryption is now mandated in so many of today's compliance and regulatory standards. In fact, most regulations exempt loss of encrypted files from breach reporting or alternatively, impose significantly reduced penalties.



PERCENTAGE DISTRIBUTION OF INSIDER-RELATED INCIDENTS BASED ON THE TIME TO CONTAIN

- Less than 30 days
- 30 to 60 days
- 61 to 90 days
- More than 90 days

Source: Ponemon Report

INSIDER THREATS

30%

of data breaches are as a result of insiders - employees, contractors, and business partners

RAPID GROWTH

47%

increase in the frequency of insider threats just in the past 2 years, and this number is growing

UNRESOLVED

87%

of data breaches and threats remain outstanding after 30 days

2 COMPLIANCE

It's a runaway train now with over 80 country or regional privacy regulations in existence, with increasingly demanding requirements for data residency, data subject requests and right to be forgotten.

What's this all mean? You need comprehensive visibility and control of sensitive files throughout their lifecycle. Think for a minute what it takes to track the journey of a single sensitive file.

It requires:

- Recording hundreds of transactions per file
- Traced lineage of each file and derivative
- Consistency across corporate IT, cloud services, and BYPD
- Timely audit and regulatory reporting

DLP and UBA weren't developed with GDPR and CCPA data tracing and reporting requirements in mind. Other methods, such as Security Incident and Event Management (SIEM) and an array of other purpose-built privacy tools, have emerged to meet modern day regulation requirements. However, all rely on log data as the source of file tracing which in today's infrastructure is proving more and more difficult.

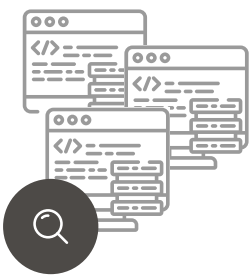
THE PATCHWORK OF DISPARATE IT AND SECURITY TOOLS MAKES FILE LIFECYCLE REPORTING COMPLEX AND PRONE TO ERROR.

TYPICAL COMPANY TOOLS AND LOG DATA

40 → **10T**

NUMBER OF IT & SECURITY TOOLS

TERABYTES OF LOG DATA PER MONTH



Gathering, correlating and reconciling logs across networks, systems, applications and devices is impractical and unsustainable.

A new approach to sensitive file tracing and reporting is needed to comply with today's regulations. Files need to be made privacy-aware to self-report all interactions without reliance on disparate tools and logs.

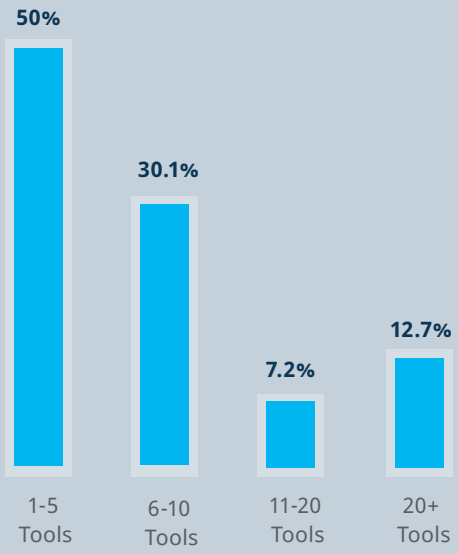
3 ALERT RESPONSE

DLP and UBA cause alert fatigue that leaves gaps in sensitive file security.

DLP and UBA depend on alerts to draw attention to investigate misuse. With increased threat vectors, rapidly evolving business environments, and the complexity of these tools, operational teams are being overwhelmed by these alerts.

A survey by the Cloud Security Alliance recently found that alert fatigue caused by a myriad of tools, generating a large number of false alerts, compromised data security.

ALERTING TOOLS



SECURITY OPERATORS

FASOO'S DATA SECURITY AND PRIVACY PLATFORM

FORTIFY

COMPLY

SIMPLIFY

FORTIFY

Fasoo's file-centric approach fortifies today's enterprise infrastructure with advanced data protection and control methods. It creates a strong frontline defense that closes security gaps in DLP and UBA solutions.

Security Travels with the File

Fasoo automatically secures sensitive files with strong protection from the start and throughout its lifecycle. There won't be repetitive content, analytics scans or ensuing alerts. Valuable staff are freed from alert monitoring when files are truly secured.

ENTERPRISE WIDE ENCRYPTION

Encryption is the strongest method of data protection but is often limited to disks or folders - protecting locations where files reside, not the file itself. It's been historically avoided at the file level because methods relied on users to decide what to encrypt and they alone held the password key. Centrally enforced encryption policies and key management enabled by a file-centric approach puts the organization in control.

ACCESS CONTROL

Identity and access management is another strong security method but is compromised as data travels, particularly in cloud-based infrastructure and software as a service environments. These services often have different levels of security and access control that can leave data exposed to unauthorized access. A file-centric approach binds user access controls directly to the file which is consistently enforced across all environments where the file travels.

GRANULAR FILE RIGHTS

This method extends control to data-in-use: when an authorized user is working on a document. It controls what a user can do with a file in use (e.g., view, cut/paste, print) and is particularly effective for protecting against insider threat, specifically malicious intent. A file-centric approach applies granular controls for maximum data protection.

COMPLY

Fasoo's approach enables privacy-aware files that self-report and can be remotely expired no matter where they reside. This deep visibility and lifecycle control overcomes shortfalls in today's solutions that weren't developed with modern day privacy requirements like GDPR and CCPA in mind.

Persistent Tracking

Each sensitive file is embedded with a unique ID that travels throughout its lifecycle documenting all interactions. The file is also classified and tagged to key downstream security and privacy controls.

SELF-REPORTING FILES

Modern day privacy regulations require detailed mapping of how data is collected, processed, used and accessed throughout its lifecycle. Self-reporting files eliminates working across a patchwork of logs from multiple systems. It provides a single source of truth for audit and regulatory purposes and enables efficient and timely response to compliance requests, like Data Subject Rights.

CLASSIFY

Categorizing and labeling sensitive files as they are created ensures appropriate policies are invoked that govern the handling of the file. Controls implemented at the file level ensures requirements like data residency can be enforced across all hybrid and cloud IT infrastructure and at endpoints. A file-centric approach ensures persistent lifecycle controls travel with the file.

LIFECYCLE CONTROL

Lifecycle control of sensitive files extends well beyond traditional compliance requirements like data retention to today's right to be forgotten and control of data at third parties. File-centric controls enable files to be expired no matter where located, even at third parties. Files can be set to expire at a pre-determined time or access selectively revoked.

SIMPLIFY

Organizations battle tool sprawl and deploying point solutions adds operational complexity. Fasoo's file-centric, platform approach is simpler to implement, less complex to administer, and operates more efficiently than today's solutions.

Integrated Capabilities

A file-centric approach creates a sequence of efficiencies that streamline sensitive data processes and uniquely enables a purpose-built, highly automated data-centric platform.

Discover | Classify | Encrypt & Remediate | Adaptive Access Control | Trace, Audit, Revoke

CENTRALIZE

Today's point solutions, implemented across wide ranging IT networks, cloud services, and endpoints foster inconsistent policies that leave security and privacy gaps. A file-centric approach enables centralized policies that give administrators dynamic enterprise-wide control. Policies are implemented consistently across the entire data inventory no matter the location.

AUTOMATE

Freeing user's from determining file sensitivity and classification helps workflows and eliminates errors. A file-centric approach instantaneously discovers, classifies and applies layered protection to sensitive files without user involvement or disruption to workflows. The embedded ID enables self-reporting files that significantly reduce privacy related administration.

UNIFY

Disparate data-centric capabilities acquired from multiple vendors creates siloed functions that poorly interoperate and leave gaps in visibility and control. A file-centric approach instantaneously discovers, classifies, and applies layered protection to sensitive files without user involvement or disruption to workflows. The embedded ID enables self-reporting files that significantly reduce privacy related administration.

FASOO

WWW.FASOO.COM

In summary

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

FORTIFY
PROTECT FIRST

COMPLY
PRIVACY AWARE

SIMPLIFY
PLATFORM

US HEADQUARTERS: 7315 Wisconsin Avenue, Bethesda, MD 20814