



# SMART CONTENT GOVERNANCE

Unleash The Power of the Modern, Cloud-Based Office...  
Without Conflict or Compromise





**IN TODAY'S KNOWLEDGE ECONOMY,** the most critical business asset is data. The challenge for IT leaders is that the most valuable type of data also happens to be the most sprawling, unstructured kind — content.

Content is data in “human readable” form. It represents the largest source of data growth for modern businesses, and the toughest to manage and control. Whether it's documents, images, videos, schematics, or 3-D renderings, humans, not machines, are the ultimate end users of all this content, and that creates enormous value but also risk. And, unlike structured databases, unstructured information must be first structured in order to understand what data is sensitive and who should (or should not) have access to it.

The traditional approach to content security has been through complex data loss prevention (DLP) deployments that aim to police data as it leaves the environment. Often this includes countless layers of classification, endpoint detection, encryption, access control, and compliance tools. The problem with these approaches is that they create unsustainable levels of complexity, for both IT and end users.

Today, there is a better way: smart content governance. Recent advances in machine learning and AI are enabling companies to deploy a streamlined data governance architecture based on content intelligence that can find and secure sensitive data at its source, and sense and respond to unusual behaviors. Applying rules at the data- and user- level vastly reduces complexity both for users and admins.

**Today, there is a better way: smart content governance. Recent advances in machine learning and AI are enabling companies to deploy a streamlined data governance architecture based on content intelligence that can find and secure sensitive data at its source, and sense and respond to unusual behaviors.**

## What's changed: Explosive growth in data...and risk

Some years back, it was still possible for organizations to require users to label, categorize, or to tag content. That is no longer the case. Every 18 months, data is growing by 50-75 percent. Global business data doubles every one to two years. According to Gartner Analyst, Darin Stewart, the vast majority of that data is unstructured data. A manual approach for content classification is now simply untenable.

The data explosion problem is further multiplied considering data now reside in multiple storage and collaboration platforms spread across various geographies. It's not only harder but also costlier for businesses to keep track of all their data and IP, exposing them to a greater risk of data breaches.

The size and scope of unstructured enterprise content makes the prospect of end-user classification untenable. It is spread out across hundreds, or even thousands of locations and we are beyond the point where it makes sense to rely on a network of humans (your employees) to effectively classify that much content and still be productive.

In the age of GDPR, CCPA, PCI and HIPAA, relying on end users to properly classify data isn't just inefficient, it's risky too. The definition of PII (personally identifiable information) under GDPR alone encompasses potentially hundreds of pieces of information.

## Strategic imperative: Protect the data, not just the infrastructure

As companies invest in stronger firewalls and better IT infrastructure, brute force attacks have become harder to pull off. For companies with little-to-no on prem infrastructure, attackers have found other ways. Often, the fastest route to procuring sensitive data is to compromise a single-user account. Once inside, the attacker can gain access to everything the user is privileged to see. Once inside, any data the user has access to can be exfiltrated, or held for ransom. As a result, it has become



imperative that companies protect the data itself, not just the infrastructure that transports it. By applying strong access control, limiting visibility of sensitive data to only those who need it, and incorporating ransomware detection and unusual behavior detection, companies can be better prepared to take on modern cyber threats.

But how do you do this without impeding user experience and productivity? Adding bulky security layers on top of content repositories undoubtedly increases complexity and cost. According to a 2018 Enterprise Management Associates (EMA) survey, 60 percent of small businesses reported increases in the severity and sophistication of cyberattacks. Yet, 85 percent of those same organizations are hesitant to deploy protections for fear that it will impact the user experience.

Antiquated document security tools and processes that get in the way of productivity are unacceptable to business users.

Smart content governance resolves the conflict between productivity and security by weaving advanced data protection, compliance, and governance into every layer of digital file sharing and collaboration. This has two big benefits. First, the approach works even in modern, “cloud-first” workplaces because it is not confined to physical infrastructure, allowing security controls to travel with the data, to distributed users and endpoints. And second, because intelligence is working behind the scenes to monitor and enforce data-use policies, automate end-to-end data protection and compliance across the content lifecycle, the process does not impede end user productivity.

**Smart content governance resolves the conflict between productivity and security by weaving advanced data protection, compliance, and governance into every layer of digital file sharing and collaboration.**

## The solution: Collaboration and governance powered by machine automation and intelligence

Smart content governance is a new paradigm, which, by leveraging machine automation and intelligence, takes a *proactive* approach to securing data at the source.

Egnyte enables companies to implement the new paradigm with the efficiency of one solution, on one screen.

### A LOOK INSIDE THE EGNYTE PLATFORM

#### **CLASSIFY**

Illuminate dark data by looking deep inside files to identify sensitive content.

#### **COLLABORATE**

Securely exchange files internally and externally, while maintaining control.

#### **COMPLY**

Address compliance blind spots unique to unstructured data.

#### **MINIMIZE**

Reduce the data footprint to minimize risk of unauthorized leaks and compliance violations.

#### **RETAIN**

Keep what is required for legal, business, or regulatory reasons, and delete the rest.

#### **ENABLE**

Build a sustainable enterprise content ecosystem on Egnyte's trusted, secure, flexible enterprise content platform.

#### **SECURE**

Protect your data at the source with robust security built directly into the content environment.

#### **GOVERN**

Gain visibility and control over your riskiest data.

## Collaborate

Collaboration is the beating heart of business — but it is also the biggest source of risk. Egnyte was built to help companies gain control of data without hindering productivity and stifling value.

Egnyte is built to help companies rethink their approach to security by leveraging an inside-out approach. Rather than layer on bulky tools to track, monitor, and restrict file sharing based on content labels or folder location, Egnyte provides a unified environment for storing and sharing files with control built directly in. Granular permissions, sensitive content monitoring, link controls, seamless cloud-device syncing, and content safeguards help prevent unauthorized sharing of sensitive data and eliminate insecure email attachments and consumer-grade sharing apps.



## Classify

Strong governance is built on the principles of visibility and control, and that begins with content-classification policies that are both functional and easy to maintain. The first step in smart content governance is the discovery of sensitive data across the organization. Many organizations struggle to achieve this visibility because data is stored across multiple legacy systems that are cumbersome to manage, siloed, or have no automated data discovery capability.

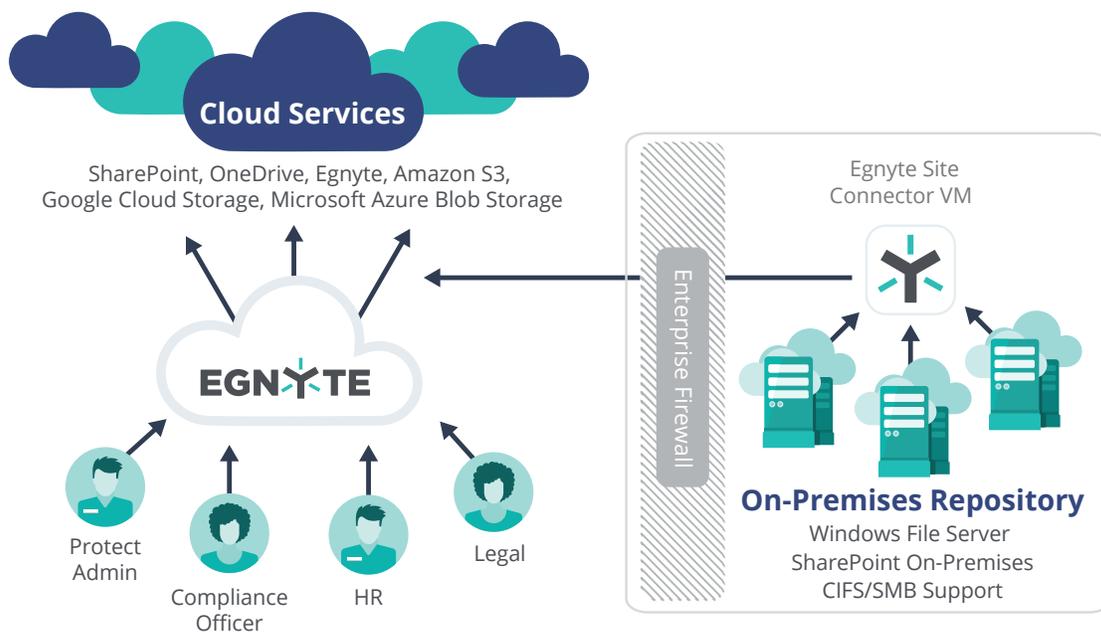
Egnyte's dynamic classification process automatically scans files across linked repositories for sensitive content like credit card numbers, addresses, dates of birth, social security numbers, and health-related information (such as patient ID numbers). Egnyte includes compliance-friendly pre-configurations, as well as custom classification capabilities.

Out-of-the-box configuration options involve selecting the geographic locations where you operate and then selecting the specific regulations that apply to your business. Egnyte then applies the relevant configurations to your classification policies, scanning for data known to be regulated under those laws.

Egnyte also allows for custom policies to be applied based on keywords, patterns, file properties, document templates, file types, and metadata. These can be configured based on specific needs in your organization, classifying data that is sensitive in the context of your business, including data related to a high-profile client, project, IP, or legal action.

Egnyte automates the discovery of sensitive data across the largest repositories (including inside Egnyte), as well as popular data sources such as OneDrive, Windows File Server, SharePoint, Amazon S3, Google Cloud, GSuite, Box, Microsoft Azure Blob, and generic CIFS/SMB repositories.

## EXTENDED GOVERNANCE ARCHITECTURE



## Comply

Egnyte makes it easy for you to adapt to the ever-evolving regulatory landscape by providing more than 30 out-of-the-box patterns to classify data against new and emerging global data privacy regulations. Simply select from the drop-down and start scanning. If regulations change, Egnyte makes the updates so you don't have to.

**THE EGNYTE PLATFORM HAS THE FOLLOWING BUILT-IN POLICIES.**



**APA**  
Australian  
Privacy Act



**CCPA**  
California  
Consumer  
Privacy Act



**DPA**  
Data Protection Act



**FCRA**  
Fair Credit  
Reporting Act



**GDPR**  
General Data  
Protection  
Regulation



**GLBA**  
Gramm-Leach-  
Bliley Financial  
Modernization Act



**HIPAA**  
Health Insurance  
Portability and  
Accountability Act

**ITAR**  
International  
Traffic in Arms  
Regulations



**NZPA**  
New Zealand  
Privacy Act



**PCI-DSS**  
Payment Card  
Industry Data  
Security Standard



**PIPEDA**  
Personal Information  
Protection and  
Electronic  
Documents Act



**SOX**  
Sarbanes-Oxley  
Act



**NOOL**  
Nevada  
Opt-Out Law

**IPDP**  
India Personal Data  
Protection Bill

**LFPD**  
Mexico Federal  
Law on the Protection  
of Personal Data

**LGPD**  
Personal Data  
Collected About  
Brazilian Citizens

Should laws change, Egnyte updates the policy and reclassifies the data. In the leadup to CCPA implementation, amendments were made to minimize the scope of data covered under the law. Egnyte updated the policy and pushed changes to customers behind the scenes, drastically reducing the number of CCPA-related findings — as much as 80 percent for some customers.

Egnyte also streamlines the process for mandatory reporting under laws like GDPR and CCPA. The Subject Access Request (SAR) workflow allows admins and other approved users to quickly search for a user's personal data and export pre-formatted reports to respond to SAR requests). Egnyte also includes reporting functionality for data breach response to maintain compliance with data privacy laws.

## Retain

To comply with contracts and regulations, certain types of data must be kept for defined periods of time. But once that time has passed, maintaining content with sensitive data is both costly and risky. Egnyte allows you to define retention periods based on data-classification policies, folders, or metadata, and automatically and securely purge that content once the retention period has expired. Content marked with retention periods can be deleted from folders, enabling users to effectively manage their work, but won't be purged from the underlying repository until the defined retention period has expired. Retention policies can be locked to prevent accidental or intentional overrides and ensure compliance with regulations as well as peace of mind.

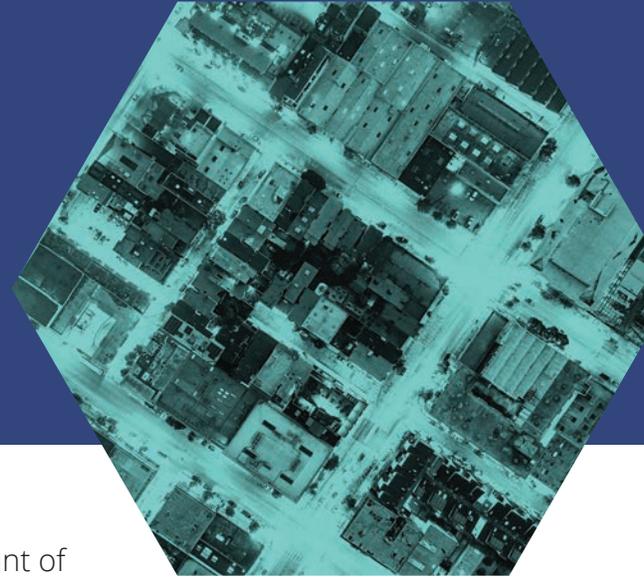
Egnyte supports legal hold, automated archiving for records preservation, and defensible deletion, enabling you to retain required data, purge data that outlives its value and creates risk, and demonstrate compliance.

## Minimize

When it comes to managing risk around business content, unchecked data growth is a major challenge. Whether migrating to new content storage and collaboration options or simply reducing the overall content



## Content Intelligence drives Egnyte's approach to data minimization by providing rich, actionable data on the age, usage, staleness, and redundancy of files.



footprint, organizations are looking to limit the amount of content they maintain to only what is necessary.

Content Intelligence drives Egnyte's approach to data minimization by providing rich, actionable data on the age, usage, staleness, and redundancy of files. Companies can evaluate and drill down on sources of data growth, and take corrective action such as deleting ROT (redundant, old, trivial data) or establishing new lifecycle policies. Data minimization has many benefits, including:

- Decreasing storage costs,
- Reducing risk and compliance costs by limiting the amount of retained content, and
- Optimizing data processing since there is less overall.

### Enable

Users love their apps — let them have what they need to be productive. Egnyte offers a secure back-end to support more than 150 enterprise apps. Egnyte also offers developer APIs and the ability to seamlessly add third-party content sources, such as Windows File Share, SharePoint, Amazon S3, CIFS/SMB, and OneDrive to get the benefits of extended classification and governance.

### Govern

Egnyte provides the tools to define where sensitive content can and cannot live in your repository and alert you when it identifies a problem. Egnyte gives you visibility into when sensitive content is shared externally and allows you to determine whether that sharing is appropriate. If it is appropriate, you can set up exceptions within the system so that you are not alerted when this type of sharing happens again.

The permissions browser allows easy auditing of who has access to different kinds of data, their level of access, and how that access was granted so that you can adjust permissions as needed.

By defining the boundaries of what kinds of data can be stored where, who can access it, and who it can be shared with, you can focus your attention on the content and users most likely to pose a risk.

Good governance becomes easier to maintain over time with good data hygiene practices. Egnyte helps hold your organization to high standards through a process of continuous monitoring and maintenance. The user-friendly interface also enables line-of-business owners to enforce data use policies in their corner of the organization.

Egnyte recommends monitoring and attending to high-risk issues on a weekly basis. As you build your data governance program, this allows you to make configuration changes on-the-go as you refine the user behavior and data-usage patterns that are acceptable. From there, configurations and data-retention policies can be monitored and adjusted on a quarterly basis as data-governance policies become more codified.

## Secure

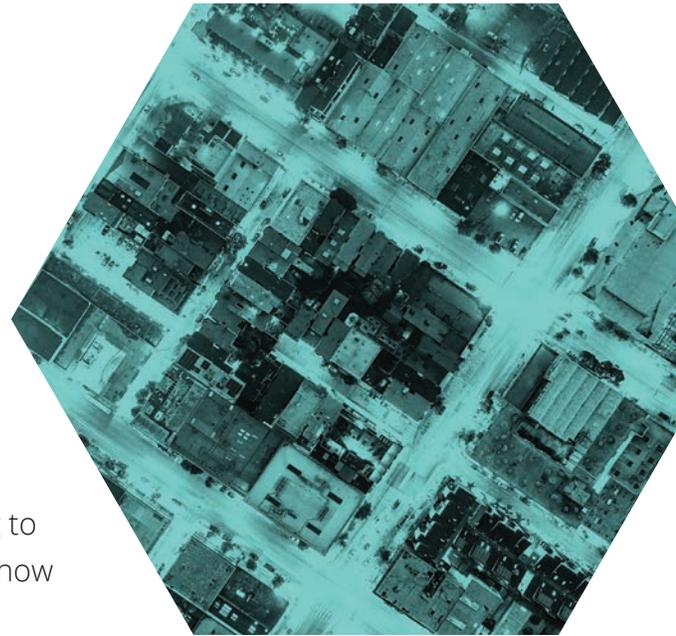
Egnyte was architected to place security closest to the source of risk: enterprise content and the humans that interact with it. It weaves data security into every layer of enterprise file sharing with unusual user behavior detection to deter insider threats and compromised accounts, as well as signature-based and zero-day ransomware detection.

Egnyte offers multi-factor-authentication, AD integration, and secure storage in SOC2 certified data centers and provides encryption both inside and outside the content repository.



**Good governance becomes easier to maintain over time with good data hygiene practices.**

Egnyte has been developed to overcome the alert fatigue that has become common with many data security solutions. Egnyte alerts are designed to act as red flags, rising above the noise and notifying admins of any activity that falls outside boundaries. Additionally, Egnyte provides the ability to customize alerts based on recipient, issue type, sensitive content type, and level of severity. It also leverages machine learning to become better at alerting as it learns more about how users interact with data inside your organization.



When it comes to remediation, a variety of filters allow you to easily drill down into the issues you want to focus on first. From there, administrators can quickly address high priority items by expiring public links that contain sensitive data, taking action on compromised accounts, or moving or deleting sensitive content that is being shared too broadly or stored in unauthorized locations. Additionally, audit reports track key actions taken in the system, like logins, allowing or disallowing sensitive content in specific locations, moving or deleting files, and viewing sensitive content.

### **Powered by the Egnyte Content Intelligence Engine**

The Egnyte Content Intelligence Engine delivers real-time analytics and insight so businesses can keep their data safe while extracting maximum value from their content. Content Intelligence leverages machine learning to proactively identify threats like ransomware and malicious insiders, lock down risky content, and diminish the attack surface by finding and removing old and unused data before it can be compromised.

### **Robust for IT, User-Friendly for Business**

EMA cites the single biggest barrier to implementing better data protection solutions as concern over poor user experience. Many businesses are wary of deploying tools that rely on end-user classification, require hardware or local software installs that may prevent data sharing that is necessary for people to do their jobs, or slow productivity. That is why Egnyte was designed with user experience in mind, leveraging strong, centralized data management and a behind-the-scenes architecture that does not impact workflow.

Modern enterprises need a powerful content services solution that enables them to discover, manage, and safeguard the vast unstructured content that is used to drive their business. It has to be simple enough that it is adopted widely across the organization, and must also align with the organization's security and compliance requirements.

With Egnyte, companies have the visibility they need to spot and stop potential problems and strengthen their overall data security, while maximizing their users' productivity. As the only file-sharing solution that supports multiple deployment options, with cloud and hybrid options, Egnyte provides the flexibility and control needed to address the security, compliance, and collaboration needs of the most demanding organizations around the world.



Egnyte is the content services platform for a content-critical era. Driven by an industry-leading Content Intelligence Engine, Egnyte leverages machine learning and AI to enhance employee productivity, automate data management, and reduce file-sharing cost and complexity. Built with data governance, privacy, and security at its core, Egnyte fuels business growth for more than 16,000 companies worldwide. Investors include Goldman Sachs, Google Ventures and Kleiner Perkins Caufield & Byers, as well as technology partners, such as CenturyLink and Seagate Technology.



**EGNYTE**

[www.egnyte.com](http://www.egnyte.com)