EGNYTE

4 Must-Haves for Cloud-First Content Governance

How to Achieve Complete Visibility, Control, and Protection Over Your Data

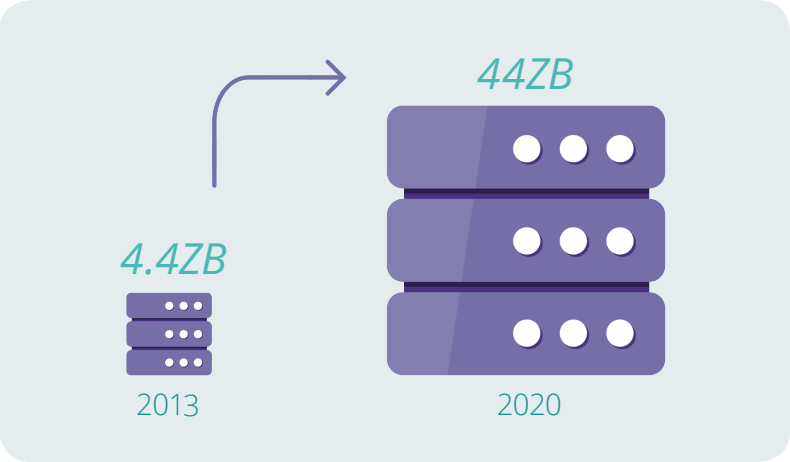
Table of Contents

A Crisis in Content Governance

It's a tricky balancing act: How do you maximise the value you get from your vital business data while ensuring it's secure?

On the one hand, you want anywhere/anytime access to the unstructured content your customers, employees, and partners rely on: documents, images, spreadsheets, presentations, and all the other files that help your business run. On the other hand, you need to maintain control over the sensitive information contained in these resources.

Adding to this challenge is the increasing difficulty of managing the zettabytes (ZB) of new content emerging from the expanding digital universe. As IDC reports, **digital content is on track to balloon to 44ZB in 2020, up from just 4.4ZB in 2013—and 95 percent of it will be unstructured.**[1] This dizzying data sprawl amid cloud and on-premises repositories raises your risk of non-compliance with industry and government data regulations. What's more, the time-consuming, error-prone manual processes you may use to make the most of your content prevent you from pursuing other IT priorities.



The growth of content: 4.4ZB in 2013 to 44ZB in 2020

Concerned? Many of your peers are. In fact, according to ESG, 48 percent of enterprises say that among all data security tools, file sync and sharing applications are most in need of security controls and monitoring oversight.[2]

It's clear: The time for you to take action is now. To get on the path to cloud-first content governance, you have to support your business with these four must-haves:

1. Manage the Entire Data Lifecycle
2. Find Your Most Sensitive Content
3. Promote Comprehensive Compliance Coverage
4. Achieve Rapid Time-to-Value

Here's what you need to know.

[1] IDC, 2014.
[2] ESG: "Meeting Data Governance Requirements Starts with Data Visibility: Tackling the Enterprise Data Management Gap," 2017.

MUST-HAVE #1:

Manage the Entire Data Lifecycle

Modern businesses require a comprehensive yet agile approach to content governance that works from the day content is created to the day it's archived or deleted. With unprecedented data growth making it nearly impossible to manage sensitive content quickly and effectively, you'll want to consider a governance solution that takes your whole data lifecycle into account, regardless of your sources.

Challenges

The more data you house, the higher your risk of being hacked. But without a dedicated governance tool, your IT admins lack the visibility and control they need to protect your content efficiently. It's simply not possible to manage today's volume of data manually unless you have a full-time employee dedicated to enforcing permissions and monitoring sharing of sensitive content. Even if you do, they're likely faced with an overwhelming number of alerts to address—so overwhelming, in fact, that **32 percent of IT professionals report ignoring alerts entirely**.[3] These challenges make it difficult to separate the signal from the noise and, ultimately, to know when it's time to archive and delete data.

How to Overcome

It's not enough to try to apply governance and security measures on top of an insecure repository. Start with a content repository built for your business. You'll unify your multiple data silos and gain better control over all your content, helping to boost productivity and reduce risk. From there, you can add in advanced data governance at every step of the data lifecycle:

- **Discover** sensitive data throughout your organization and where it is improperly shared or over-permissioned.
- **Define** the boundaries of where sensitive data is allowed, who can access it, and how it should be handled.
- **Remediate** exposed over-permissioned data and stop external threats with one click.
- **Get alerted** when sensitive data is outside of defined boundaries, exposed, or under attack.
- **Report** progress on overall risk reduction.
- **Retain** or **retire** data automatically to reduce risk.

The 6 steps of the data lifecycle

[3] Cloud Security Alliance and Skyhigh Networks, 2017.

MUST-HAVE #2:

Find Your Most Sensitive Content

You can't control what you can't see. In order to protect your sensitive business information, you need to know what you have, where it is, who has access to it, and how they're sharing it. Answering these critical questions begins with fast, efficient data classification.

Challenges

Consider the following: Back in 2007, an AIIM report found that **22 percent of organisations provided users with no guidance on corporate classification policies**. Fast-forward nine years later to 2016, and more than a third of admins said inconsistent metadata and classification policies was their biggest issue.[4,5]

If you're still relying on end-users to perfectly adhere to data storage guidelines or to tag files manually using inflexible data classification templates, you may want to reconsider. Not only does this eat up valuable resources, preventing your team from working on other priorities, it provides few safeguards for the times when content is improperly stored or tagged. And let's face it: The human brain can't easily process complex, metadata-based, folder-level, and geography-specific classification rules, let alone hundreds of patterns of personally identifiable information (PII)—and we shouldn't expect it to.

Classification difficulties: the #1 challenge for many organizations

How to Overcome

You can't realistically rely on your team to be able to efficiently and effectively classify your content at scale. Turn to automated data discovery and classification processes that scan the content of all files across your repositories—not just the metadata. With data classification powered by machine-learning, you'll be able to detect and categorise more than 400 sensitive pieces of information like Social Security and credit card numbers, even if they're buried deep within a document.

[4] AIIM: "Industry Watch: SharePoint," 2010.
[5] AIIM: "The Impact of SharePoint," 2016.

MUST-HAVE #3:

Promote Comprehensive Compliance Coverage

GDPR. FINRA. HIPAA. PIPEDA. SOX. GLBA. SEC. PCI-DSS. CCPA. The list goes on. You need to know you're handling unstructured data according to strict government and industry regulations and requirements, from data storage, to PII discovery and classification, to breach notifications, to data subject access requests and beyond.

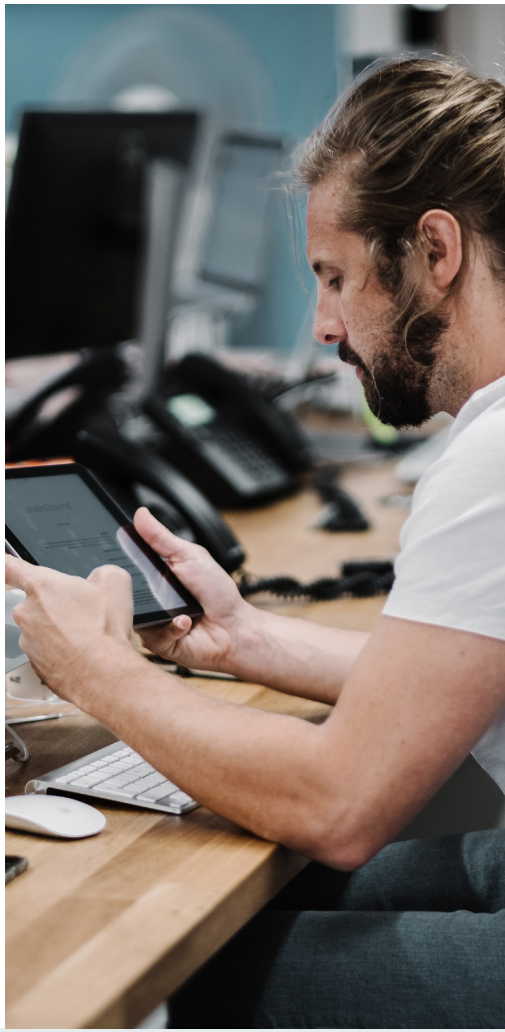
Challenges

Don't have deep visibility into your sensitive content? You're not just hindering productivity and compromising security—you're also making it more difficult to comply with industry and government data regulations, such as GDPR-mandated 72-hour breach notifications and Right-to-Be-Forgotten requests, as well as competing data retention and deletion stipulations in HIPAA, GLBA, FINRA, and others. Fail to meet all your requirements in time, and your non-compliance penalties could escalate as your reputation among customers and partners drops.

A selection of industry and government authorities and regulations

How to Overcome

To promote regulatory coverage that your business depends on, start with a compliance-friendly repository and layer automated data discovery and analysis processes on top of it. This way, you'll be able to easily specify the regulations that apply to your content and flag or resolve any potential violations. With the power to automatically discover regulated data and restrict who sees it, you'll pass your audits, avoid any potential non-compliance penalties, and further boost customer and partner trust.



MUST-HAVE #4:

Achieve Rapid Time-to-Value

The most sensitive content requires the most comprehensive security and governance solution. But when weighing your options, you have to consider the financial, time, and labour costs: Does it work with the budget? Does it require you to provision new servers? Are any professional services needed for setup, maintenance, or support? And how fast can you get it up and running?

Challenges

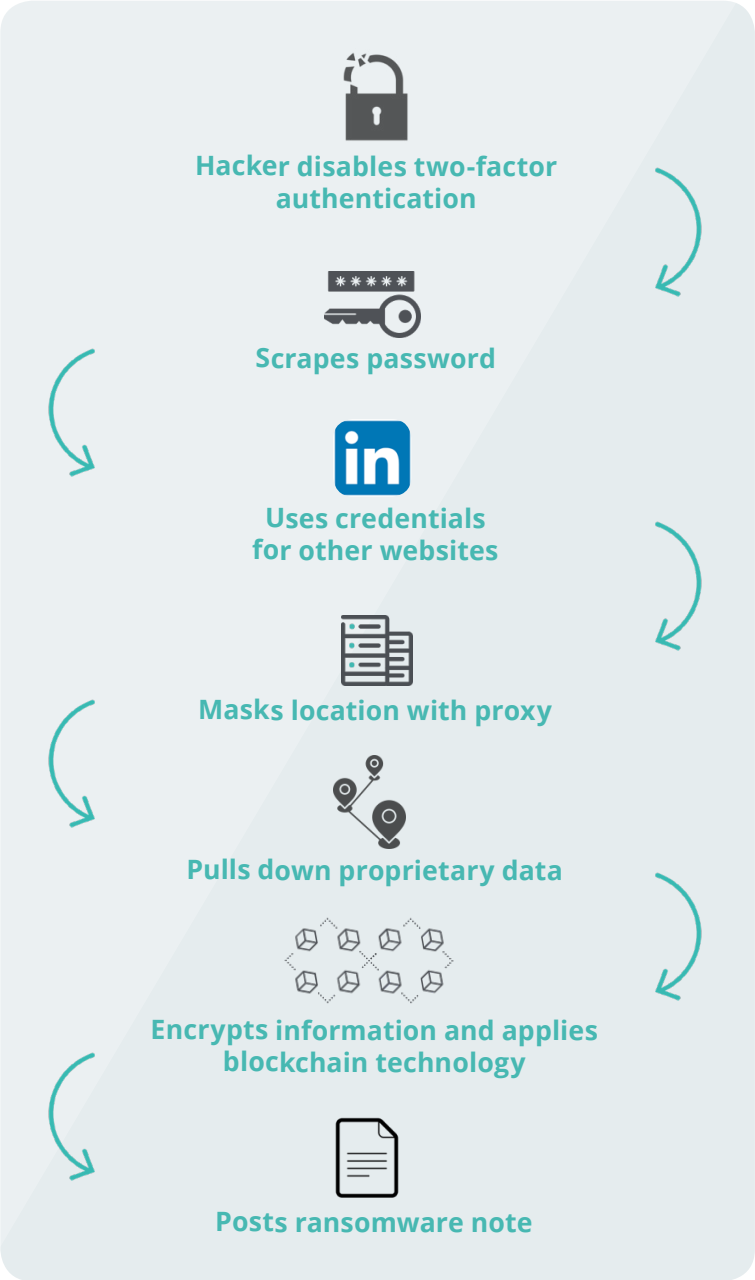
Supporting a new content governance solution usually calls for new hardware, new infrastructure, a team of consultants, and specialised IT skills. Then there are the time and labour expenses, particularly steep costs for the **23 percent of organisations that have only one employee working in the data protection and privacy function.**[6] And the longer you wait to wrangle your data, the riskier it becomes.

How to Overcome

Instead of bringing in new hardware and building a new infrastructure, opt for a rapid-deploy software as a service (SaaS) solution. Why? Because a cloud-first, SaaS delivery makes it possible to scan data and detect issues right away. What's more, a SaaS implementation has more predictable long-term costs and allows you to deploy new features and services without provisioning and maintaining new hardware. Whatever SaaS solution you choose, it should be simple to set up and easy for all members of the team to use—especially if it's a team of one.

The share of organisations that have only one employee working in the data protection and privacy function

[6] CPO Magazine: "Data Protection and Privacy Officer Priorities 2019."



One example of how a ransomware attack against a vulnerable business can unfold

The Importance of Security at Every Layer

As former Cisco Systems CEO John Chambers once said, "There are two types of companies: Those who have been hacked, and those who don't yet know they have been hacked."

Think your sensitive content is completely safe? Think again. Businesses like yours are constantly at risk of a data breach through ransomware and other malware introduced by poor security practices and leaks caused by malicious or careless insiders. Unless you have unusual behavior detection capabilities in place, you may miss malicious insider or careless employee activity. And if you do, you leave your business open to malware threats such as ransomware attacks, in which hackers steal your data and threaten to publish or block it unless a hefty sum is paid.

What makes ransomware attacks such a huge threat to your business is that hackers know you'll pay to get your data back, even though a full half of ransomware victims never end up seeing it again.[7] **And the threat is only growing worse, with ransomware attacks up 195% in the first quarter of 2019—more than a 500% increase from this time last year.**[8]

[7] CyberEdge Group, "2019 Cyberthreat Defense Report."
[8] HIPAA Journal, "Ransomware Attacks Increased by 195% in Q1, 2019."

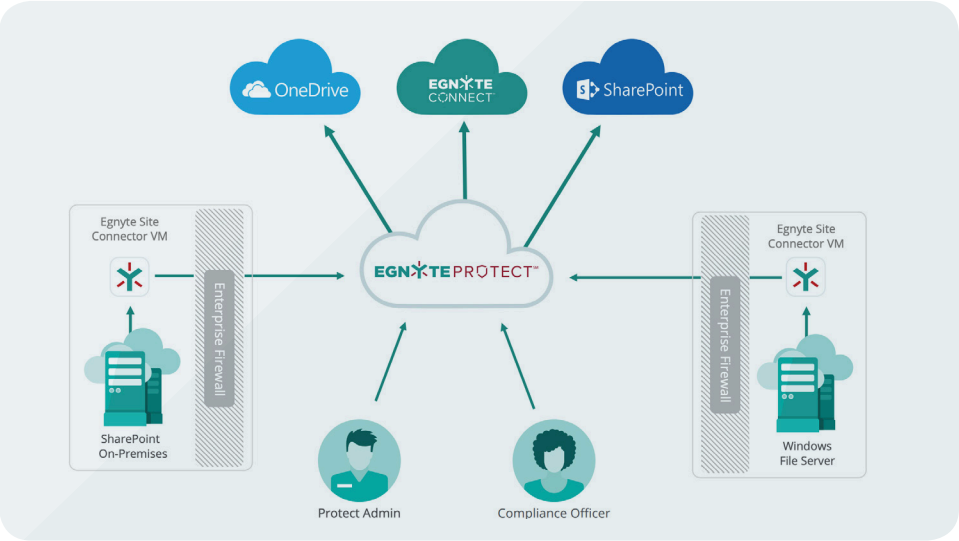
THE SOLUTION:

Complete Visibility, Control, and Protection

So how do you maximise the value of your content and boost visibility and control over your sensitive data, all while safeguarding your business from ransomware and insider threats?

Egnyte offers the leading SaaS-based data governance and compliance solution for businesses. Providing real-time visibility into unstructured data repositories (whether in the cloud or on-premises), Egnyte can help you quickly and easily incorporate all four must-haves of cloud-first content governance into your business.

Egnyte is the first secure content platform built for business, providing data lifecycle management, content classification, and data governance for Egnyte's secure hybrid-cloud repository as well as for third-party sources such as Windows File Share, SharePoint, OneDrive, and more.



A high-level look at the Egnyte architecture

The Egnyte User Experience

With an intuitive end-user experience, Egnyte is easy to navigate. It helps you address key data governance challenges in your organisation through five processes:

1. **Data Discovery:** Use compliance templates and custom keywords or match to more than 400 pre-configured patterns of PII to find the most sensitive data you house.

2. **Permissions:** Search to find which users and groups have access to which folders, check on permissions levels, and see who granted specific permissions.

3. **Content Control:** See which files have sensitive content, who has access to them, and how they're being shared. Need to remediate? Simply move content or delete it from unpermitted locations. With the Content Safeguards feature, you can even protect your repositories from data leaks by automatically restricting outside access to sensitive content.

4. **Threat Detection:** Get alerted when your users download, delete, or access unusual amounts of sensitive data. Detect known ransomware signatures and file extensions in your content repositories and disable compromised accounts.

5. **Data Lifecycle Management:** The greater the data, the greater the risk. Egnyte offers automated, classification-based content retention, archiving, deletion, and legal hold to help you reduce your data footprint with minimal heavy lifting.

EGNYTE IN ACTION:

Top 8 Use Cases

Take a look at some of the many ways Egnyte can empower your business to connect, protect, and unlock value from all your content.

Stop Malicious Insiders:
Analyse user activity to spotlight anomalous behavior and revoke access.

Comply with Data Privacy Regulations:
Discover data regulated under GDPR, CCPA, FINRA, HIPAA, PCI, CCPA and more. Be ready to respond to breach notifications and subject access requests, and establish automatic retention periods.

Prevent Accidental Data Loss:
Identify and correct over-privileged access and public exposure points.

Mitigate Ransomware and Other Attacks:
Detect infected or compromised user accounts and files and take action before it affects your business.

Inventory and Secure Your Sensitive Data:
Locate all your sensitive data. Set and enforce boundaries. Move data from the wrong locations to the right ones.

Pass Your Audit:
Ensure unstructured data repositories are compliant with appropriate regulations, such as HIPAA, PCI-DSS, SOX, GLBA, and SEC. Report on proactive and reactive remediation activities.

Meet Customer and Partner Requirements:
Demonstrate how you protect both your data and their data to become a trusted partner and win more bids.

Optimise Data and Lower Risk:
Minimise your data footprint through policy-driven retention schedules, defensible deletion, and automated archiving.

CUSTOMER SUCCESS STORY:

How Preqin gained control over 9 trillion data points and decreased costs

Preqin has been the most reliable source of data, solutions, and insights for alternative assets professionals around the world. The recognized market leader, Preqin's products and services span a wide range of asset classes, including private equity, venture capital, hedge funds, real estate, infrastructure, private debt, natural resources, and secondaries.

Compared to available cloud options, Preqin's on-premise file servers were beginning to look dated. They weren't built for collaborative workstyles, the evolving regulatory environment, or today's sophisticated multi-cloud world.

As a result, the staff faced considerable delays when accessing files and documents. Recurrent VPN issues meant documents crashed mid-edit. Files corrupted and weeks of work was lost.

Researchers had problems sharing information. Version control was an issue too, with numerous copies of the same data stored on multiple file servers across the globe.

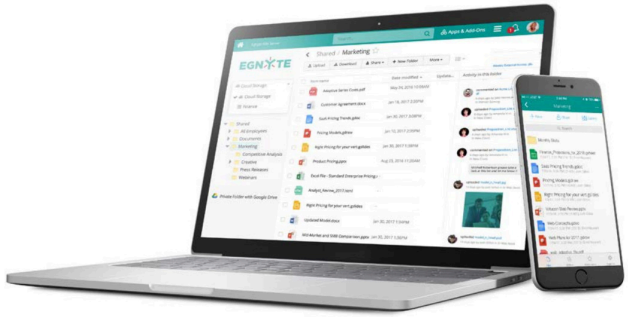
After reviewing solutions– including Microsoft OneDrive – Prequin decided to go with Egnyte's cloud-based file management and sharing solution, Egnyte Connect. It was enterprise-grade solution met all of Preqin's evaluation criteria –from resilience and data residency through to ease of use and user experience.

With more than 400 power users, Egnyte Connect is now the default file management and sharing tool across Preqin's global business. Centrally-managed Egnyte Protect is driving information governance and compliance.

"We have had over 270 GDPR subject access requests. Before Egnyte, each request took three weeks to service. Now it takes as little as 2-3 days"

— Dave Boxall, VP InfoSec & Engineering, Preqin

The IT impact has been significant. The team no longer needs to maintain, update, or patch its poorly performing legacy file server infrastructure. Plus, the on-premise copy eliminates single point of failure and assures business continuity. As secure link sharing takes hold within the company, further savings can be made by retiring SFTP servers. Plus, fewer support calls from users is containing costs and freeing skilled IT resources for other business-critical tasks.



Ready to get started?

Start a free trial online, or contact the Egnyte team today.

GET A FREE, PERSONALISED DEMO

+44.020.3356.3714

EGNYTE | Smart Content Collaboration & Governance

Egnyte transforms business through smarter content allowing organisations to connect, protect, and unlock value from all their content.

Egnyte gives IT centralised control and protection over their files, and gives users fast access to their content—no matter how and where work happens. Founded in 2007, Egnyte is privately held, headquartered in Mountain View, CA and supports thousands of businesses worldwide. Investors include Google Ventures, Kleiner Perkins, Caufield & Byers, CenturyLink, and Seagate Technology.

CONTACT US

+44.020.3356.3714

Central Working
2 Blagrave Street, Reading
Berkshire RG1 1AZ, UK

www.egnyte.com