EGNYTE

Always-On Content Governance: Lessons From the Frontlines

How Four Companies Achieved Visibility and Control of Their Unstructured Data Assets

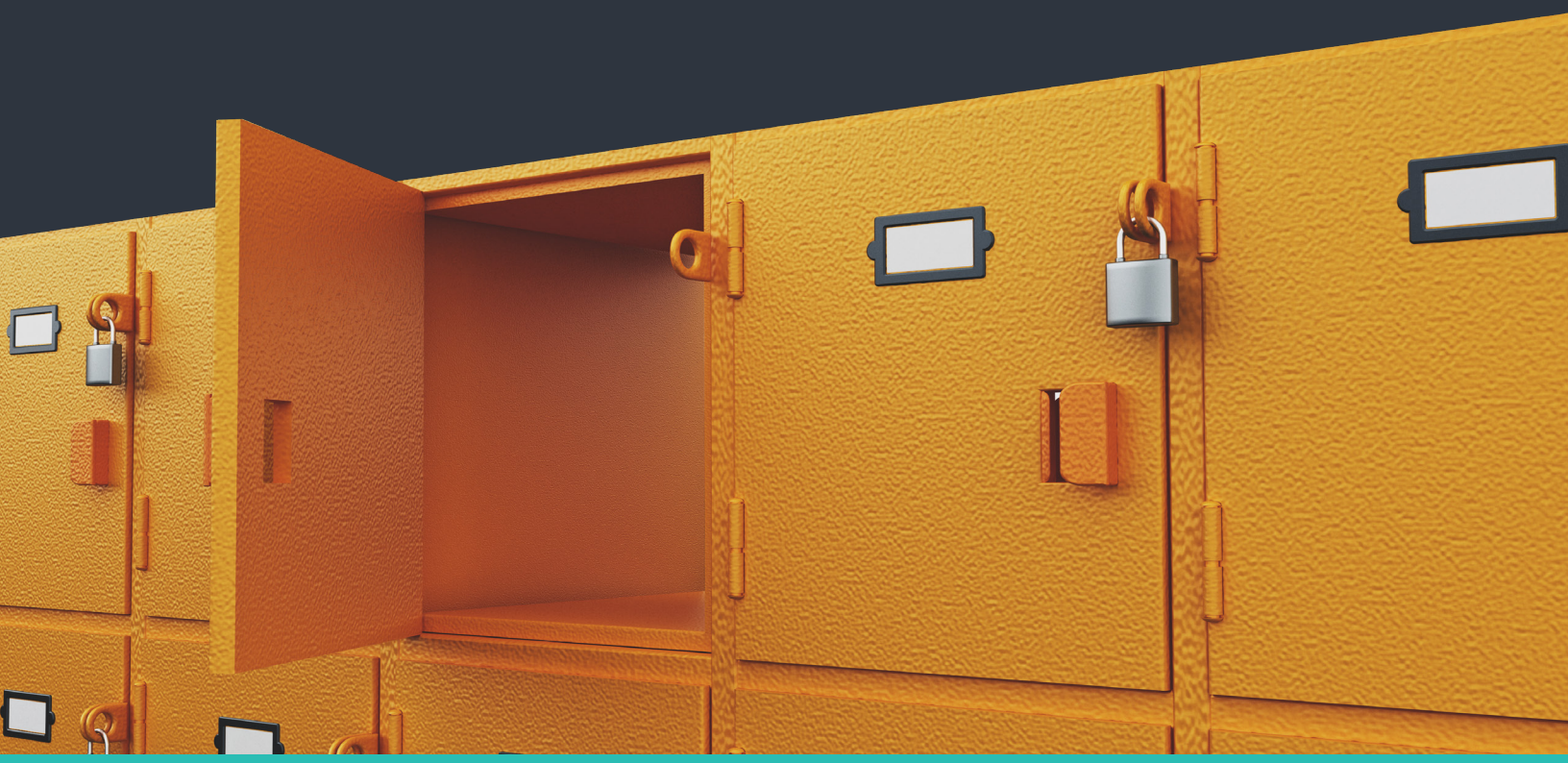


Table of Contents

Introduction

It's a tricky balancing act: how is the value of critical business data maximized while ensuring it's secure?

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

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 ballooned to 44ZB in 2020, up from just 4.4ZB in 2013—and 95 percent of it is unstructured.[1]** This dizzying data sprawl amid cloud and on-premise repositories raises the risk of non-compliance with ever-increasing industry and government data regulation changes. Operating out of compliance can lead to substantial fines and loss of brand trust and customer confidence. What's more, time-consuming error-prone manual processes used to govern and manage content prevent you from pursuing other IT priorities.

Concerned? Most 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]

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."

It's clear: the time to act is now. Four companies already have. Learn how they attained better content governance by taking taking a step to:

- Find the most sensitive content
- Manage the entire data lifecycle
- Promote comprehensive compliance coverage
- Increase governance speed and efficiency

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

[2] IDC, 2014

ROCKBRIDGE

Finding the Most **Sensitive Content**

You can't control what you can't see. In order to protect 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

Challenge

Consider the following: back in 2007, an AIIM report found that **22 percent of organizations provided users with no guidance on corporate classification policies.** Fast-forward nine years later to 2016, and more than a third of admins still said inconsistent metadata and classification policies was their biggest issue.[3][4]

Relying on end users to perfectly adhere to data storage guidelines or to tag files manually using inflexible data classification templates is problematic. 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.

Rockbridge, a private equity firm in the hospitality industry, traditionally relied on labor-intensive internal algorithms to classify company data - much of it containing sensitive information like Social Security numbers and credit card details. The algorithms were time consuming to run and offered little-to-no auditing capabilities. Ensuring useful results required a significant amount of manual work.

Solution

Teams can't realistically be relied on to efficiently and effectively classify 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, it is possible to detect and categorize hundreds of sensitive pieces of information like social security and credit card numbers, even if they're buried deep within a document.

Rockbridge found significant and immediate time savings by implementing Egnyte. Iterative scanning, focused only on changed data, coupled with more accurate detection, cut time spent generating and reviewing compliance reports from 40 hours a week to 10 hours a week. Time previously spent identifying issues were spent proactively preventing or fixing them. It became possible for the IT team to automate immediate action to disable links and move files to the correct location when sensitive data is shared outside of the company.

[3]AIIM: "Industry Watch: SharePoint," 2010.

[4]AIIM: "The Impact of SharePoint," 2016.

GP. Bullhound

Managing 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 manually sensitive content quickly and effectively without a scalable, automated governance solution, you'll want to consider a governance solution that takes your whole data lifecycle into account, regardless of sources.

Challenge

The more data a company houses correlates with a higher risk of being hacked. Since 2015, ransomware attacks on organizations and municipalities have increased considerably; yet, their acceleration is difficult to accurately quantify, as many organizations do not disclose ransomware attacks. The costs to businesses, however, are real and rising: according to a prediction by data-security firm Cybersecurity Ventures, global ransomware damages are forecasted to reach $20B by 2021, vs. the estimated $325M in damages in 2015.

Without a dedicated governance tool, IT admins lack the visibility and control they need to protect content efficiently from these attacks. It's simply not possible to manage today's volume of data manually unless there is a full-time employee dedicated to enforcing permissions and monitoring sharing of sensitive content. Even with that luxury, that employee is likely faced with an overwhelming number of alerts to address—so overwhelming, in fact, that **32 percent of IT professionals report ignoring alerts entirely.**[6] 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.

This was a major problem faced by GP Bullhound, a boutique investment banking firm with offices across eight European countries. They lacked visibility into their data, where it was being stored and how it was being used, putting them in a vulnerable position and subject to attacks, both internal and external.

Solution

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 that allows for the unification of data silos and better control of all content, boosting productivity and reducing risk. From there, it becomes possible to add in advanced data governance at every step of the data lifecycle:

- **Discover** sensitive data throughout repositories 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.

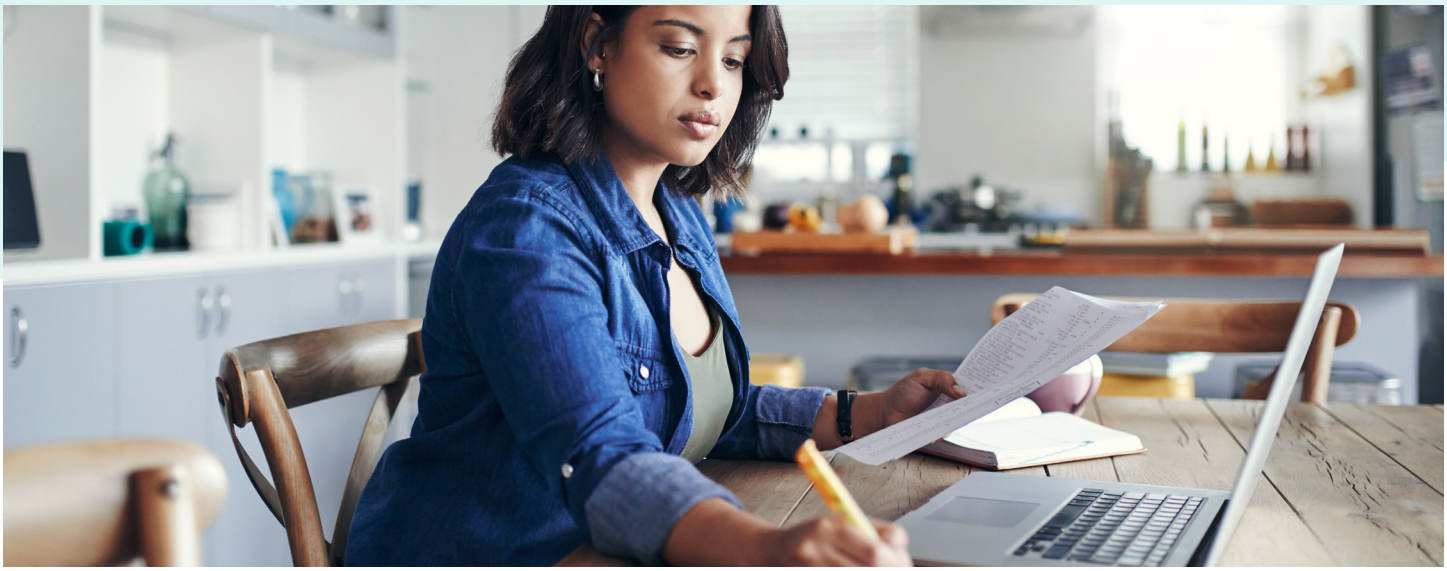
With Egnyte, GP Bullhound found the visibility into external sharing and unusual behavior and alerting helps them implement these strategies. They can monitor their geographies, and get alerts when an employee does something out of their normal profile so that they can investigate further. The team does not have to log into the solution every day to determine what needs follow up, knowing that they will get alerts of high severity issues, like unusually large downloads or deletions, or external sharing involving sensitive data.

"Ignorance is bliss, but once you've seen something you can't unsee it," said Dave Nish, Vice President of Technology at GP Bullhound. "We like the visibility into the 'known unknowns.'"

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

@preqin

Promoting Comprehensive **Compliance Coverage**



GDPR. FINRA. HIPAA. PIPEDA. SOX. GLBA. SEC. PCI-DSS. 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.

Challenge

Don't have deep visibility into your sensitive content? It's not just hindering productivity and compromising security—it's 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 for HIPAA, GLBA, FINRA, and others. Fail to meet all requirements in time, and non-compliance penalties could escalate. In fact, the European Union has levied 11 fines of more than €1M ($1.14 USD) as of July 2020, including a €204M ($232M USD) fine in July 2019, for GDPR violations.

This was the spectre staring down Preqin, a leading European provider of financial data and information on the alternative assets market. With their legacy, on-premises file servers, demonstrating GDPR compliance and actioning subject access and right-to-be-forgotten requests in an efficient and timely manner presented a major problem–exposing the company to fines and damage to their reputation.

Solution

To promote regulatory coverage that businesses depend on, start with a compliance-friendly repository and layer automated data discovery and analysis processes on top of it. This way, it's easy to specify the regulations that apply to content and flag or resolve any potential violations. With the power to automatically discover regulated data and restrict access, it becomes easier to pass audits, avoid any potential non-compliance penalties, and further boost customer and partner trust across multi-national jurisdictions.

For Preqin, the discovery and reporting tools within Egnyte demonstrate compliance with multiple regional, national and state data-protection laws. They also make it easier to stay on the right side of clients. For example, since GDPR came into force, the company has received more 270 subject access requests. Before, each request would take up to three weeks to complete; now requests can be completed within a matter of days.

Balfour Beatty

Increasing Governance **Speed and Efficiency**

The more regulated your (or your customers') industry is, or the more sensitive your content is, the more comprehensive a security and governance solution has to be. But when weighing your options, you have to consider the financial, time, and labor costs: Does it work with your 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?

Challenge

Supporting a new content governance solution usually calls for new hardware, new infrastructure, a team of consultants and specialized IT skills. Then there are the time and labor expenses, particularly steep costs for the 23 percent of organizations that have only one employee working in the data protection and privacy function[7]. And the longer you wait to wrangle your data, the riskier it becomes.

For construction giant Balfour Beatty, the costs of their existing file-sharing and governance systems included, but were not limited to, the IT costs. A typical project involved hundreds of employees and produced tens of thousands of pages of documentation, construction drawings and project specifications. These documents needed to be shared internally and externally with teams of engineers, architects, designers and trade partners. File-versioning issues and miscommunication led to delays and rework, and manual content management threatened to extend closeout times and limit profits for the business.

Solution

Instead of bringing in new hardware and building a new infrastructure, opt for a rapidly deployable software as a service (SaaS) solution. Why? A cloud-first, SaaS delivery can make it possible to scan data and detect issues right away. What's more, a SaaS implementation has more predictable long-term costs and allows the deployment of new features and services without provisioning and maintaining new hardware. Whatever SaaS solution chosen, 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.

By choosing Egnyte, reducing reliance on the VPN and their inherent security issues, and quickly implementing the solution, Balfour Beatty has reduced costs, accelerated closeout time and delivered faster time to value, all of which lead to increased revenue and profit. The IT team no longer has to rely on local staff to maintain file servers and backups, but now achieves the same results with fewer people on a greater scale. In fact, on its initial Egnyte implementation, Balfour Beatty saved an estimated $5M in file-sharing and governance costs.

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

The Egnyte **Difference**

So how can you maximize the value of content, boost visibility and control of sensitive data, and also safeguard against ransomware and insider threats, all at once?

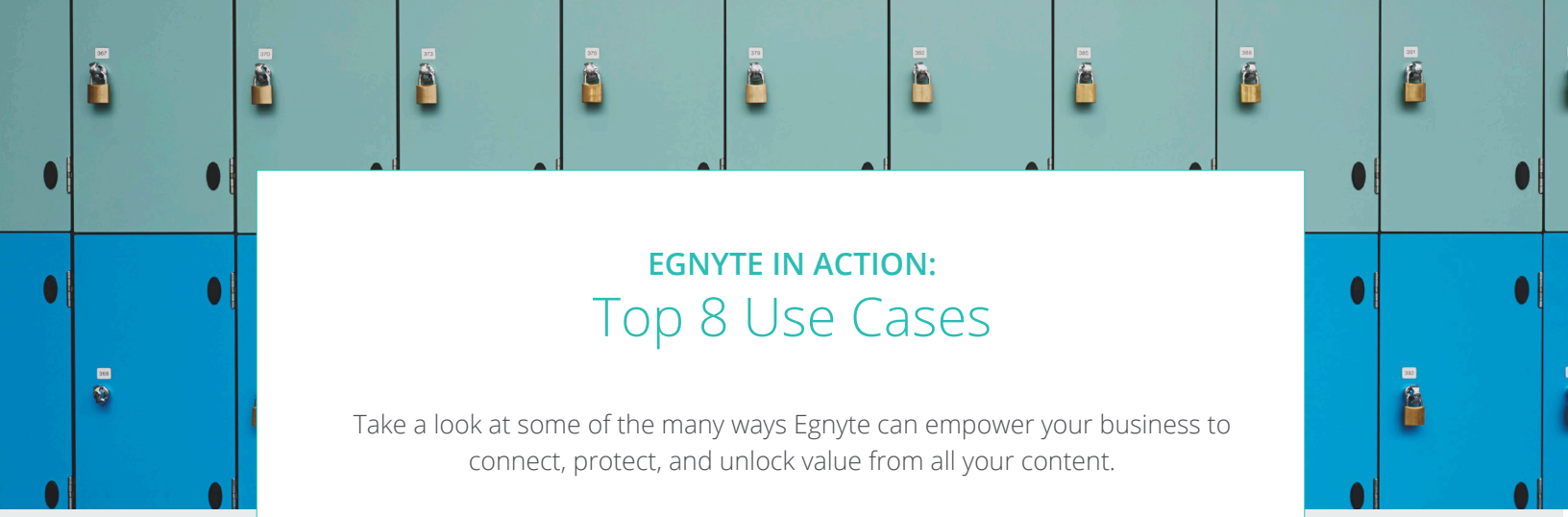
Egnyte offers the leading SaaS-based data governance and compliance solution for businesses. Providing real-time visibility into unstructured data repositories wherever data may reside, Egnyte helps quickly and easily incorporate cloud-first content governance into IT infrastructure.

Egnyte is the first secure content services 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 SharePoint, OneDrive and others. With Egnyte, it becomes easy to provide a unified view of all content, no matter where it lives, while also enhancing user productivity.

The Egnyte User Experience

With an intuitive user experience, Egnyte is easy to navigate for users while being robust enough for admins. It helps address key data governance challenges in organizations through five processes:

- **Content Classification and Sensitive Content Management:** Use pre-built compliance templates and custom keywords or match to more than 500 pre-configured patterns of PII to find and protect sensitive data you house.
- **Permissions:** Search to find which users and groups have access to which folders, check on granular (not hierarchical) permissions levels, and see who granted specific permissions.
- **Content Safeguards:** Create policies to classify sensitive data or leverage machine learning to score files by risk level and protect repositories by automatically restricting outside access to sensitive content.
- **Threat Detection:** Get alerts of anomalies in user activity like mass downloads or deletions or accessing unusual amounts of sensitive data. Detect the presence of known ransomware signatures and uncover zero-day threats right at the source.
- **Data Lifecycle Management:** The more data you have, the greater the risk. Egnyte offers automated, classification-based content retention, archival, deletion and legal holds to help minimize data with minimal heavy lifting. Additionally, the content lifecycle dashboard can show hotspots in file activity, files by age, etc., giving you more insight into the content that lives in your organization.



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:
Analyze user activity to spotlight anomalous behavior and revoke access.

Comply with Data Privacy Regulations:
Discover data regulated under GDPR, CCPA, FINRA, HIPAA, PCI 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 Audits
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.

EGNYTE

In a content critical age, Egnyte fuels business growth by enabling content-rich business processes, while also providing organizations with visibility and control over their content assets. Egnyte's cloud-native content services platform leverages the industry's leading content intelligence engine to deliver a simple, secure, and vendor-neutral foundation for managing enterprise content across business applications and storage repositories. More than 16,000 companies trust Egnyte to enhance employee productivity, automate data management, and reduce file-sharing cost and complexity. Investors include Google Ventures, Kleiner Perkins, Caufield & Byers, and Goldman Sachs. **For more information, visit www.egnyte.com**

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com