



Smart Content Governance



Full Lifecycle Management and Protection of Unstructured Data

Increased visibility, control and protection

TABLE OF CONTENTS

The Growth of Unstructured Data	3
Extracting Business Value From Data	3
Managing and Securing Business Data	4
Protect The Full Data Lifecycle	4
Discover	
Define	
Remediate	
Alert	
Report	
Retire	
Benefits	5
Architecture	7
Cloud Content Repositories	
On-premises Content Repositories	
Protect In Action	8
Use Case 1: Stop Data Theft	
Use Case2: Secure High-Value Content	
Use Case 3: Align Permissions Across Repositories	

The Growth of Unstructured Data

Each year, the “digital universe” grows by 50-75%. At this rate, new data created each year will reach 44 Zettabytes by 2020, which is a four-fold increase from 2016. This includes structured or machine-generated data, and unstructured data generated by humans, e.g. spreadsheets, presentations, documents, email, video, etc.

Businesses are primarily responsible for this huge expansion of unstructured data. The volume of global business data doubles every 1.2 years. With such rapid growth, and multiple storage and collaboration options, it's difficult for businesses to keep track of all their data and intellectual property, putting them at risk for data breaches.

“As data volumes grow, so does the complexity and cost of storing and managing the data... (this) requires infrastructure that many businesses don't currently have or haven't budgeted for.”

IDC white app, sponsored by Dell
EMC, Unlock the Power of Data
Capital: Accelerate DX, May 2018

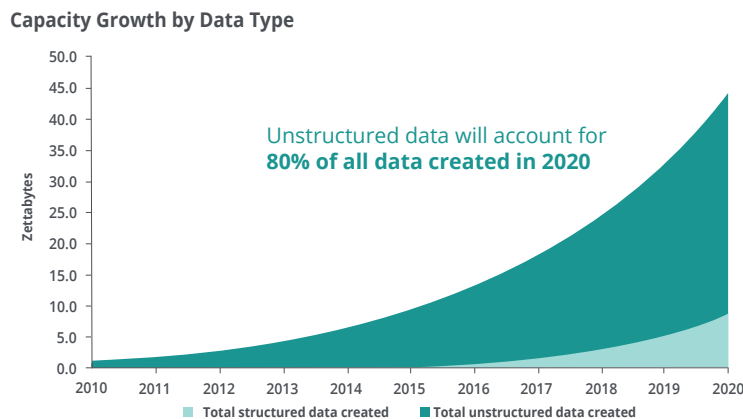


Figure 1: Why you should care about unstructured data [source](#)

Extracting Business Value From Data

The businesses that figure out the true value of data are the ones that succeed. Data drives growth, enabling businesses to differentiate themselves and maintain a competitive edge. In fact, 5 of the 6 most [valuable businesses](#) in the world (based on market cap) are data companies.

“While ‘Big Data’ technologies and techniques are unlocking secrets previously hidden in enterprise data, the largest source of potential insight remains largely untapped. Unstructured data represents as much as 80% of an organization's total information assets,” explains Darin Stewart, Gartner Analyst.”

Valuable data is being created in many different forms, in all parts of the business. For example, written text transactions help customer service companies better understand their customers' preferences; clinical notes help improve patient care and safety for healthcare companies; and even non-financial information can help financial advisors make better recommendations to clients. These interactions between employees and their customers and business partners generate valuable data that may contain sensitive content, like personally identifiable information (PII), data subject to regulatory compliance, or company IP. As a result, businesses face tremendous new challenges to keep this valuable and sensitive data from being intentionally or unintentionally exposed to the public.

Managing and Securing Business Data

Unstructured data is stored in various cloud and on-premises repositories. With so much data being produced, businesses need a tool to manage and protect it throughout its full lifecycle. Businesses should be able to easily analyze and classify the content added to and shared from their repositories in order to build a comprehensive understanding of:

- The types of content they create and maintain, including sensitive data
- Where this content is located
- Who has access to it
- And how it is used, shared, and protected

Because unstructured data can be generated by anyone, it can be harder to manage and protect than structured data. But businesses still need to protect this valuable content from external threats like ransomware, and internal threats like malicious users or unintentional exposure. Gaining full visibility into where unstructured data is stored and how it is used can help businesses prioritize and focus on protecting the most valuable data first.

The future belongs to unstructured data and the valuable business insights it contains. With Egnyte Protect, businesses can more easily locate, control, and protect sensitive content, enabling their employees to freely access relevant data and collaborate with each other, their customers, and their business partners.

Protect The Full Data Lifecycle

The Lifecycle Approach to Protecting Unstructured Content

Every organization handles sensitive data – the personally identifiable information of employees, financial transactions with customers and vendors, legal contracts, etc. The question is whether your organization is handling it properly, adequately protecting it in compliance with regulations, preventing it from falling into the wrong hands, and maintaining it only as long as necessary.

These are the key tasks that Egnyte Protect can help you manage to ensure that your data is protected throughout its lifecycle, from creation to retirement. Our Content Protection Lifecycle approach encompasses the six phases described below: Discover, Define, Remediate, Alert, Report, and Retire.

“With Egnyte Protect, BuzzFeed was able to meet requirements for data governance, without disrupting content creation and workflow, which was imperative to a digital media powerhouse where our content creators are fueling our immense growth. At the end of the day, Egnyte lets us be smarter about our content, which makes us smarter about our business.”

Jason Reich

Director of Global Security
BuzzFeed

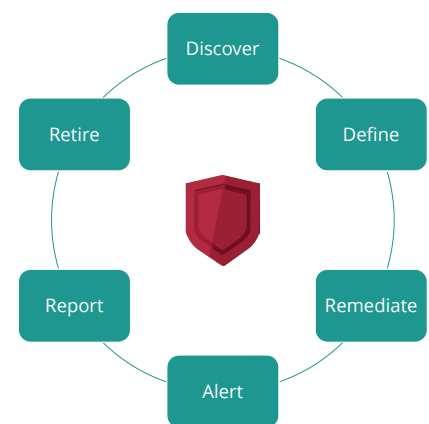


Figure 2: Protect the full data lifecycle

Discover

The first step in the Content Protection Lifecycle is discovery of sensitive data across the organization. Many organizations struggle to achieve this visibility because legacy systems are expensive, cumbersome to implement and manage, and don't provide results in a timely enough manner.

Protect offers both out-of-the-box classification policies, based on jurisdiction-specific regulations like GDPR and HIPAA, and the ability to create custom classification policies tailored to your business. Protect scans reveal all locations with data matching the classification policies. Additionally, Protect scans for:

- Accidental exposure issues like unsecured public links, external sharing, or sharing with large groups
- Malicious intent issues like ransomware, compromised accounts, and unusual access
- Poor practices like individual sharing, empty or unused groups, and malformed permissions

Most initial scans are complete within a week, depending on the amount of data involved. Subsequent scans, which happen in real time, are performed only on changed data.

All issues are assigned a severity score and all locations are assigned a risk score based on the type and amount of sensitive content present. This approach not only gives you visibility into where your sensitive data lives, but also an easy way to prioritize your response based on risk.

Define

Egnyte Protect is architected to allow you to define what's acceptable in your organization, enabling more meaningful alerts while still maintaining complete visibility into sensitive content. Just because sensitive content is detected in a location doesn't mean that it shouldn't be there. Many groups within your organization handle sensitive data on a daily basis. You want to be sure that data is accessible only to those who require it. Egnyte Protect provides the tools to define the types of content that are allowed in specific areas and not allowed in others. The solution can then alert you when that type of content appears in a disallowed location. Further, the Egnyte Protect Permissions Browser allows you to easily audit who has access to different kinds of data, their level of access, and how that access was granted so that you can fix permissions as needed.

Similar to how some sensitive content is appropriate in certain locations (e.g. HIPAA-regulated data in Human Resources folders), some sensitive content is appropriate to share with external parties (e.g. benefits providers). Egnyte Protect 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.

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 that is outside of those boundaries, and more likely to be at risk.



Benefits

FAST

- Up and scanning in <30 minutes
- All data classified within one week
- Automatically scale with zero impact

EASY

- Move from trial to full implementation with no downtime
- Simplified policy definition based on business locations
- Our team of specialists does the policy maintenance work for you

COMPREHENSIVE

- Complete coverage of key unstructured data types
- Over 30 countries, including all EU, US, Canada, Australia, and New Zealand
- Gain full data lifecycle visibility, control, and protection from creation to disposal

Remediate

As mentioned above, Egnyte Protect assigns a severity score for issues and a risk score for sensitive content locations to help you prioritize and tackle the most pressing items first. A variety of filters allow you to easily drill down into the issues you want to focus on first. Most remediation actions can be performed directly from the Protect interface:

- Compromised Account: disable the account, force a password reset, or add a user exception
- Unusual Access: disable the account to stop data theft
- Ransomware: disable the account to stop infection spread
- Public Links: expire the link
- Empty or Unused Groups: delete the group
- Sensitive Content Locations: designate the content as allowed in the location, move the content to another location, or delete the content

However, some remediation actions require permissions changes, which can only be handled from within the underlying repository. Egnyte Protect provides detailed instructions for addressing these types of issues, listed below:

- Sharing files and folders with external parties
- Sharing files and folders with groups with large membership
- Sharing files and folders with individuals, instead of groups as is best practice
- Malformed permissions in Windows File Shares

While Egnyte makes it easy to address issues surfaced in Protect, you may also need to use other approaches. For example, you may determine that a sprawling anything-goes folder structure is no longer tenable in your organization and begin the work to standardize it leveraging the insight provided by Protect. You may find that certain groups of employees are consistently mishandling data and begin an education program. The data Protect provides on how content is handled can help you build support for more comprehensive initiatives focused on improving overall data protection.

Alert

Alert fatigue can be a real problem with security solutions. But content sprawl coupled with increasing cyber attacks, compliance requirements, and fines means that alerts remain a key piece of any data protection strategy. Egnyte strives to ensure alerts issued through Protect are signals instead of noise by giving admins the tools to define what is necessary and accepted in the organization, as described above in the Define section. Alerts should be generated only on what is outside of that definition. Additionally, the Protect solution provides the ability to customize alerts based on recipient, issue type, sensitive content type, and severity/risk level. The more you use Protect, the more the system learns about how data should be handled within the organization, and the more meaningful the system alerts become.

“Solutions such as Egnyte Protect Solution offer IT departments the SaaS delivery of a solution that comes with built in analytical insight, scalability, security and quick time to value to control content in the cloud and on-premises.”

Sean Pike

Program Director, eDiscovery and Information Governance, IDC

Report

Systems like Protect provide visibility into the risk posed by sensitive data in your organization. Being able to report on that risk and how it is mitigated over time is critical to demonstrate the effectiveness of your data protection program. Access issues and sensitive content location lists can be exported from the system and shared with relevant business units. 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, among others.

Retire

Certain types of data must be kept for defined periods of time. But once that time is past, maintaining content with sensitive data is both costly and risky. Protect allows you to define retention periods based on either folders or content types, 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.



With Protect, Egnyte:

- Shows you where your sensitive data is located across your organization
- Helps you better manage exposure, permissions, and access
- Support adherence to best practices
- Alerts you on critical deviations
- Ensures that data is maintained only as long as necessary and properly disposed to reduce overall risk.

From creation to disposal, Egnyte protects the full data lifecycle.

Architecture

How Egnyte Protect Works

-  **Egnyte Protect** - Delivers content classification, identifies issues, sends real-time alerts, enables remediation
-  **Content Repositories** - Can be a cloud EFSS solution like Egnyte Connect, OD4B, SharePoint Online, or on-premises repositories like SharePoint Server or Windows File Server

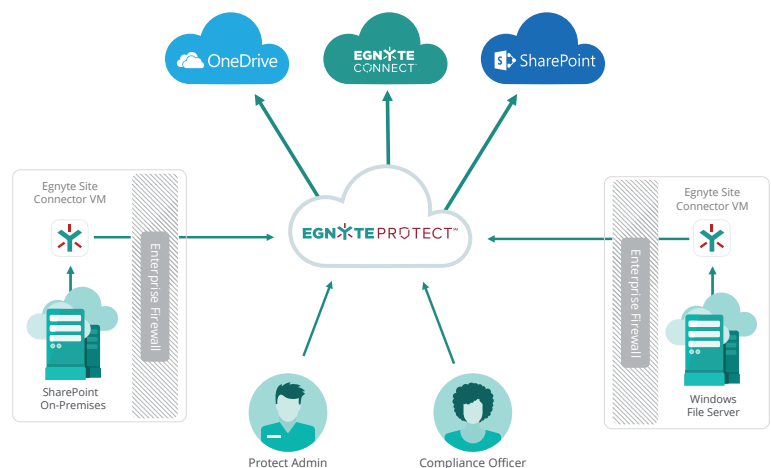


Figure 3: Egnyte Protect integrates with multiple repositories in the cloud and on premises.

Cloud Content Repositories

An Egnyte Protect cloud deployment consists of a connector service that serves as a conduit between the cloud repository and the Egnyte Protect cloud-based service. A tenant within the Egnyte Protect cloud-based service can be hosted in either the U.S. or the E.U., depending on customer need.

On-premises Content Repositories

An Egnyte Protect on-premises deployment consists of an on-premises Site Connector VM and a Windows Service agent that runs on each on-premises repository. These components serve as a lightweight conduit between the on-premises repositories and the Egnyte Protect cloud. One Site Connector is required per site and it can easily scale as the number of repositories increases.



Protect In Action

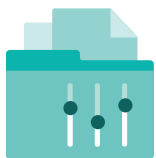
Use Case 1: Stop Data Theft

An employee is planning to leave the company, but has not shared this with anyone. She downloads an abnormally large number of files from the enterprise content repositories. Egnyte Protect uses a machine learning algorithm to forecast expected usage. It notices this abnormal user behavior and sends an alert to an IT administrator.



Use Case2: Secure High-Value Content

The R&D team regularly collaborates on high-value content including product roadmaps, customer data, patents, engineering diagrams, etc. with other parts of the company, and it's often kept in different repositories depending on the project. The CISO uses Egnyte Protect to make sure the sensitive content is secure and only resides in designated locations. She starts by blacklisting public folders and creating a custom policy to detect the high-value content, and then whitelisting the folders where it's allowed (e.g. Engineering folder). In addition to this, there are pre-defined classification templates (e.g. PCI-DSS, HIPAA, GLBA, GDPR, etc.) to ensure that all of her content repositories comply with industry-specific regulatory requirements. This gives her peace of mind without added complications.



Use Case 3: Align Permissions Across Repositories

The finance organization in your company is using a SharePoint server for file management, while the marketing department is using a cloud-based file sharing solution to access and share content. Egnyte Protect scans the files in the cloud and on-premises repositories to determine if the access permissions are aligned and if they meet compliance. All of this happens with no impact on end users.



READY TO GET STARTED?

GET A FREE DEMO



Egnyte transforms business through smarter content allowing organizations to connect, protect, and unlock value from all their content. Our Content Intelligence platform delivers smart content collaboration and governance in the cloud or on-premises to thousands of businesses around the world even the most regulated industries. Founded in 2007, Egnyte is privately held and headquartered in Mountain View, CA. Investors include venture capital firms, such as Google Ventures and Kleiner Perkins Caufield & Byers, as well as technology partners, such as CenturyLink and Seagate Technology.

www.egnyte.com | +1-650-968-4018 | 1350 W. Middlefield Rd, Mountain View, CA 94043, USA