SANS

Analyst Program

Product Review

# Take Sensitive Data Protection to the Next Level in 2024

Written by **Dave Shackleford**

December 2023

EGNYTE

# Introduction

Global organizations are adopting cloud solutions for a variety of compelling reasons—from new business opportunities to reduction in cost to overall improvement in operational efficiency. Sadly, cyberattackers are taking advantage of the rapid proliferation in cloud data and the lack of comprehensive data protection strategies. A recent Wall Street Journal article found that cyber insurance claims for ransomware attacks increased 27% in the first half of 2023, and the number of 2023 incident notifications had already surpassed the 2022 total.[1] In addition, victims were on track to pay $900 million in ransom payments by the end of 2023, up from $457 million in 2022.

Data protection in the cloud is one of the more significant challenges facing enterprises today. Huge challenges—including compliance and privacy violations, potential breaches or exposure, and accidental misconfiguration of cloud services and data storage objects that could lead to illicit data access—affect enterprises that rely on users to collaborate and share sensitive data in the cloud.

In its updated Top Threats to Cloud research[2], the Cloud Security Alliance lists numerous risks to cloud data, including:

- Insufficient credential and key management
- Accidental cloud data disclosure/exposure
- Cloud storage data exfiltration

Organizations seeking to properly secure data in cloud environments must (out of necessity or for regulatory compliance requirements) consider the vast array of options for storing the data depending on the types of collaboration services in use. While doing so, they need to understand how the solutions might impact government-related and industry cybersecurity mandates.

There are many different controls to consider and implement, most of which are specific to the data types and services customers are using. Key considerations for any cloud data security strategy should include encryption and data protection services and options available within the cloud, data life cycle and archival options, backup capabilities, data loss prevention, and data storage monitoring.

The most recent SANS Cloud Security Survey found that nearly 60% of enterprises are looking to the cloud for disaster recovery and business continuity strategies, 42% are focused explicitly on archiving and storing data, and more sensitive data than ever is being stored in the cloud.[3] With this shift, it's imperative that we look at more capable, progressive options for cloud data storage and protection, which is why we were excited to review the Egnyte secure collaboration platform.

---

[1] "Ransomware Comes Back in Vogue for Cybercriminals," www.wsj.com/articles/ransomware-comes-back-in-vogue-for-cybercriminals-5f09091?mod=Searchresults_pos2&page=1

[2] "Top Threats to Cloud Computing Pandemic Eleven," https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven

[3] "SANS 2022 Cloud Security Survey," www.sans.org/white-papers/sans-2022-cloud-security-survey (Registration required for download)

In this review, the SANS team accessed Egnyte as both an end user and an IT administrator responsible for data security and collaboration best practices and policies. After reviewing the platform, we found that Egnyte:

- Provides a variety of excellent and granular dashboards that highlighted specific risks and aspects of data security in our account, as well as vertical-specific reporting for financial services, life sciences, etc.
- Has a wide range of data security policies and controls that range from ransomware and malware detection to sensitive data recognition and protection, as well as permissions and auditing controls
- Supports several storage systems including Microsoft 365, Google Drive, Amazon S3, Azure storage, Salesforce, and more
- Offers strong data classification and life-cycle controls, along with regulatory and compliance reporting. They also have "Snapshot Recovery" capabilities as a lightweight backup system for ransomware recovery.

For organizations looking for a comprehensive data storage and sharing platform in the cloud, we recommend considering Egnyte for its relative ease of use, strong visibility, and alerting controls. The platform shows what data is within each user account and how security programs can be structured to accommodate cloud storage services with more capable controls than traditional on-premises models. It also includes a strong AI engine that can help to analyze data quickly and efficiently. This product and those like it could facilitate a more robust defensive strategy that helps prepare for ransomware and other malware, as well as overall business continuity and data recovery practices.

## Egnyte User Experience

Today, many organizations rely on cloud-based services to aid users in coordinating file sharing and project collaboration. As attackers increasingly focus on end users, security options like sharing and encryption become more important. Egnyte provisioned us with a prebuilt account environment. To begin, we looked at the core options and capabilities available as an end user of the solution. The web-based interface was simple to use, with files and folders readily available, and a simple navigation model as depicted in Figure 1.

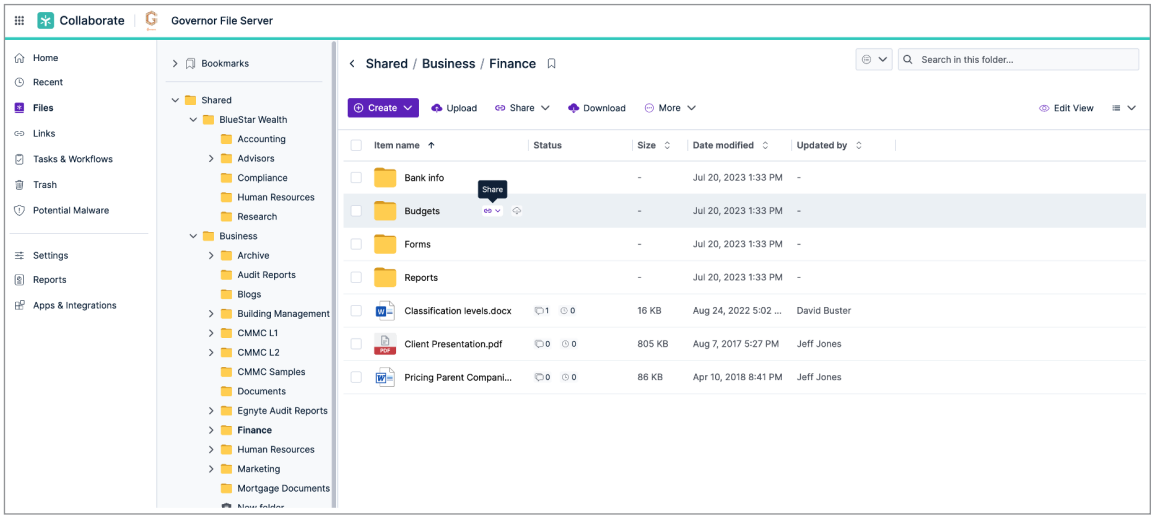


*Figure 1. End User Web Interface*

Although we didn't test this, the Egnyte team demonstrated that we could integrate the platform into Windows and Mac (or mobile operating systems) as an application and as a shared drive for simple and easy accessibility. The interface was highly intuitive with regularly accessed files and links to files and directories. Within this interface, we also could easily share or edit documents, making this an amazingly simple collaboration platform tool. Users can easily link and share documents and files as well, with options to share with anyone, only users with a specific password, only Egnyte users, or a specific group of users, as shown in Figure 2.

Users can mandate encryption for downloads as well as watermarks that include the IP address of the recipient to track them. Users also can choose to have link shares expire on a certain date. As shown in Figure 3, user sharing also can be restricted by centralized policies that govern sharing capabilities, access to shared documents, and sharing expiration. Although administrators can enforce curbs on what users can and cannot do with sensitive information, Egnyte provides greater user flexibility than many solutions by also offering the ability for users to manage document security themselves where appropriate, alleviating operational overhead on admins.

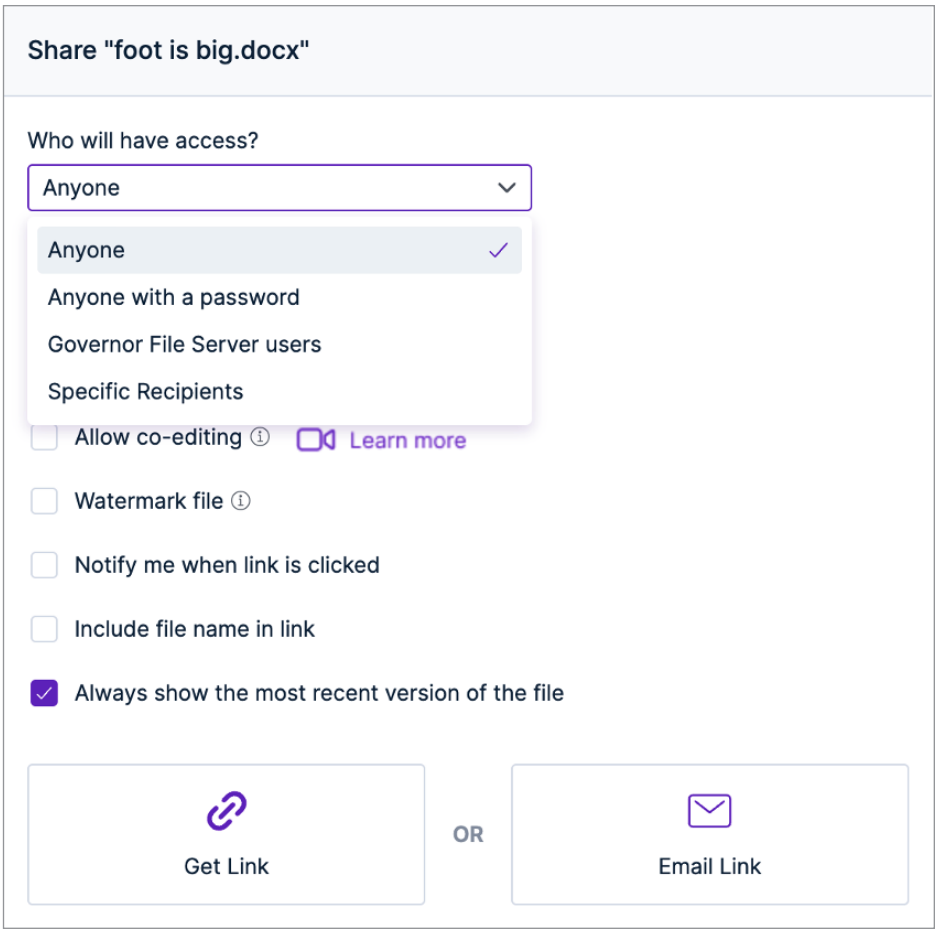


*Figure 2. User Document Sharing Options*

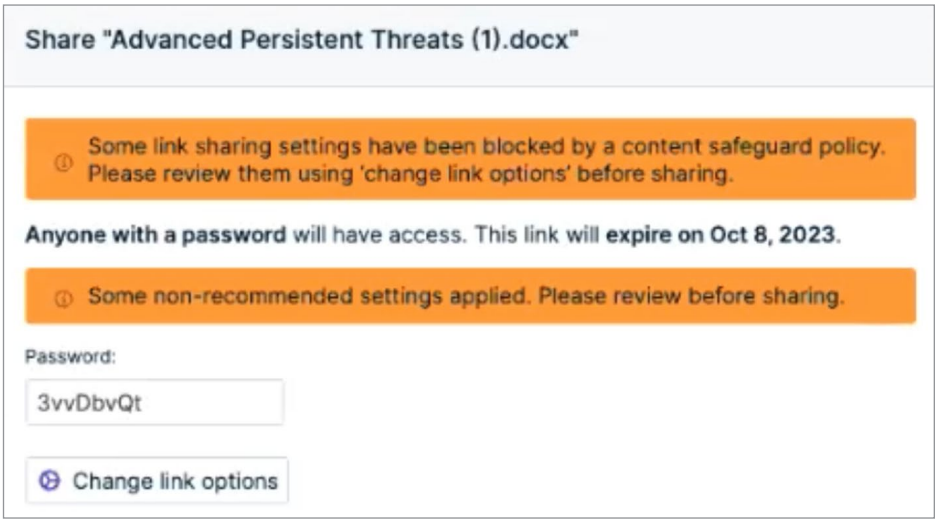


*Figure 3. Centralized Content Sharing Policies*

Users also have enormous flexibility in adding and controlling folder permissions, as shown in Figure 4.

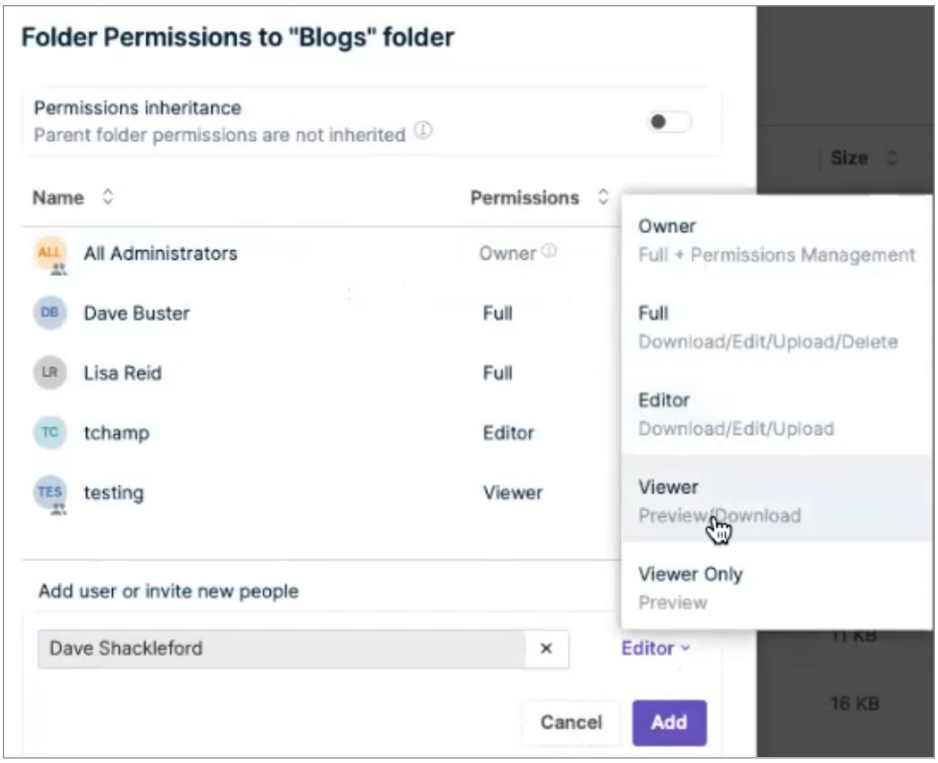


*Figure 4. Folder Permission Control by Users*

For all files, version control and history information are available to users. In addition, all files uploaded into Egnyte are scanned against VirusTotal's known signatures for malware analysis, which can be used to quarantine suspicious files. If files are somehow corrupted (by ransomware, for example), all files and folders structures are automatically captured in snapshots on a regular basis to support full restoration for ransomware recovery. Egnyte leverages AI capabilities to look for unusual patterns of access or behavior related to file uploads, access, and export to determine what may be malware or suspicious/malicious behavior too. The "Potential Malware" section of the end user interface highlights any suspected files that could be compromised, making it easy to investigate and/or troubleshoot.

It was clear that the platform has security and suspicious/malicious behavior detection built into the users' perspective, which could easily lead to better security awareness and education training.

## Large Language Model AI Document Features

Egnyte recently rolled out additional AI to help users work with files. The Preview screen allows users to ask questions about a document and have ChatGPT respond with answers based on the contents of that document. Users can ask for specific information to save tedious searches for individual specifications or can request broader information such as "which location had the highest concentration of contamination." In all cases, Egnyte provides a link to the specific location where the information was found in the document for verification.

## Sensitive Data Discovery and Protection

After reviewing the end user experience, we shifted into the administrative side of things within the Egnyte platform. Egnyte provisioned us with an administrator account, so we quickly accessed the “Secure and Govern” menu of the platform where security and operations teams can configure and enable policies and settings. The “Summary Dashboard” in Figure 5 shows a list of open operational issues, risks, and more.

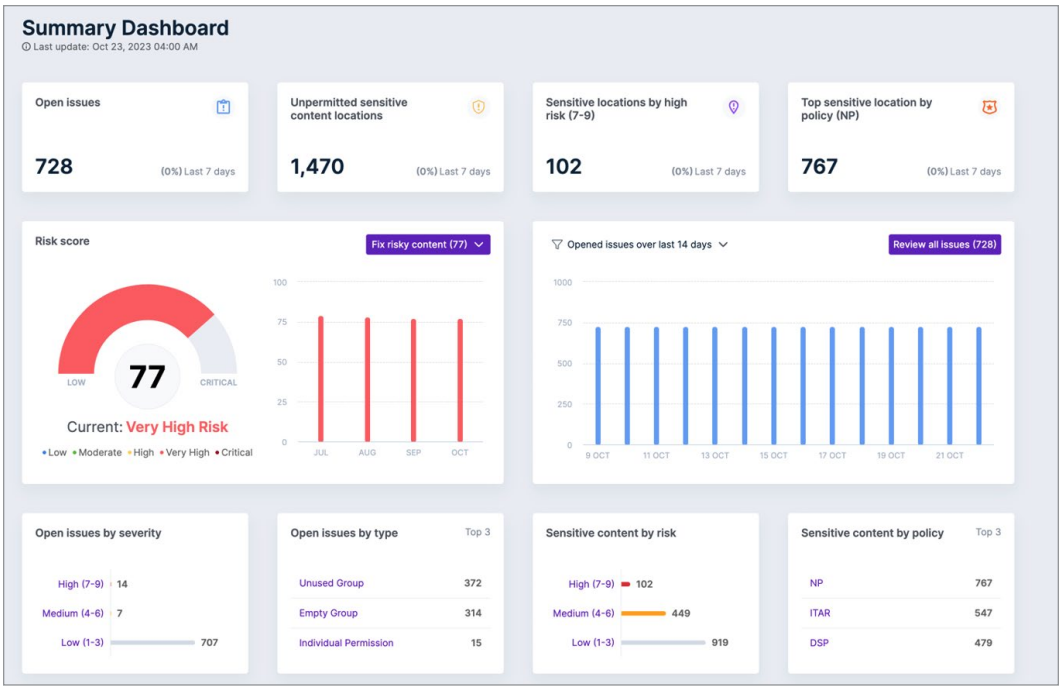


*Figure 5. Summary Dashboard in Egnyte*

Any of these sections can be clicked to gain more granular detail about specific areas. For example, we wanted to drill into the high-risk issues that significantly influence the risk score shown on the main dashboard. After selecting the “Fix risky content” menu on the dashboard, we then chose the option to view “Open issues with high severity,” which took us to the “Issues” dashboard shown in Figure 6.

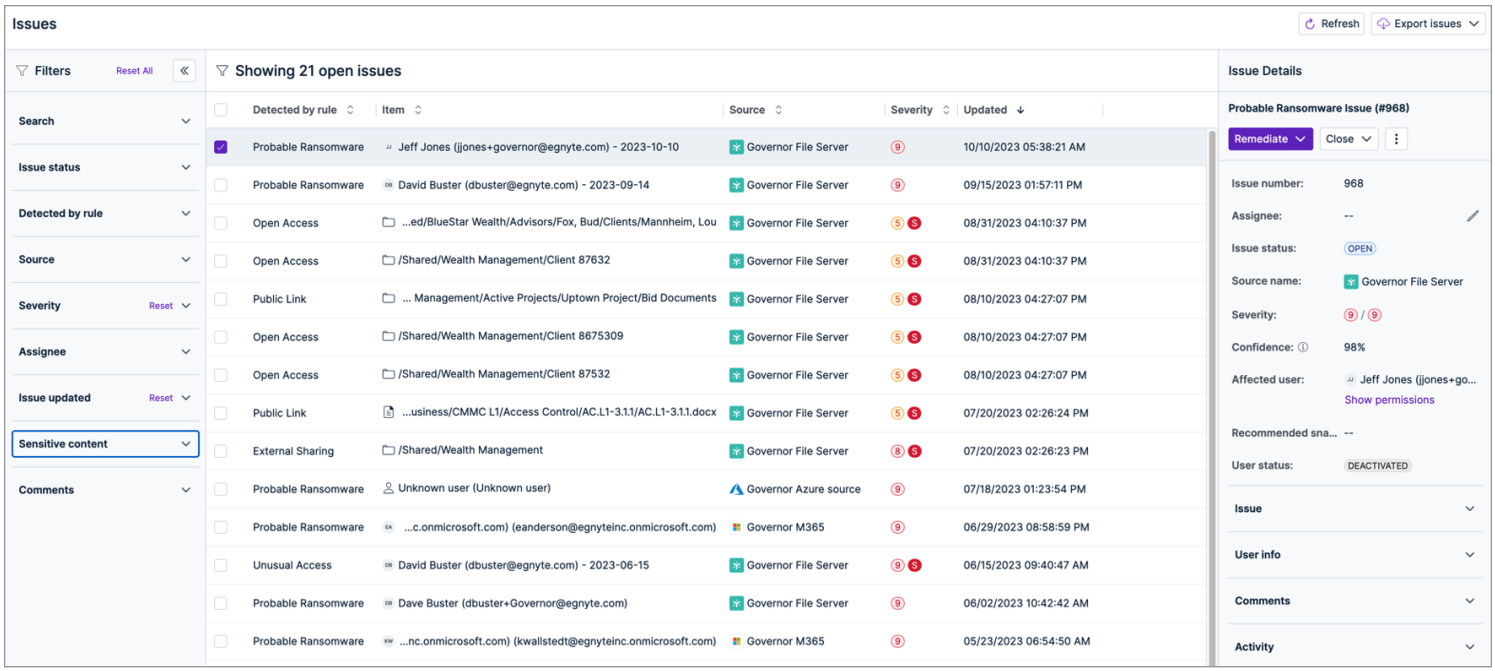


*Figure 6. High-Risk Issues Dashboard*

This dashboard offers a wide range of functionality for administrators. We specifically filtered the issues by name or issue ID, issue status, the triggering policy rule, the data source, severity, who the issue was assigned to, how recently the issue was updated, the type(s) of sensitive content associated with the issue, and more. This dashboard also conveniently allows administrators to assign issues to specific users or groups as well as to perform remediation actions such as deactivating an account, removing permissions, restoring content from a backup in the case of ransomware, configuring IP address allow lists, and many others.

Although we didn't configure or add these ourselves during the review, it's worth noting that Egnyte supports an enormous range of content sources, including on-premises file shares as well as a long list of cloud-based storage services, as shown in Figure 7.

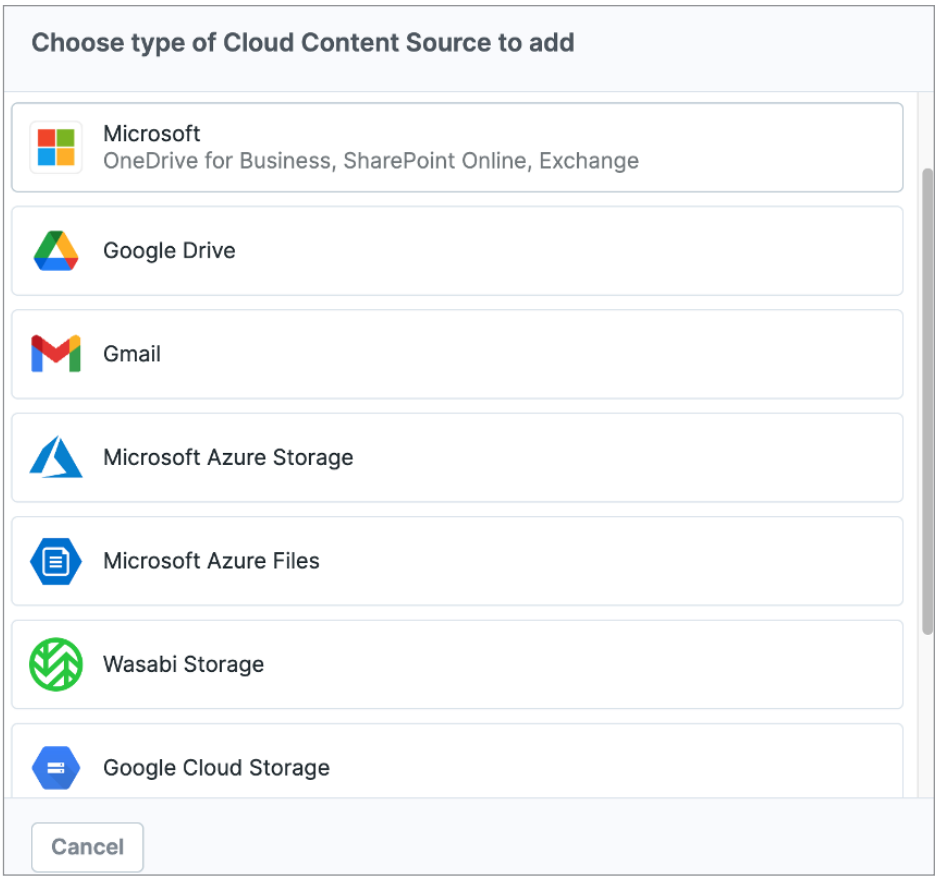


*Figure 7. Examples of Cloud Storage Services Supported by Egnyte*

Amazon S3, Dropbox, and others are also supported, which makes Egnyte a strong centralized security and collaboration control platform for a diverse, multicloud organization that may have numerous types of storage in use. This is a significant benefit because Egnyte can scan these repositories natively and automatically, relieving organizations from the burden of setting up unique data assessment and protection policies for each of them.

One of the strong security features offered in Egnyte is the range of available analysis rules, which covers the following types of potential issues that are automatically scanned within storage environments:

- **Empty groups—**Groups with no users
- **External sharing—**Files and folders made accessible to users outside your organization
- **Inactive users—**Users who have not been active within a configurable time period
- **Individual permissions—**Files and folders with permissions assigned to users, not groups
- **Open access—**Folders accessible to large groups of users
- **Probable ransomware—**Detection of user accounts that are likely infected with ransomware
- **Public links—**Files and folders with publicly available links
- **Suspicious logins—**Unusual login activity that may indicate a compromised account
- **Unused groups—**Groups not used to assign any permissions
- **Unusual access—**This policy detects user activity related to large numbers of files accessed or downloaded, which can indicate insider threat activity.

In all cases, these policies not only are enabled by default, but they also are configured easily by selecting them and choosing configuration parameters and individual risk rankings. “Unusual Logins” detects logins from different locations that could indicate impossible travel or access from forbidden countries. In Figure 8, the policy for “unusual access” is shown—an administrator can simply select the user behavior that should be monitored and flagged for indications of potentially compromised accounts or insider activity (including an unusual number of files accessed by that account for that particular user, time of day ranges, and more).

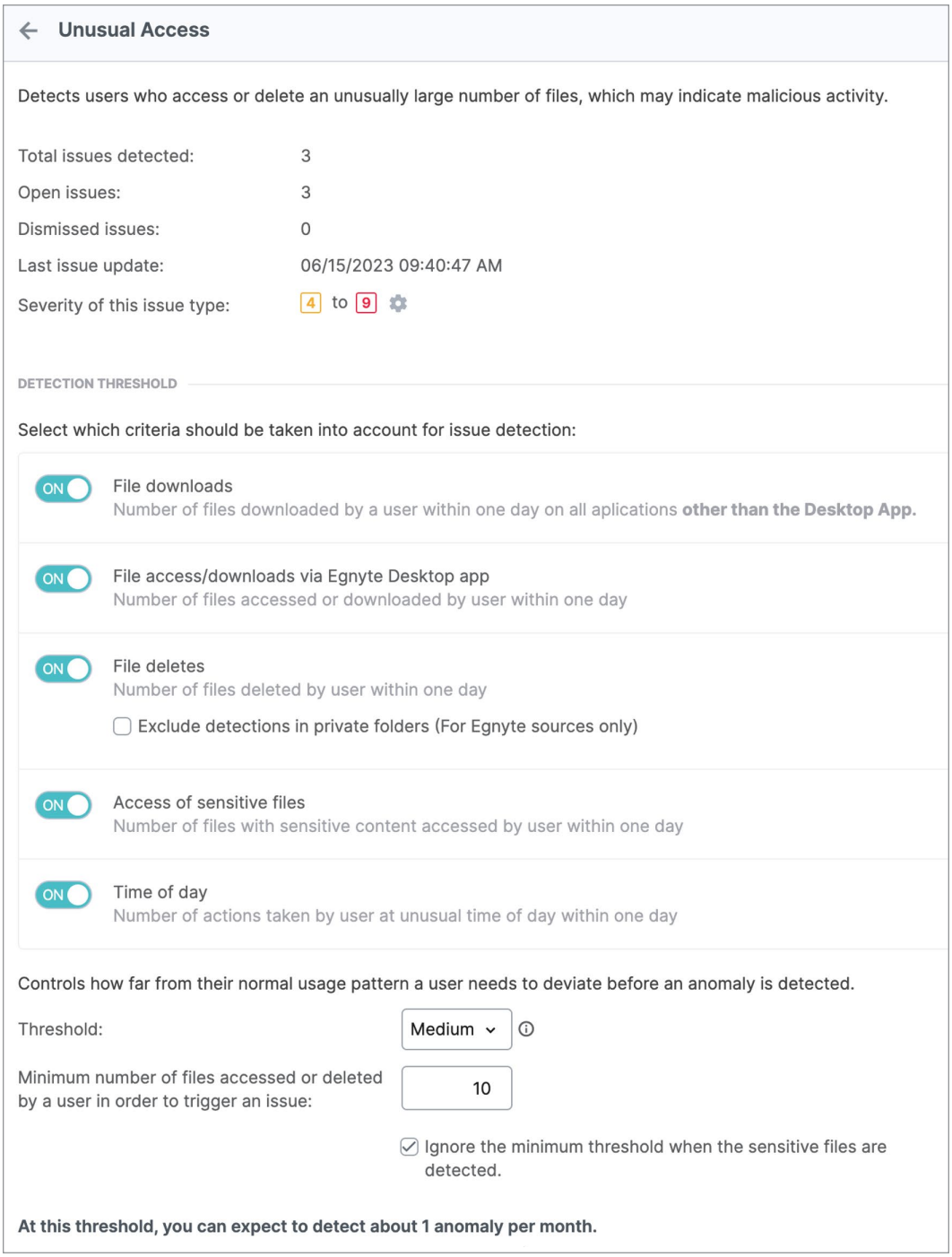


*Figure 8. Configuring a Detection Policy*

Egnyte employs a sophisticated machine learning (ML) and AI-based model in the background to monitor activity, looking for signs of ransomware infection and suspicious account activity. Egnyte's models are purpose-built for each individual user—profiles are developed based on their actual patterns of normal activity. Another example of Egnyte's ML model is detection of ransomware activity. Ransomware can be detected based on sophisticated patterns of content and file access that Egnyte monitors and tunes over time. This could be related to specifically disallowed file extensions, the number of files accessed, sudden changes in file structure or extensions, and even just the entropy of changes within a folder and/or account within a given period (see Figure 9).

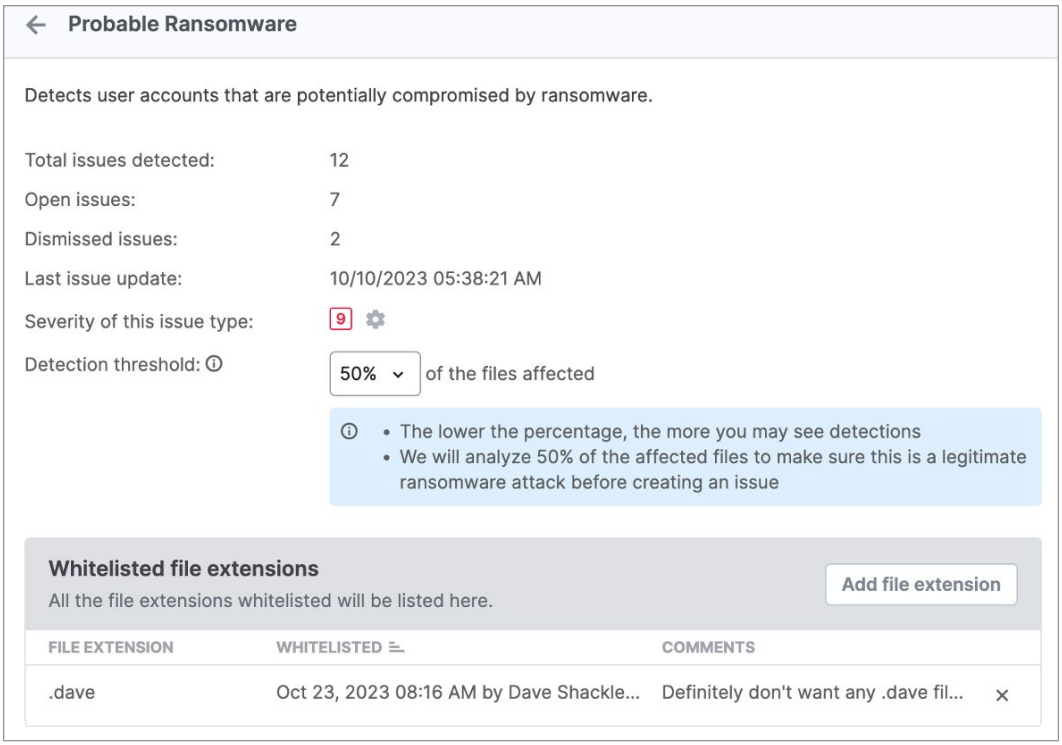


*Figure 9. Probable Ransomware Policy with a Blocked Extension*

## Permissions

As we would expect with a sophisticated collaboration platform, Egnyte supports granular permissions that can be set for users and groups across any files and folders. The platform comes with several built-in roles, including full administrators, basic users who simply need to store and access content, read-only roles for auditing and monitoring, data owners who have more control over specific content types and locations, and power users who may need more flexibility in sharing and managing content. Customized roles can be created easily with an interface that simplifies setting configuration for permissions, issues management (for example, if any issues related to that role come up), access to and control over sensitive content, and more. See Figure 10.

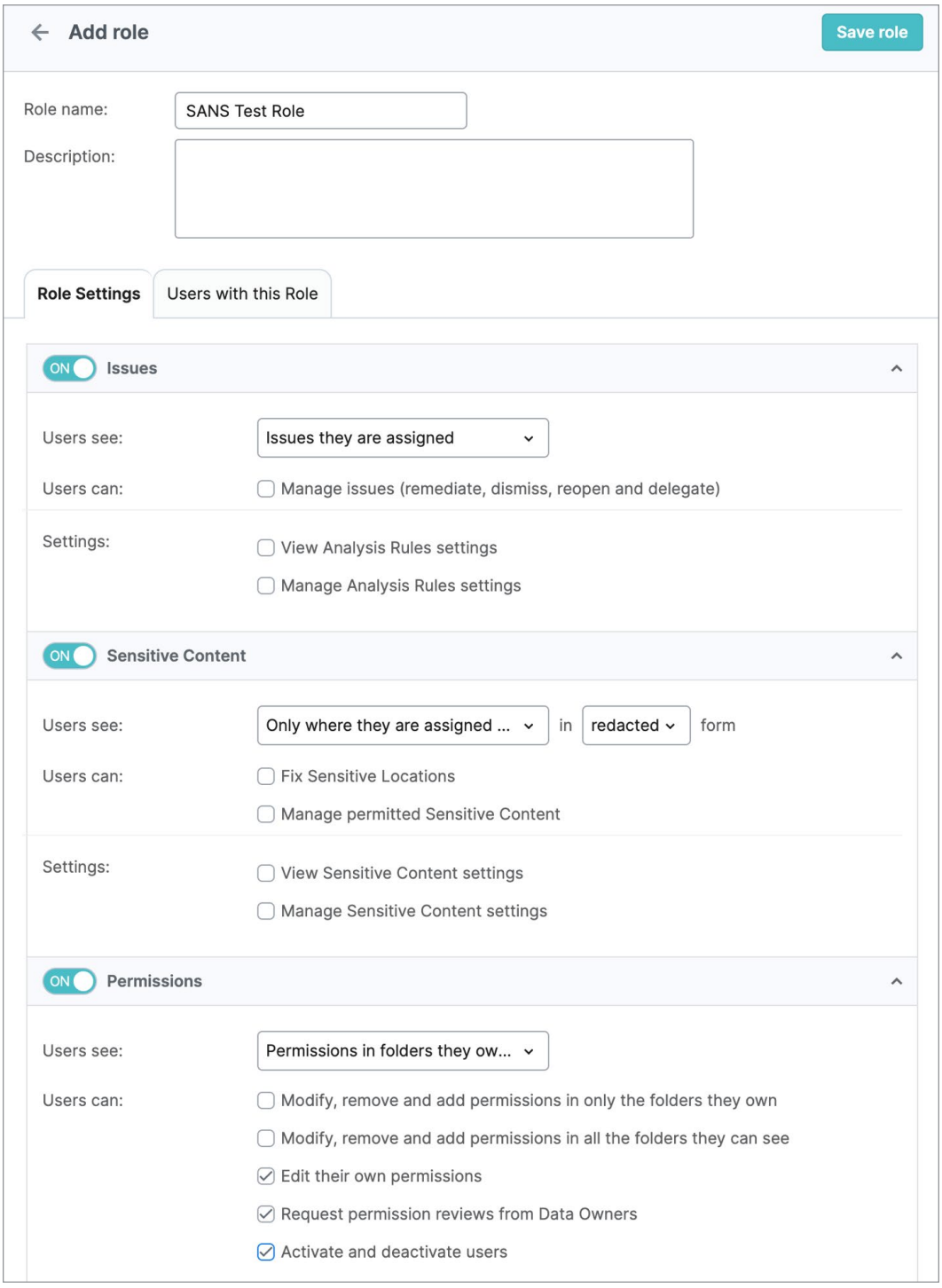


*Figure 10. Creating a Custom Role*

Egnyte also has a permissions dashboard that shows permissions for each folder, which can be used to request a review of folder permissions from a data owner. See Figure 11.

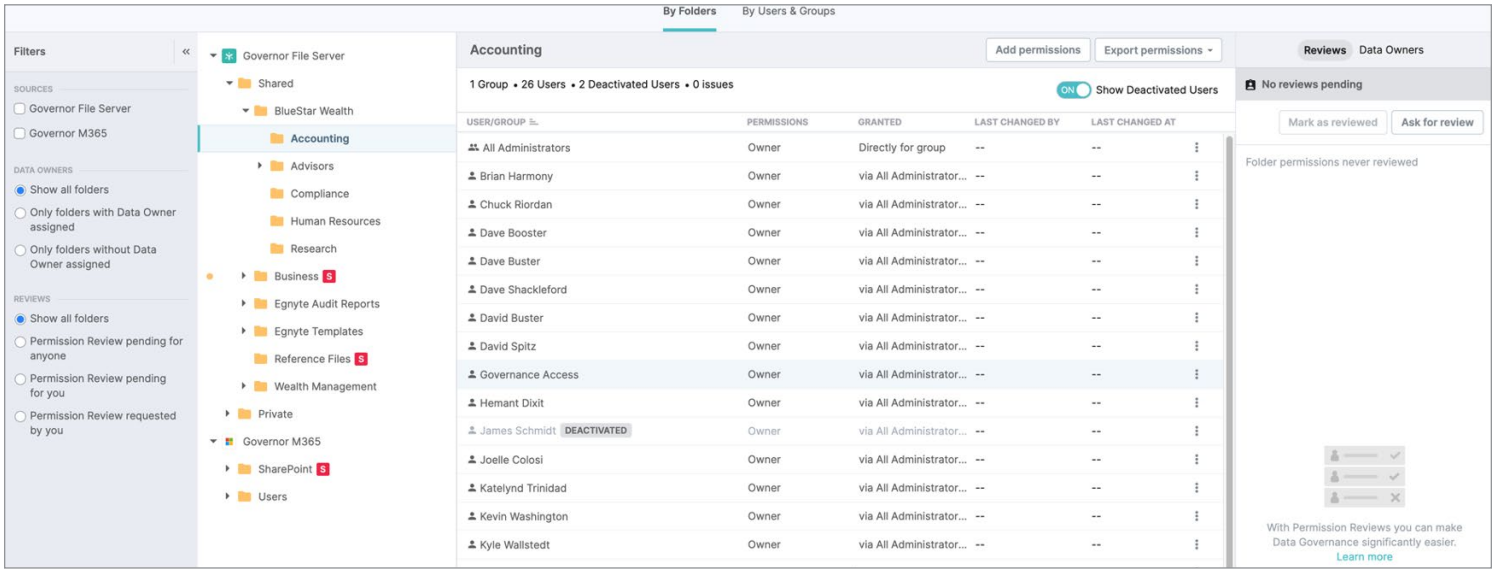


*Figure 11. Egnyte Permissions Dashboard with Review Request*

## Content Classification

Using its specialized ML and AI algorithms, Egnyte scans every word in every document to look for specific content that may fall under particular compliance and regulatory requirements (or even industry-specific requirements). Admins can enable specific built-in compliance policies, such as PCI DSS, GDPR, and the Virginia Consumer Data Protection Act (VCDPA) for data privacy; HIPAA for healthcare; or generic policies that look for secrets and encryption keys, which are used to mark and label documents and content as sensitive throughout the Egnyte ecosystem. By default, Egnyte constantly scans the entire repository and reads dozens of different types of documents, including word processing, spreadsheets, and PDFs. It even scans image files for text using optical character recognition (OCR). In addition, admins can create customized policies that include risk scoring and customized pattern matching, as shown in Figure 12.

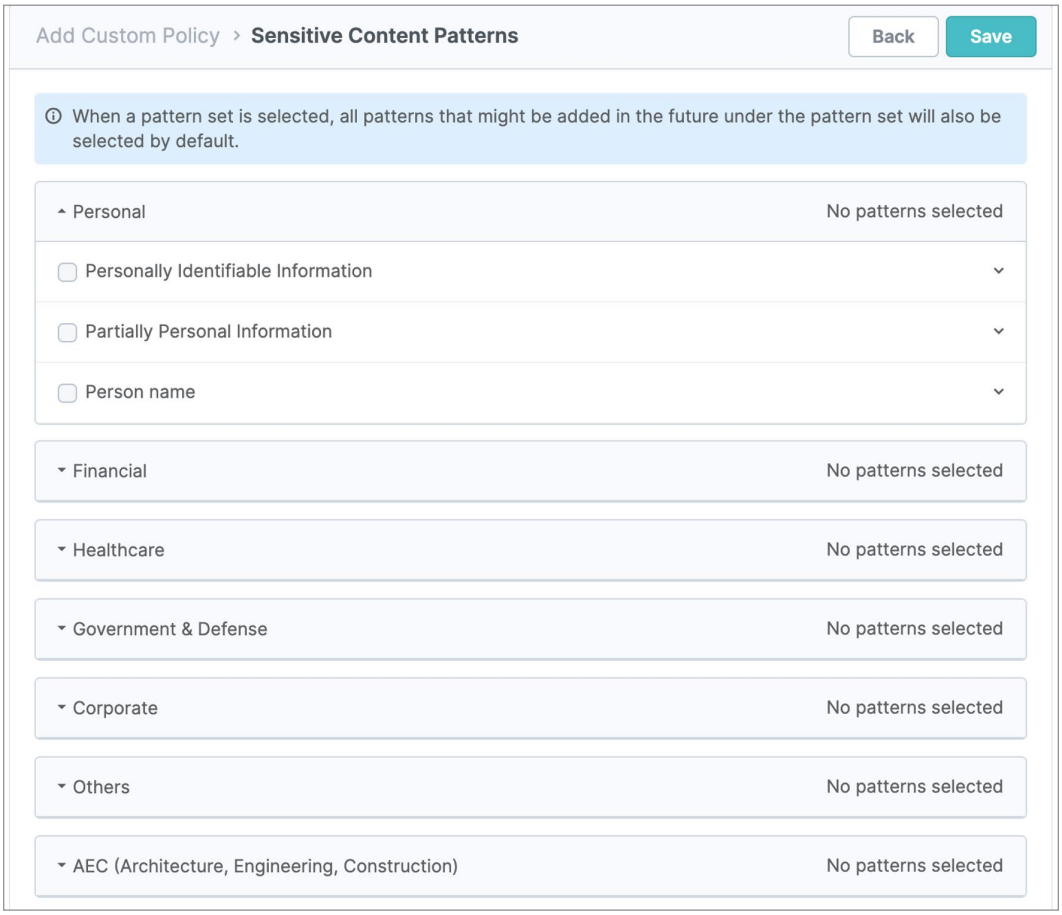


*Figure 12. Customizing a Content Classification Policy*

In addition, the Egnyte content policy engine allows for customized keyword lists and document classes. Keyword lists are just what you'd imagine: simple ASCII text words that should be discovered and possibly flagged in conjunction with sensitive data classifications. They are particularly useful for internal intellectual property and other non-standard keywords. In addition to detecting text that may be sensitive, Egnyte has been pre-configured to recognize dozens of document classes by format including contracts, resumes, offer letters, invoices, and many others. One of the more sophisticated capabilities we observed with Egnyte were the customized document classes. Admins can upload one (or several) "training documents" that possess desired characteristics to train the Egnyte AI model for monitoring and alerting. Ideally, Egnyte recommends uploading at least 20 documents to help train the model, and this feature can help organizations build highly customized content recognition patterns and document classification types. The "Sensitive Content" dashboard shown in Figure 13 shows all sensitive content that was discovered and labeled within the Egnyte platform.

Admins can choose to move and/or delete files based on the sensitive content and location.

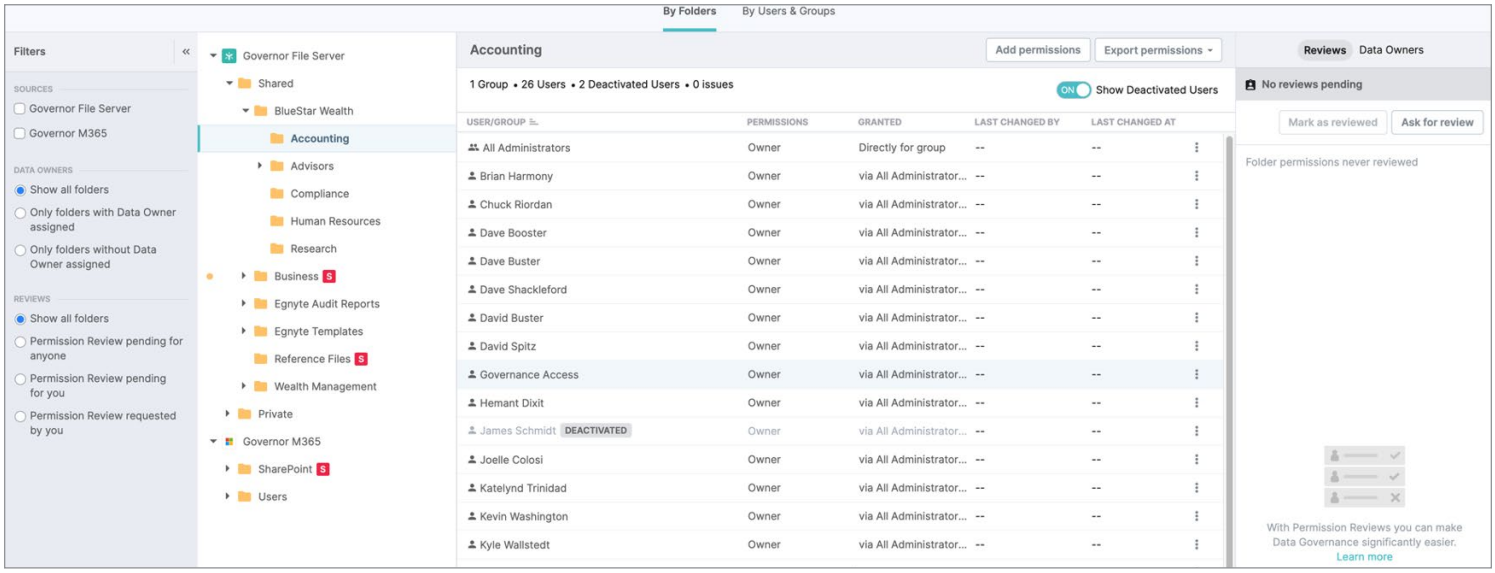


*Figure 13. Sensitive Content Dashboard*

## Content Safeguards

At the next level of sensitive data protection, Egnyte offers a variety of content safeguards. Here, admins can create a variety of granular restrictions that allow data access control and sharing based on data types, risk scores as determined by Egnyte AI, specific storage and sharing locations for the data, as well as specific individual and group sharing policies and expiration dates. See Figure 14.

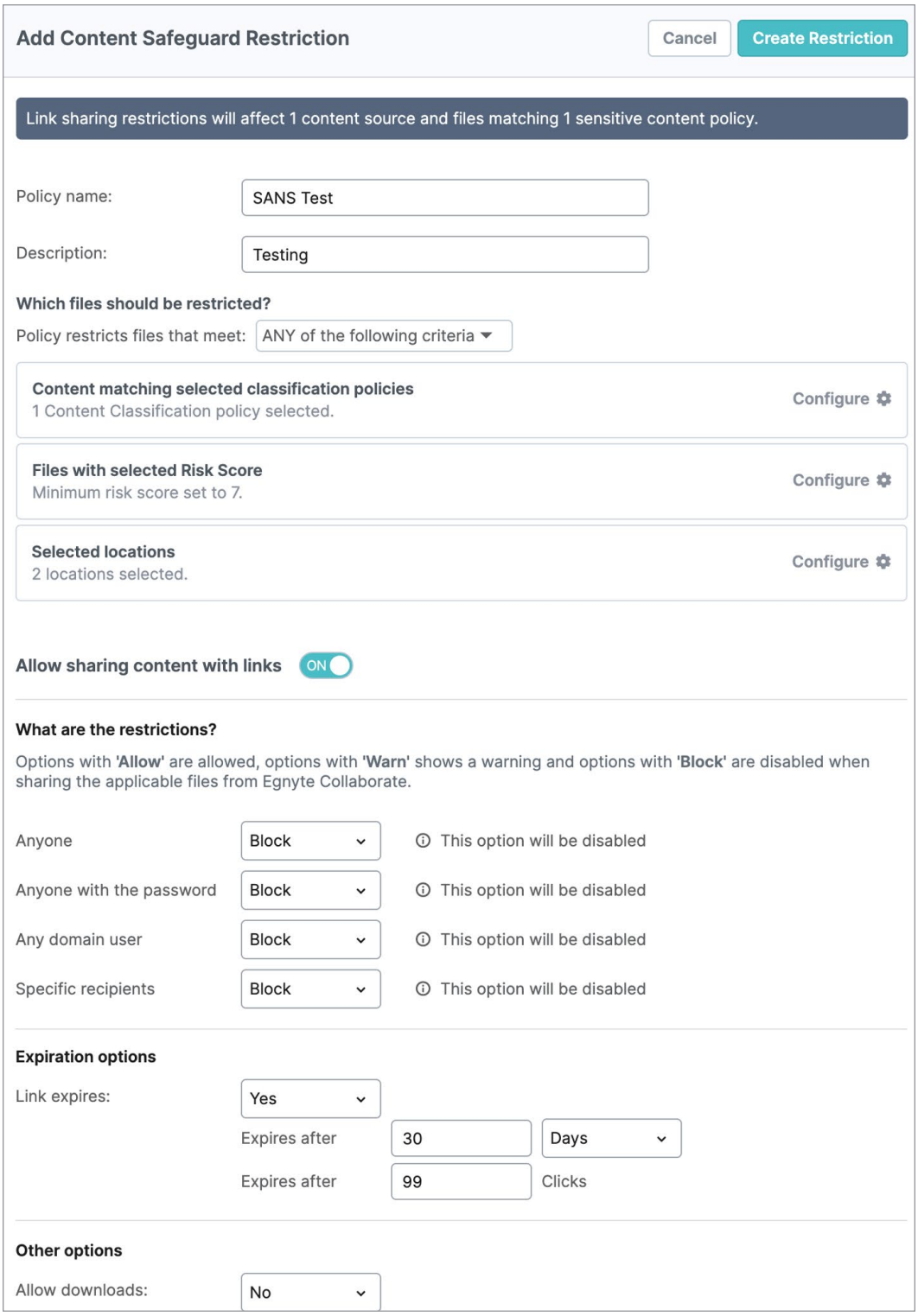


*Figure 14. Content Safeguard Restrictions*

As most organizations find, certain stakeholders and executives want (or need) exceptions, and Egnyte makes it easy to create them for content safeguards (see Figure 15).

Content safeguards make it easy for organizations to develop and implement large-scale content control policies they can apply across users, groups, storage locations, and more, with a means to exempt individual users, groups, and content on an as-needed basis.

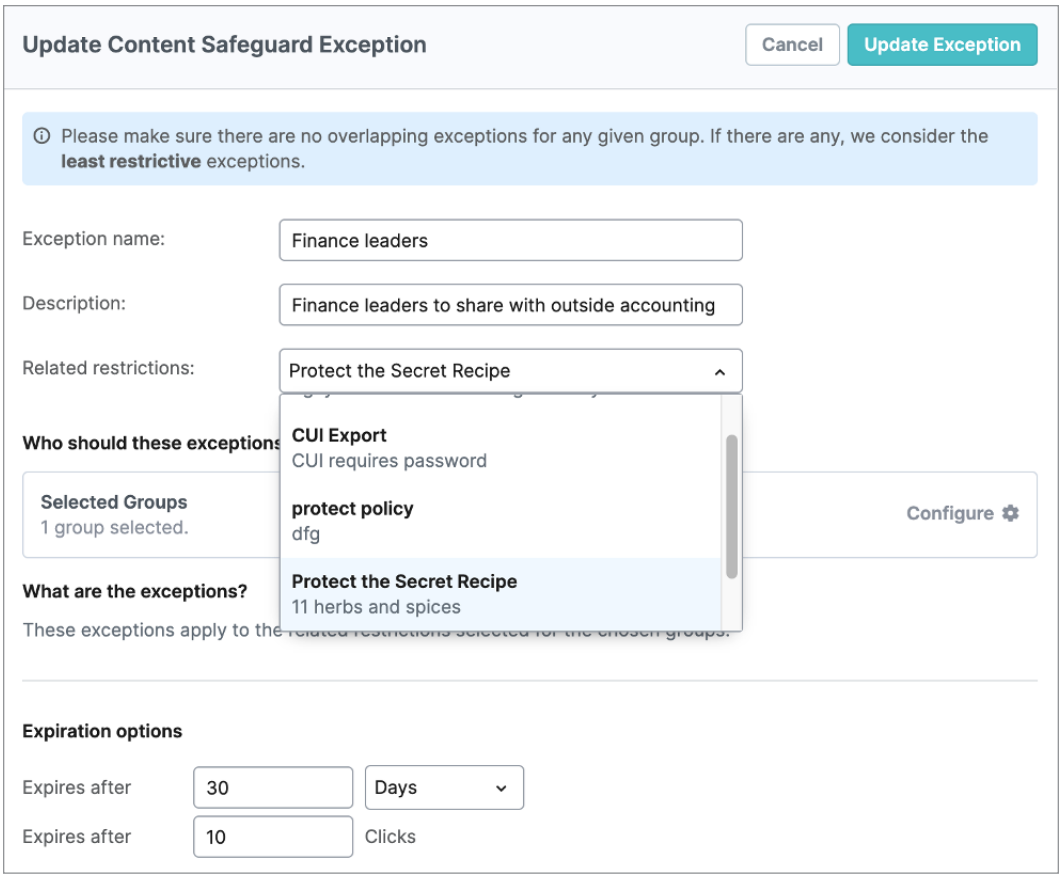


*Figure 15. Content Safeguard Exception*

# Content Life-Cycle Policies, Monitoring, and Alerting

Egnyte readily manages and monitors content life cycle within the platform and does so across numerous data storage locations and types. The policies you can create for document life-cycle control are flexible, with the ability to specify retention periods and archive destinations. They also have options to archive, move, or replicate data to specified locations. You can choose to delete data after a specified time in many storage environments. See Figure 16 for an example of a content life-cycle policy.

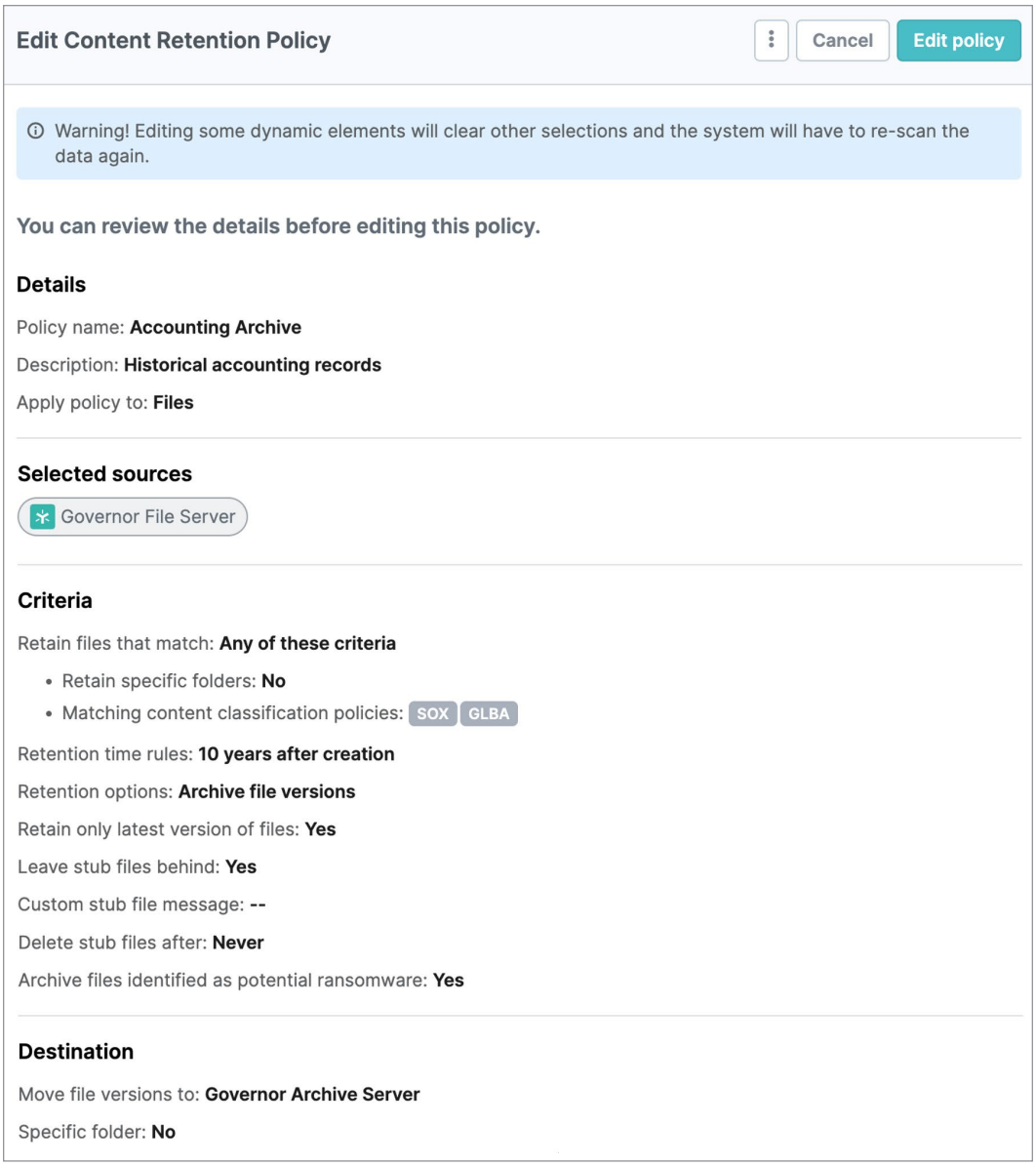


*Figure 16. Content Life-Cycle Policy*

To help discover and track documents (for content life-cycle and IT security policies), Egnyte supports document labeling that includes metadata, rule-based document labeling, and data tagging. These metadata labels are automatically applied to specified content types based on classification policies (data types and pattern matches or other attributes, as defined in security and AI policies). A simple document label we created that matches any payment card data is shown in Figure 17.

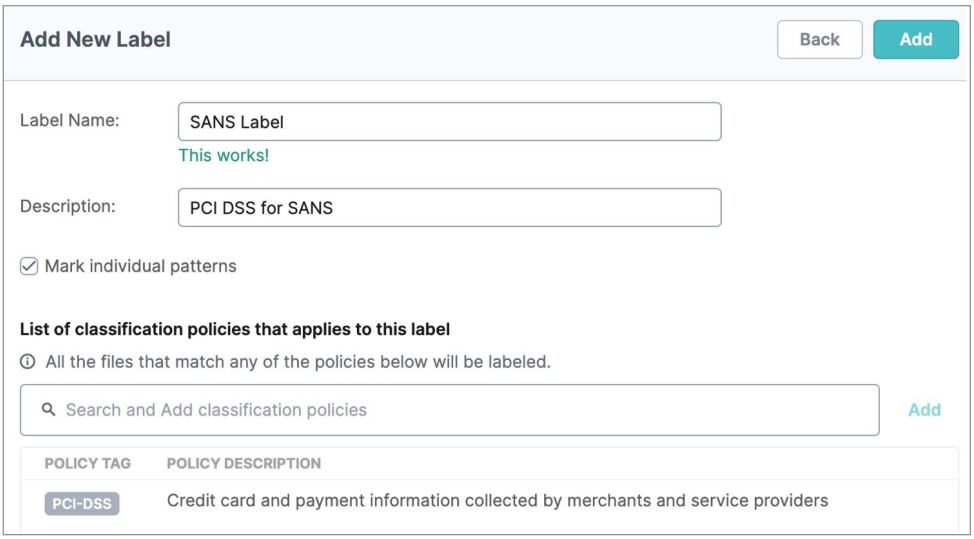


*Figure 17. A Sample Document Label*

Lastly, Egnyte has a comprehensive dashboard for monitoring, alerting, and reporting on content life-cycle policies and matches. This dashboard shows a wide range of data related to content locations and life-cycle policies, including file types and retention cycles/policies, the age of the data in that location, the changes in folder size over time, files by age and access times, and more. A wide array of filters is available, too, making searches for data parameters in large, complex storage accounts much simpler. See Figure 18.

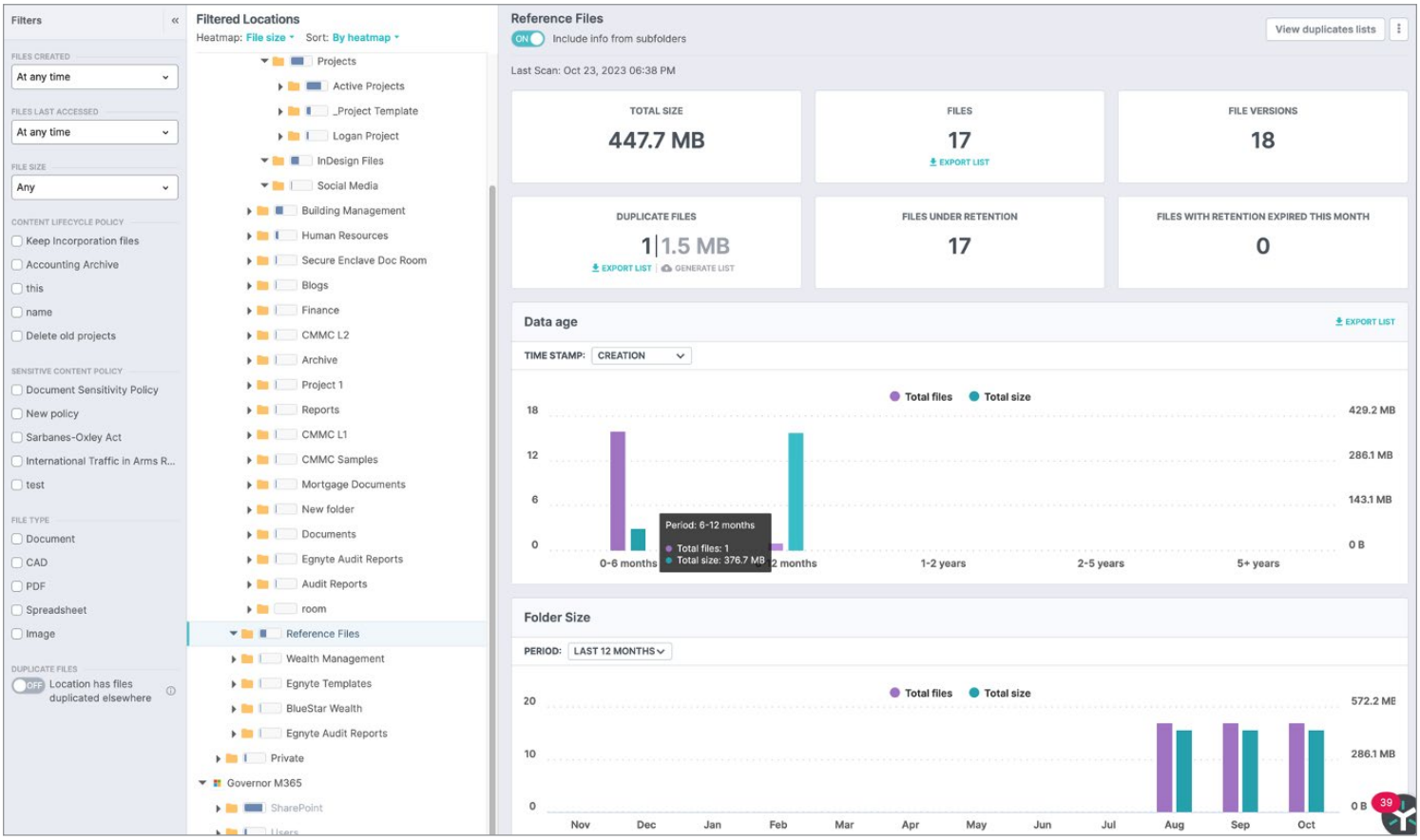


*Figure 18. Content Life-Cycle Dashboard*

Egnyte has a thorough data duplication analysis engine in place that can help admins highlight locations where duplicate data is stored. In larger organizations with a huge volume of content, this can help identify needless redundancy and overlap that could prove costly to maintain and reduce content sprawl and expensive storage requirements.

## Malware Protection and Recovery Features

Although mentioned in some earlier parts of this review, it's worth noting that Egnyte has a strong story around malware detection/isolation as well as data recovery in the case of ransomware events. Within the user context of Egnyte, any suspicious files and content that Egnyte believes may contain malware is now flagged in a "Potential Malware" menu item (and alerts are sent too). Maybe most importantly, users can restore snapshots of data easily on a rolling 30-day cycle, as shown in Figure 19.

This snapshot restoration can apply to individual files and folders or entire folder and file system structures.

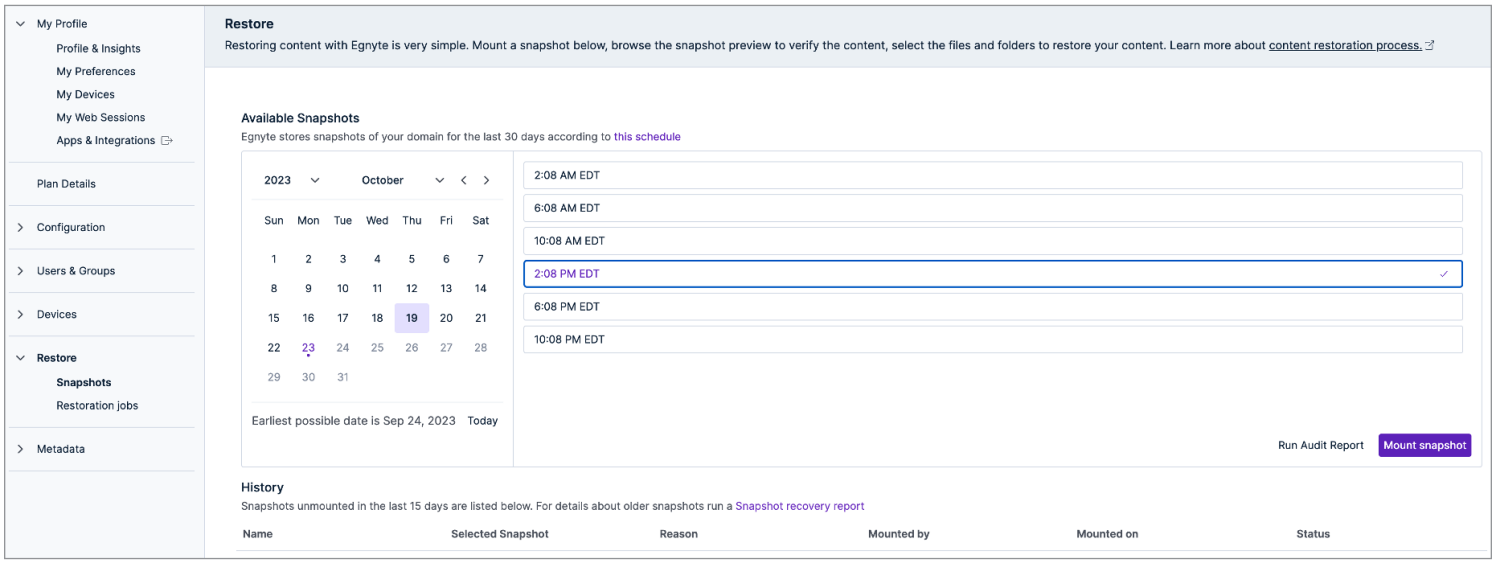


*Figure 19. Restoring Data Snapshots in Egnyte*

# Legal Holds

Egnyte supports a legal hold system that is remarkably simple to configure and maintain. Admins can designate particular data types and locations as well as users/groups involved. They can also declare an open-ended or finite time frame for the hold to be in place. New or existing cases can be referenced easily to keep workflow as streamlined as possible (see Figure 20).

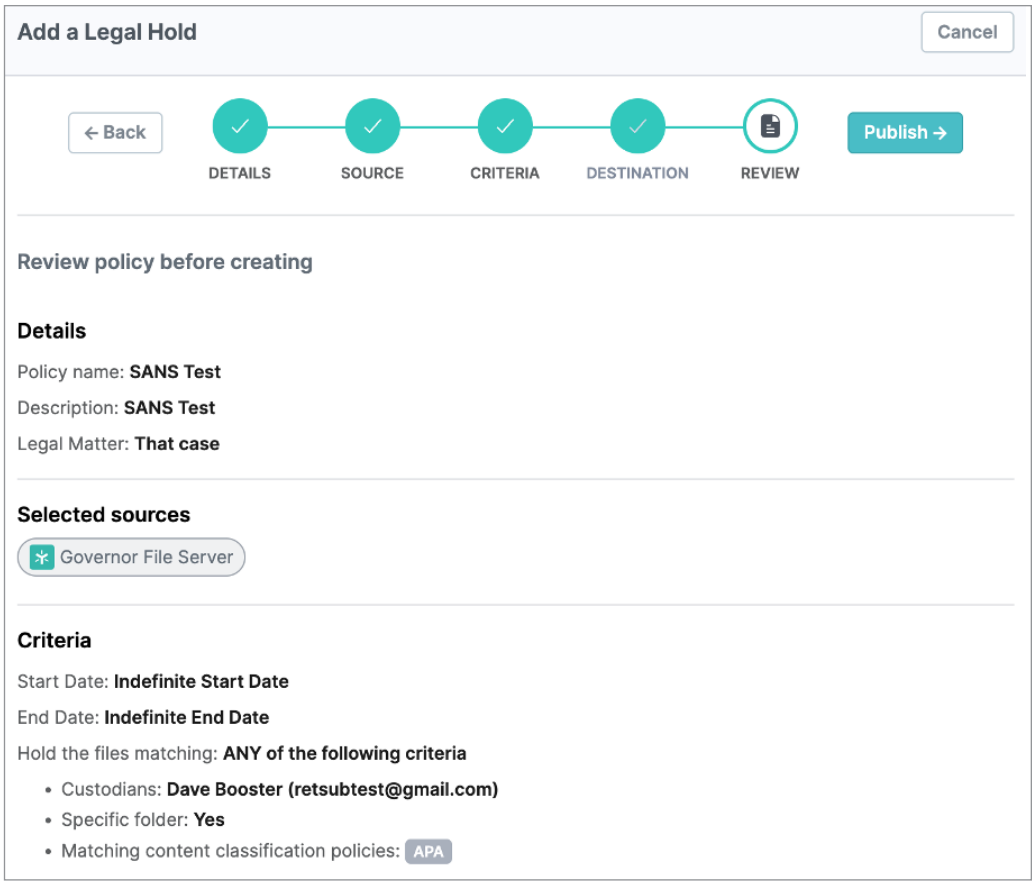


*Figure 20. A New Legal Hold Policy*

## Reporting (Audit Reports and Breach Reports, Different Menus)

Egnyte offers a range of capabilities to help organizations meet regulatory compliance requirements. First, along with the data classification and labeling capabilities that were referred to earlier, there are a range of different reports available that align with specific regulations. These include reports on folder permissions, user and group permissions, and a plethora of audit reports that include:

- File and folder inventory and structures
- Permissions and login activity reports
- User and group provisioning reports
- Configuration and snapshot recovery reports

## Conclusion

It's obvious that the team at Egnyte continues to innovate and look for ways to help organizations protect themselves and their data in the cloud. The company recently rolled out "Secure Data Enclave" offerings that enable organizations to register separate specific domains to accommodate highly sensitive document and data storage.

They include:

- A specialized EgnyteGov enclave that addresses clients' Cybersecurity Maturity Model Certification (CMMC 2.0) requirements.
- For non-US Department of Defense (DoD) use cases, Egnyte offers a separate secure enclave that's aligned with ISO 27001 certification requirements.
- Lastly, Egnyte Document Room enables organizations to create a highly isolated, controlled, and monitored storage location for them to collaborate on and share sensitive financial transaction data, merger and acquisition documentation, and private equity/venture capital fundraising details.

Although SANS did not review these solutions directly, they were fully available and adopted by customers at the time of this writing. They demonstrate that Egnyte is focused not only on helping organizations meet regulatory requirements, but also on improving the status of data security controls with simple, clean workflows and controls, across different industries.

Our review showed that the platform was not only highly accessible but also extraordinarily capable. In fact, we didn't see any gaps or deficiencies in this platform relative to storage, data classification and monitoring, life-cycle controls, and even retention and recovery. Organizations of all types and sizes could readily make use of Egnyte to store and protect their valuable data. With the wide range of pre-built policies and data classification elements available, an organization's entire file storage and management program could easily be set up and maintained within the Egnyte platform.

## Sponsor

**SANS would like to thank this paper's sponsor:**