SANS

Analyst Program

Product Review

Data First: Defending Your Organization from Within

Written by **Matt Bromiley**

September 2021

EGNYTE

Introduction

Let's consider security controls and defenses in one of two categories, classified by source and data flow: **outside-in** and **inside-out**. Many organizations invest considerable resources in the former, working to prevent adversaries from gaining a foothold in the environment. Perimeter defenses are structured to only allow certain traffic in and out, and endpoint defenses are configured to detect even the slightest execution of malicious code. Conversely, organizations appear to spend less time on internal defenses. Lateral network movement is seldom captured, and many organizations operate on the belief that if an account has access to something, it is trusted. Unfortunately, "trust" can introduce blind spots that require visibility.

As we have seen repeatedly, however, these approaches fail to completely secure our enterprises. Adversaries and malicious documents continue to find a way in, attacks like ransomware have never been more successful, and sensitive data still leaves the environment. Perhaps it is time to ask ourselves the proverbial "Is this thing still working?" Do we need to focus our efforts elsewhere? Is our data truly secure, or have we just avoided an attack thus far? We must also consider the obvious: When an attacker gains access to an environment, whether it is a ransomware or espionage attack, how do we protect our most valuable assets from theft or extortion?

When an attacker gains access to an environment, whether it is a ransomware or espionage attack, how do we protect our most valuable assets from theft or extortion?

In this product review, we examine a platform that addresses these concerns and more: Egnyte. Realizing that an organization's data is critical to continuous operations, Egnyte has created a robust platform that offers extremely granular governance and security controls. Combining data security with collaboration and cloud integration, Egnyte gives organizations new capabilities to secure their data, and subsequently their organization.

Some of our key takeaways from working with Egnyte's platform included:

- Granular insight into risks surrounding sensitive enterprise content
- A wide range of detections for data security issues, including public links, incorrect permissions, and external sharing
- Ransomware detection and data protection via granular analysis and monitoring of data changes
- Security and governance controls across a wide range of file storage systems beyond Egnyte, including OneDrive, Amazon S3, email repositories, Google Drive/Cloud, and Azure Cloud, among many others.

As you read this review, we encourage you to consider the following:

- What are you doing to secure your data and various data repositories?
- How much visibility do you have at the perimeter vs. your own data?
- Is your security program structured around external threats trying to break in?
- Does your security team (if you have one) keep an eye on the data that employees use, to ensure that malicious files are not uploaded to, or sensitive data is not removed from, the environment? If so, how?

If you answered yes to the last question or are confident in your ability to manage your own data, we encourage you to compare Egnyte's capabilities with your own. How easy is it to use? How quickly can an analyst go from alert to remediation? These metrics, and more that we will discuss, are critical to evaluating your current data security capabilities.

While much of our review leans toward Egnyte augmenting a security team, it is not strictly a security product. Even organizations with a minimal security team have data to protect and will find value in a data security platform such as Egnyte. Egnyte's platform is simple to spin up and link to your data, allowing for a rapid security implementation with little effort and overhead.

Hands on with Egnyte

Many may already be familiar with Egnyte as a storage solution. In fact, as shown in Figure 1, the default screen for many users is exactly that—a storage solution.

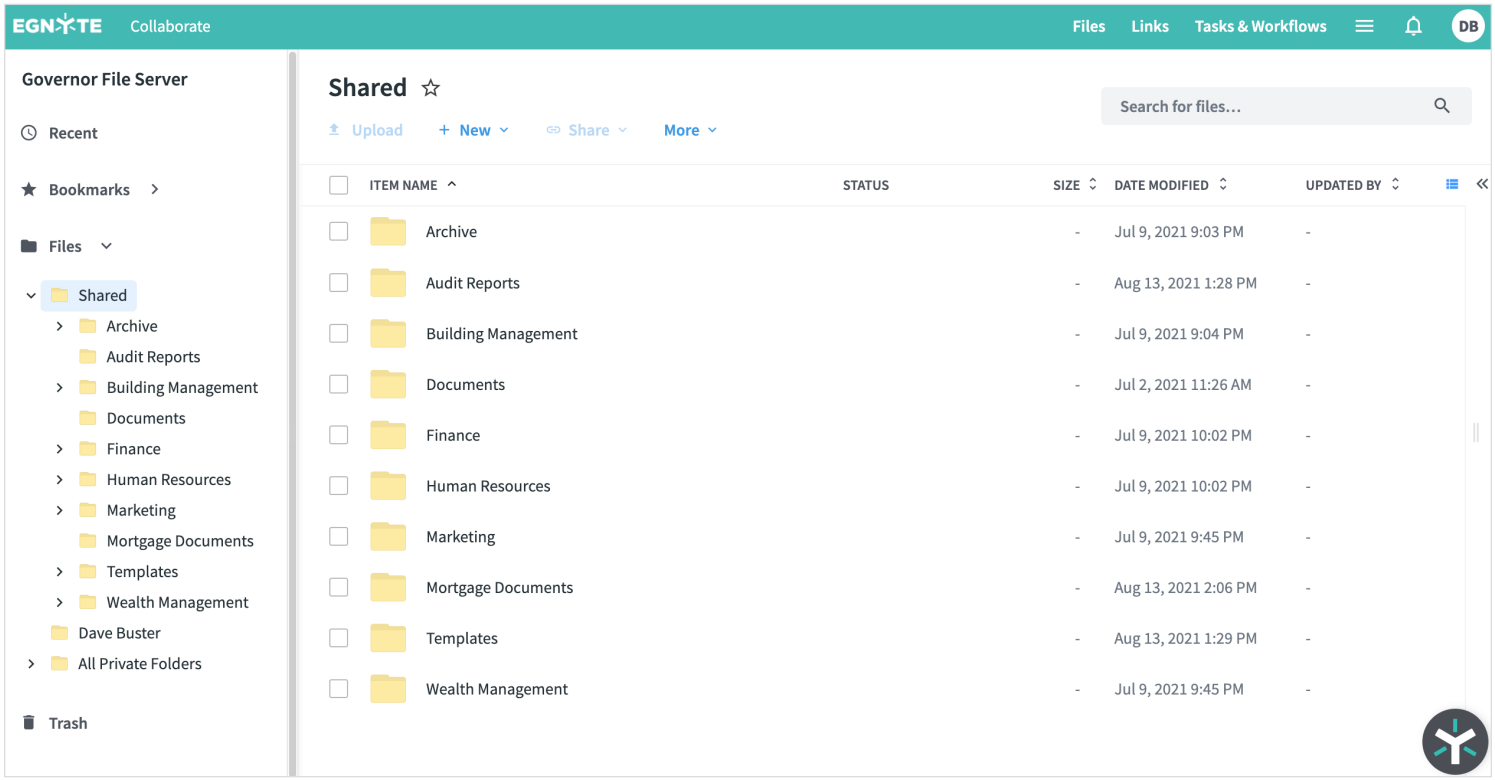

Figure 1. Snippet of Egnyte's Collaborate Dashboard

We quickly realized, and are happy to share, that **Egnyte's platform is so much more than simple data storage**. Other platforms offer to hook in and secure data repositories but are not themselves storage mechanisms. While not the primary focus of this paper, we think the fact that Egnyte understands storage so well gives it a unique vantage point in helping organizations maintain and secure their data.

Much more than data storage, Egnyte's platform offers incredible insight, governance, and reporting on the data that is critical to your organization (such as IP or sensitive employee information). While much of our review will focus on Egnyte as a platform, it is important to note that Egnyte also integrates with other storage providers.

With the correct privileges, analysts and administrators can select the Secure & Govern tab and be transported to an informative, well-structured dashboard that provides insight into your data operations. See Figure 2 for a snippet of the Risk Summary dashboard.

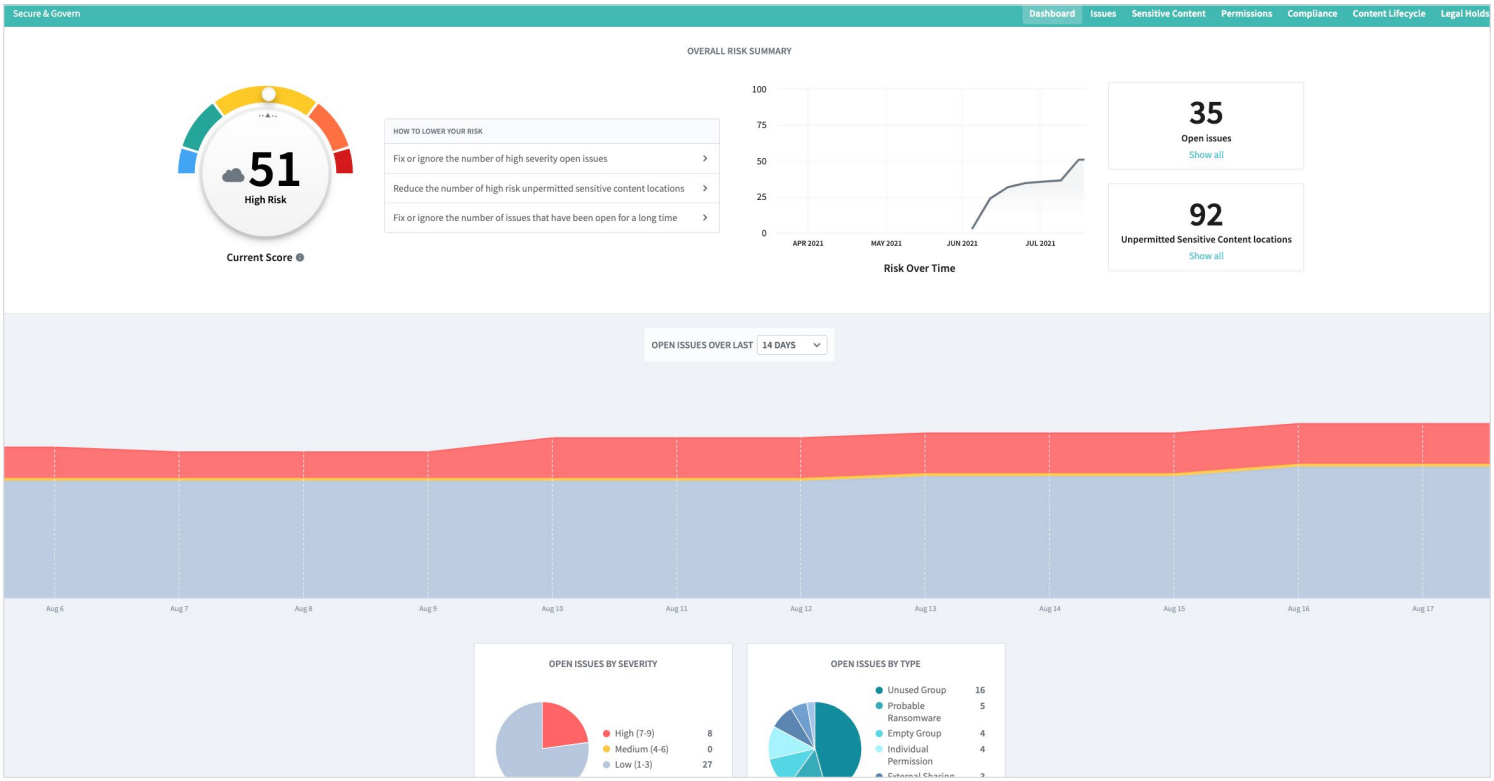

Figure 2. Snippet of Egnyte's Risk Summary Dashboard

We were pleased to see that the dashboard shown in Figure 2 provides a crisp snapshot of the current state of our data security. An overall risk score—based on various factors determined by Egnyte, the state of our data, and other issues—provides an up-front "How good or bad is it?" score that we think stakeholders and information security managers will appreciate.

Continuing through the dashboard, Egnyte provides high-level statistics that yield valuable data for security analysts, such as open issues and unpermitted sensitive content locations. As we integrate data security into a security program, the question "What should we do now?" is one that analysts ask often. Egnyte delivers on that question up front and makes it easy for analysts to determine where they need to focus efforts and tasks next.

Another feature of the main dashboard that we enjoyed was advice on "How to Lower Your Risk." A snippet of this section is provided in Figure 3.

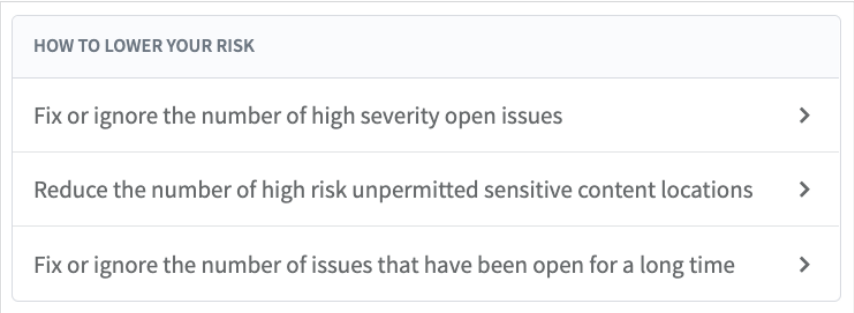

Figure 3. Snippet of the "How to Lower Your Risk" Information Box from the Risk Summary Dashboard

Each risk-lowering recommendation is also interactive, meaning analysts can click and be taken immediately to areas of the organization that require remediation. We love this feature! One pathway we always look for in security products is how quickly analysts can go from problem to solution, and Egnyte gets them there quickly. We will explore one of these risk-lowering options shortly.

Continuing through the main dashboard, the Egnyte platform also keeps track of currently open issues and the organization's risk profile over time. Figure 4 zooms in on the high-level statistics of open issues.

Each risk-lowering recommendation is also interactive, meaning analysts can click and be taken immediately to areas of the organization that require remediation.

As seen in Figure 4, Egnyte provides key data points about issues in the environment that allow for analyst prioritization. Our test environment includes six open high issues, which we might want analysts to tackle first. Conversely, we also might focus our efforts based on the type of open issue. It could easily be argued that "Probable Ransomware" presents a higher risk than "External Sharing," but we'd need to explore the data content to evaluate each correctly.

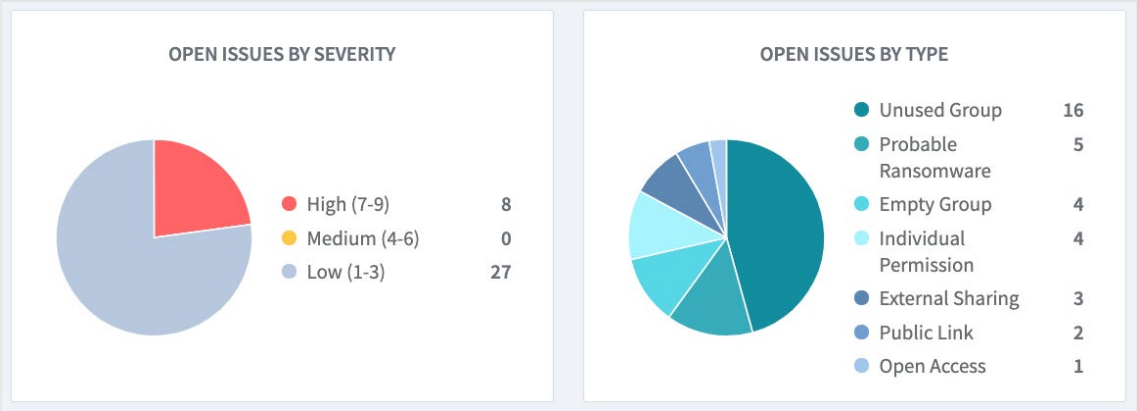

Figure 4. Snippet from Egnyte's Risk Summary Dashboard

This initial dashboard is where the Egnyte platform (correctly) forces you to consider your data security practices differently. Each text, issue, and dashboard panel are interactive, allowing analysts to follow breadcrumbs immediately. Even the types of issues shown in Figure 4 give us a new perspective on our data: "What is public facing or what has been shared outside of the environment?" "Are user permissions correct, and is there any data impact that might alert me to an ongoing incident?"

Note that we can make this assessment based on the state of our data. Egnyte is not deploying endpoint agents or tapping into PCAPs across the wire. Instead, with an understanding of what data and users *should* and *should not* do, we get extremely granular and welcome insight into our organization's data security. We appreciated that this depth of insight was provided without the need for an agent or a traffic monitoring device. This feature allows Egnyte to easily run parallel to other security solutions, providing robust detection and response capabilities.

Egnyte's platform offers unique visibility into data security but does so without intruding on other security controls. This allows it to be deployed and run parallel to other security controls, which means you can add data security to your current security tooling or build from the ground up with data security and governance at the forefront.

Responding to Issues with Egnyte

Responding to open and ongoing issues is where security teams will likely spend most of their time. Solving issues and remediating the environment are top priorities, and Egnyte rises to the occasion to assist analysts in these tasks. Figure 5 provides a snippet of the Issues dashboard.

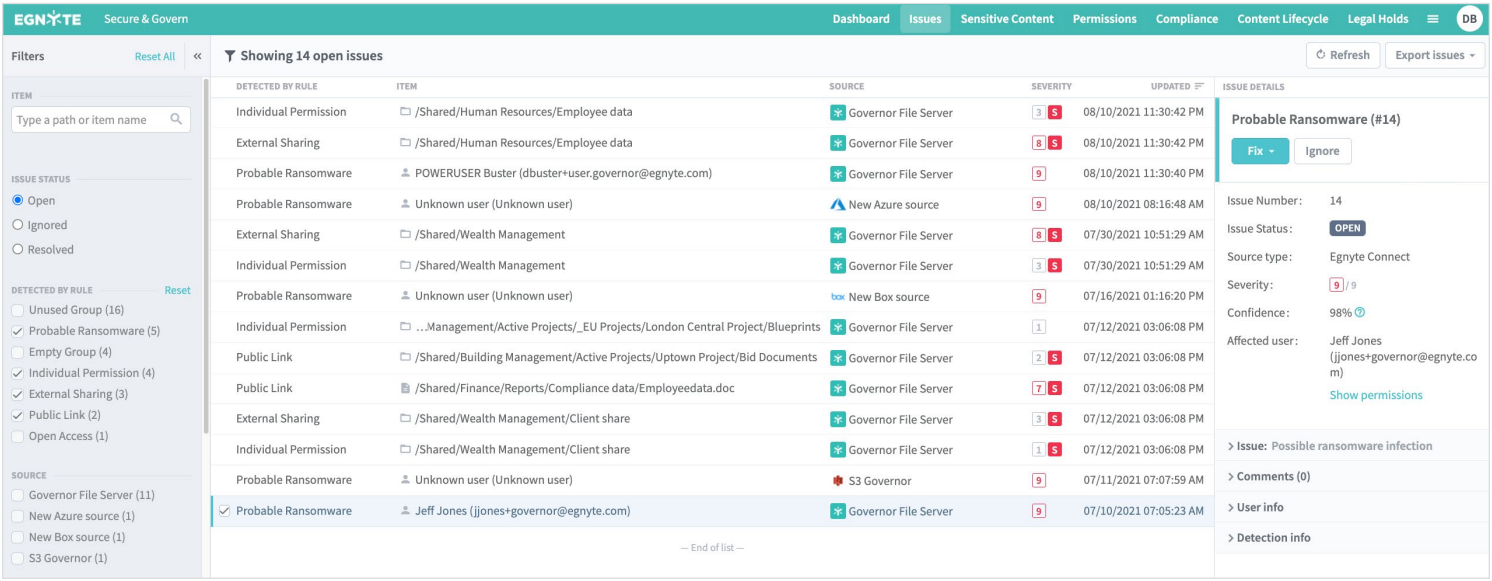

Figure 5. Snippet of the Issues Dashboard

As seen in Figure 5, Egnyte's Issues dashboard is packed with invaluable data for security analysts. Immediately we can see:

- The rule that triggered
- The item that triggered the rule
- The source of data
- The severity of the issue
- Time frame(s) relevant to the issues

When analysts are presented relevant data up front, they can make decisions faster and with more confidence. For example, as seen in Figure 5, the Probable Ransomware issues display the highest severities, while External Sharing and Public Links are rated lower (although not too much lower). Let's examine one of the Probable Ransomware alerts in detail.

As shown in Figure 5, we have Probable Ransomware issues on four different platforms:

- Azure
- Box
- S3
- Egnyte File Server

First, let's point out the obvious: These are multiple storage providers. A single organization using just two, let alone four, of these various storage providers is not uncommon. The Egnyte team realized just how pervasive the use of multiple storage platforms is and ensured that they could offer the same type of detection across platforms.

We won't touch upon multiplatform integration every time we see it, but throughout this product review, you will commonly see multiple providers in various screenshots. This diversity is an important attribute of the Egnyte platform. Egnyte provides organizations a way to unite their storage providers under *one detection and response platform*. We know from experience that even *identifying and classifying* an organization's various sources is one task no security team wants to undertake. With Egnyte, it's integrated seamlessly.

Continuing with our examination of a Probable Ransomware issue, on the initial dashboard, Egnyte provides an Issue Details tab that provides even more relevant data points. See Figure 6.

We can easily see what triggered this issue. Via file inspection and integrity monitoring, the Egnyte platform identified a folder with "ransom note" files inside. Analysts are also provided:

- The offending user account
- The issue status
- The platform's confidence in its assessment
- Permissions associated with the user

We also are provided path details, such as the name of the file/ransomware and the top-level folders. Scrolling down further (yes, there's more data!), Egnyte provides additional data points on the user account, the permissions, and the source system, among others. We also can export a list of affected files directly from the platform (not shown in the screenshot).

If you looked carefully at Figure 6, you also might have seen a highlighted Fix button. Utilizing this button (see Figure 7) provides the security team with an opportunity to disable the user account and immediately prevent any additional access to the affected file server.

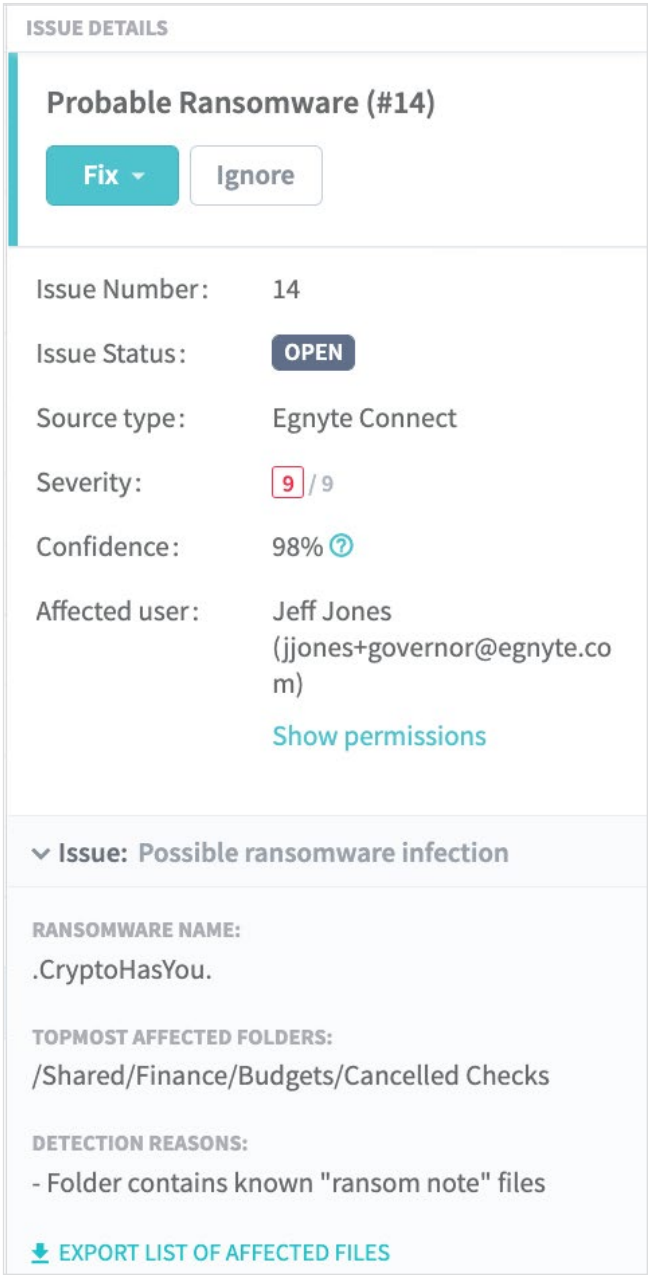

Figure 6. Snippet of Issue Details from the Issues Dashboard for a Probable Ransomware Event

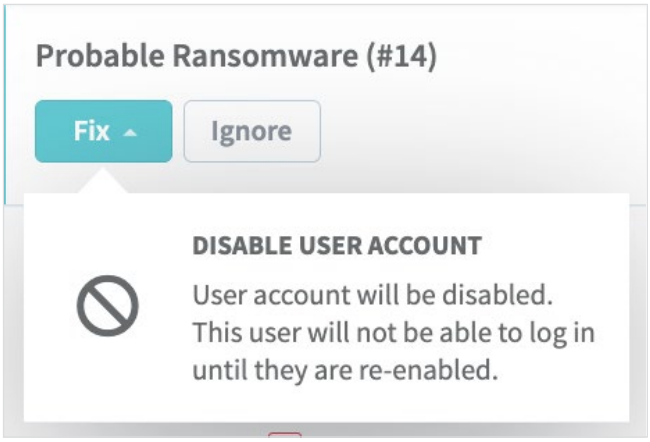

Figure 7. Snippet of the Fix Button from an Open Issue

This integrated feature presents an enormous advantage for security teams. Without detailed data security, if a ransomware attack is detected, security teams often must scramble to identify users, the source of the attack, how the attacker is moving around the network, root cause analysis, and more. With the Egnyte platform, we get to the heart of the ransomware attack: An attacker has stolen and is abusing credentials to move throughout the environment and encrypt files. Perhaps one of the best immediate reactions the team can make is to cut off that user's access in hopes of preventing additional damage.

Let's pause here to think about the technical requirements of such a request. Without a centralized data security platform, what are your current procedures for performing such a containment activity? How long would it take your security team to identify and cut off access for a particular account, if not multiple accounts? Furthermore, how quickly could your team scale that containment activity across multiple storage platforms?

In such a simple alert, we see the true power of a platform like Egnyte rise to the surface. With a centralized data security platform, we get immediate insight across *multiple* storage solutions. Plus, analysts can quickly detect and respond to incidents across the same pool of storage solutions. Integrated features like the one we just walked through are an immediate force multiplier for security teams. What may have taken hours or days to discover is identified immediately by the platform. We are always a fan of tools that make analysts' lives easier, but we are especially a fan of ones that simultaneously protect organizations.

The containment and/or remediation features are currently not available in all integrated platforms. However, that does not mean that non-Egnyte storage solutions suffer a lack of visibility or monitoring. Quite the opposite. See Figure 8, which highlights an alert of probable ransomware from a Box account. Although the Fix button is not available, analysts are still provided the same granular details, such as topmost affected folders, the reason(s) for the detection, and ransomware details (if available).

Our review of the non-ransomware issues was similar. Issue after issue, Egnyte provides useful, one-click options for analysts to quickly triage and contain an active incident. Whether it is cutting off permissions or removing an external-facing link, the multiplatform detection and response capabilities add an incredible tool to any security team's arsenal.

Egnyte's ransomware capabilities don't stop at detection and alerting. Egnyte's platform also provides recovery and remediation options, including *rolling back encrypted files*, despite an attacker's best attempts to render them unusable. What does that mean for you? According to Egnyte, no customer has paid a ransom or suffered long-term impacts of a ransomware infection.

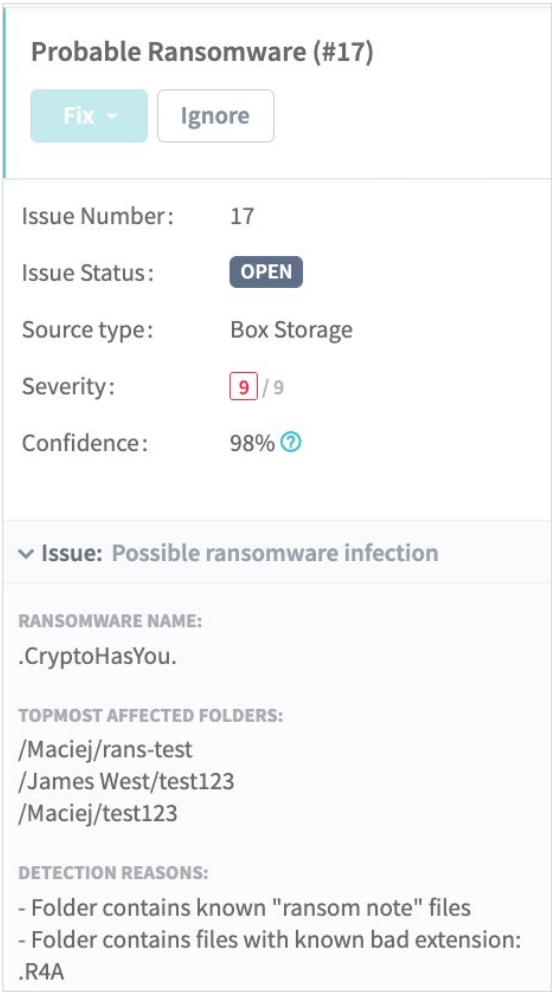

Figure 8. Alert of Probable Ransomware from a Box Account

Handling Data, Day to Day

With such deep insight in data security and storage solutions, Egnyte does more than provide alerting and detection when something goes wrong. It is also an extremely powerful tool for governance and for ensuring that your organization is handling data correctly. Also within the platform is Egnyte's "Sensitive Content" feature, as shown in Figure 9.

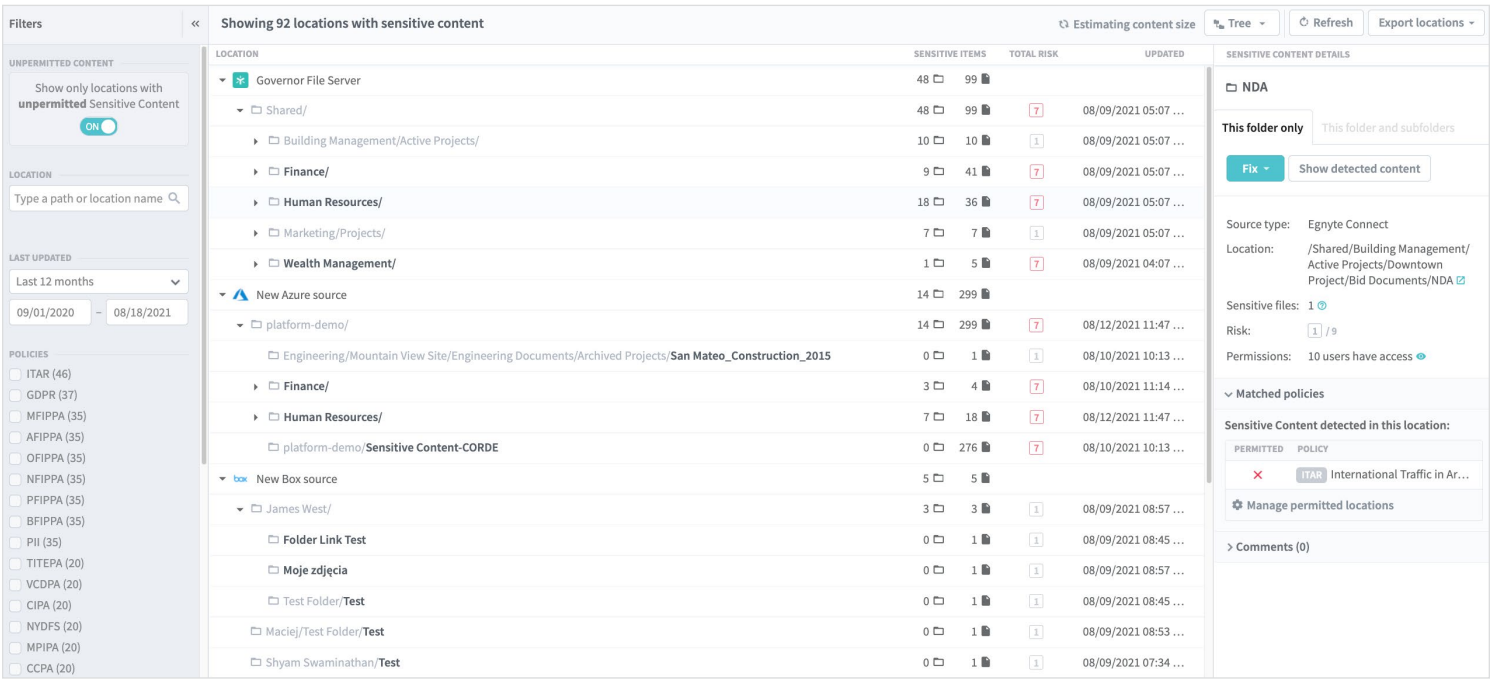

Figure 9. Snippet of the Sensitive Content Dashboard

As seen in Figure 9, Egnyte also will scan content and identify locations with "Sensitive Content." While not as critical or immediate as a "Probable Ransomware" event, monitoring sensitive data within an environment is perhaps a better representation of daily security activities. Again, the Egnyte Platform rises to the occasion and provides an excellent interface for data governance.

Figure 9 points out 92 locations with sensitive content within our environment. Like the detections we analyzed earlier, multiple storage solutions are involved: Egnyte File Server(s), S3 buckets, Azure data sources, and others. We also can see the various policies that Egnyte has configured, out of the box, to scan for and protect within enterprises. Figure 10 provides a zoomed-in snippet of some of the policies listed within Egnyte.

It should come as no surprise that this is the one feature that Egnyte gets the most feedback on from its customers: its ability to classify and protect various types of data within the organization at the click of a button. And this is to be expected. With the various rules and regulations that organizations must adhere to, it can be quite cumbersome to keep on top of all the data requirements.

Figure 10. Zoomed-in Snippet of Some Egnyte Policies

Furthermore, security teams cannot possibly be expected to defend the environment *and* stay current on the latest regulatory requirements. Egnyte abstracts this away, and with a single click of a button, an organization can reveal sources and data within that may violate certain regulations. Figure 11 provides a screenshot of the Sensitive Content dashboard, focused on GDPR.

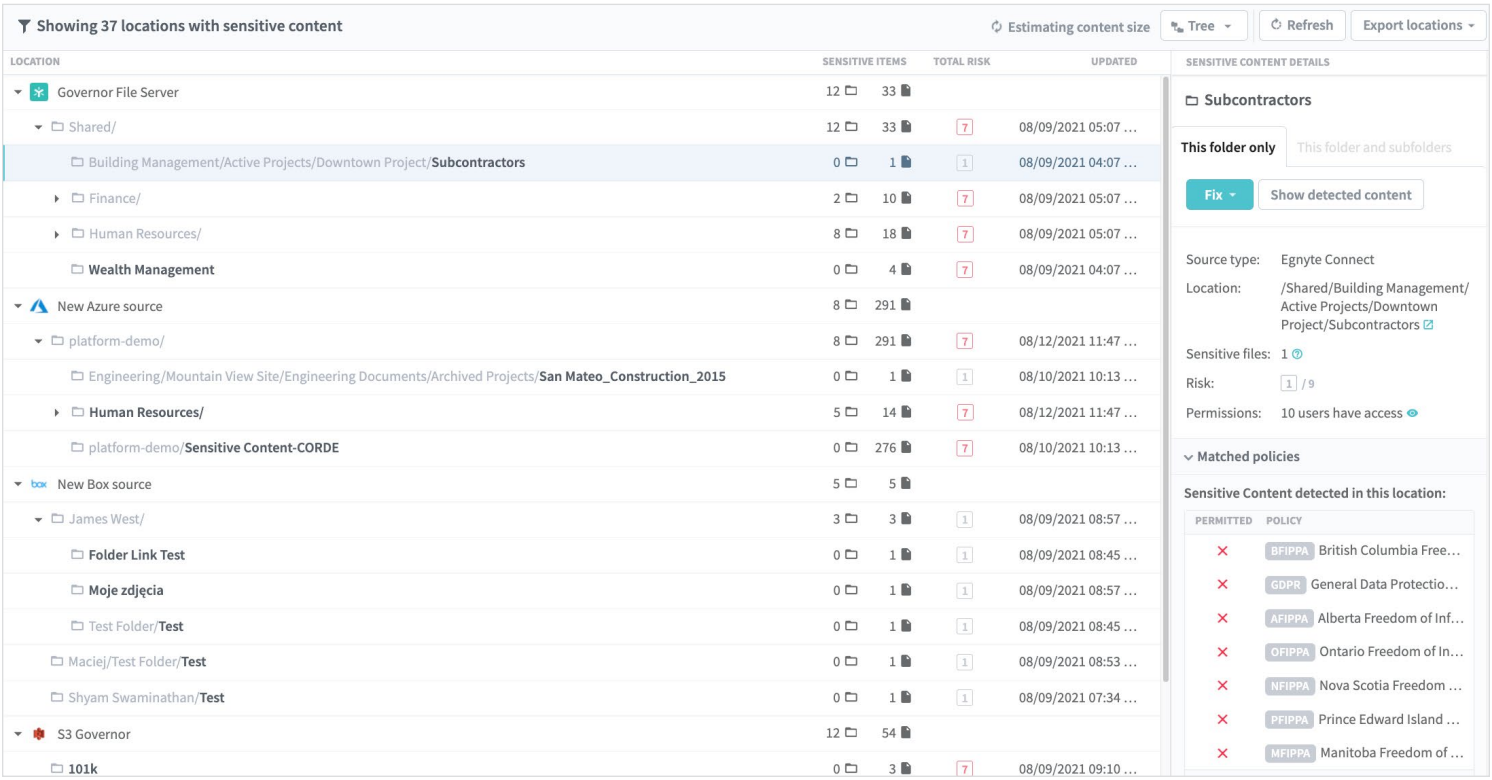

Figure 11. Snippet of the Sensitive Content Dashboard, Filtered for GDPR-Regulated Data

Figure 11 shows that it is very easy for data governance teams to access the platform and get *immediate insight* into the various classifications of data within their environment. We could continue to walk through various data types, but each example is the same: Egnyte makes this process unbelievably simple and easy to use. Also, you may have noticed above that the Fix button is available for sensitive content issues. Figure 12 provides a snippet of the Fix option with respect to sensitive content.

As seen in Figure 12, admins can move files to another location or delete sensitive files—all from the platform. We have already shown how easy Egnyte makes sensitive content *discovery*. It should come as no surprise that *remediation* and *enforcement* are equally easily accessible.

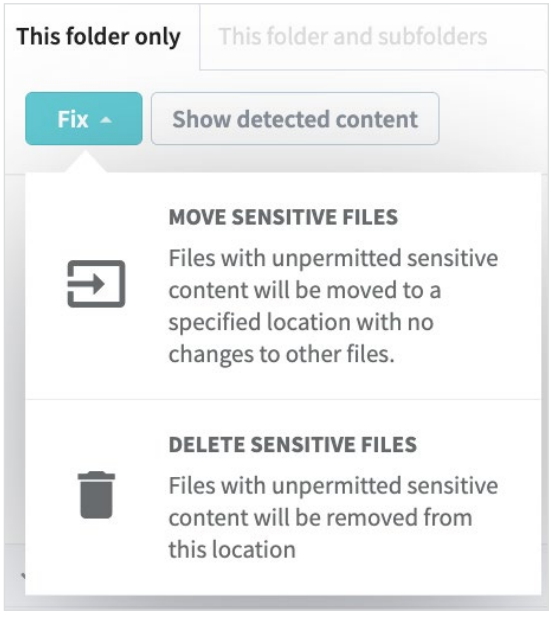

Figure 12. Snippet of the Fix Option with Respect to Sensitive Content

It can feel like an impossible task to keep up on data governance requirements and exposure within your environment. Even the smallest slip can result in fines or regulatory pressures. Egnyte abstracts these pressures away, making it easy for your team to quickly view data sources and potentially sensitive data within the environment, and fix issues immediately.

Content Lifecycle

Another impressive feature within the Egnyte platform—again, looking at the organization from a high, storage-focused level—is its Content Lifecycle feature. Figure 13 provides a screenshot of the Content Lifecycle Dashboard for the Egnyte file server in our test instance.

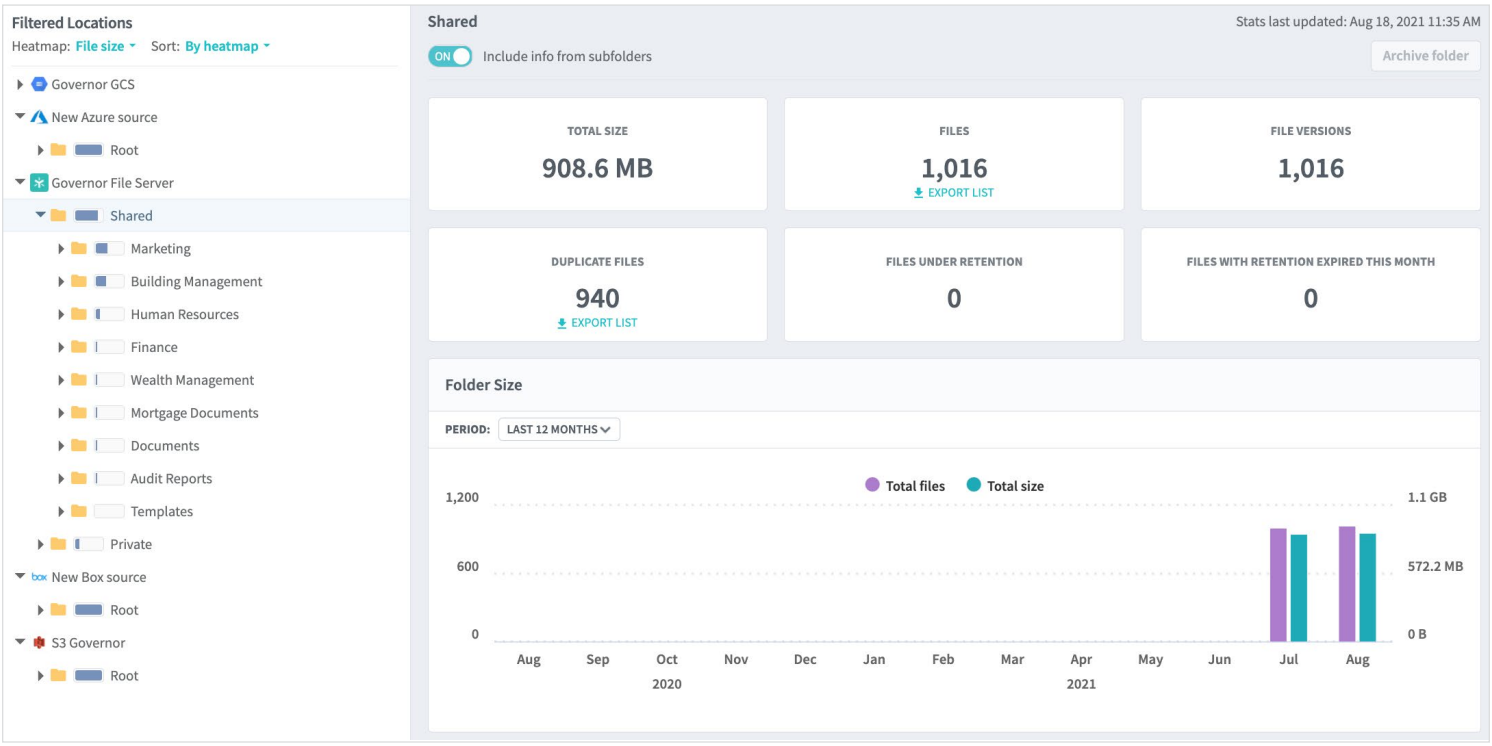

Figure 13. Snippet of the Content Lifecycle Dashboard

This feature continues to display Egnyte's ability to provide insight into an organization's data. Notice that within the Content Lifecycle, we can examine the total size of a file server, navigate through various objects, explore files, extract a list, and identify duplicates, among other tasks. Statistics include relevant storage metrics and overall file age.

Within the Egnyte platform, customers also can structure automated content lifecycle policies to assist in data retention, archiving, and deletion. In addition to the granular insights we have observed thus far, content lifecycle policies are yet another feature that gives an organization immense *control* over its data.

Legal Holds

Perhaps one of the more necessary features when it comes to data security is Egnyte's built-in capability to handle legal holds. Figure 14 provides a screenshot of the Legal Hold options.

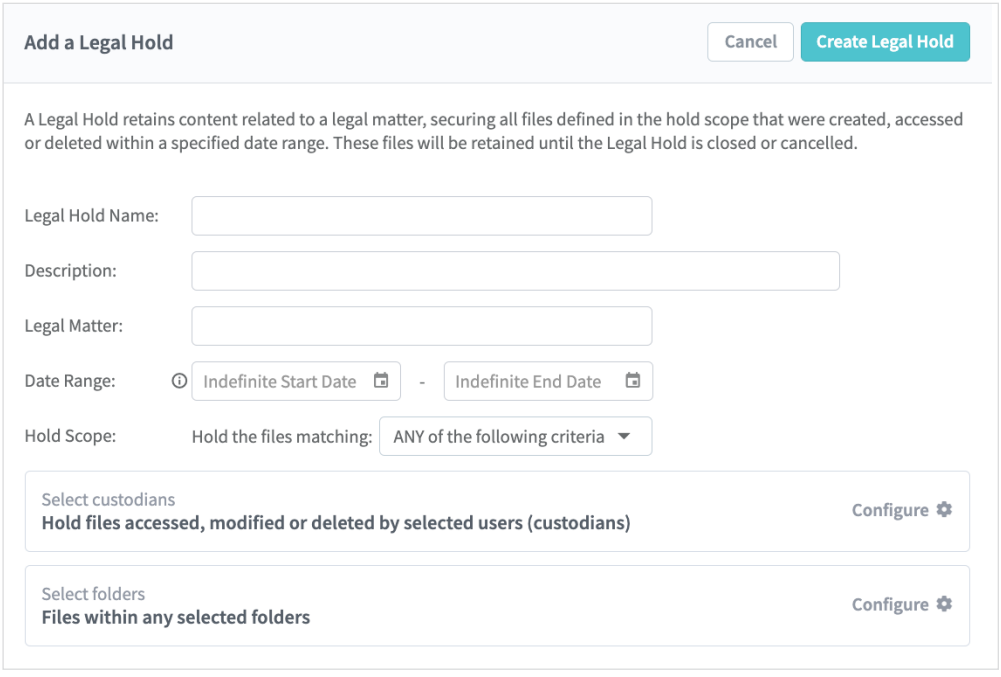

Figure 14. Snippet of the Legal Hold Options

While not a day-to-day activity of security analysts or incident responders, legal holds on data are an important element of ensuring that an organization is complying with any and all ongoing matters it may be facing. Often, legal holds may be subject to *capability*, not availability. Egnyte simplifies this process as well, providing an easy-to-use mechanism to establish legal holds on data.

As shown in Figure 14, we can easily implement a legal hold, specifying key legal hold details, scope, and range, and select specific custodians and folders. Legal and e-discovery teams should celebrate these features, as this capability is one that many organizations cannot easily implement.

Conclusion

In a nutshell, our key takeaway from this review is a single word: **simplicity**. Data security, governance, and management are often cumbersome tasks that require various technologies, specialized teams, and lengthy processes. The Egnyte team thought these through and put together a platform that can **incorporate multiple data sources and simplify the necessary, daily procedures that organizations must perform to protect themselves, their data, and their users.**

Egnyte did not stop there. With all the visibility and metrics included, they also built out a robust detection and response platform that allows for controlled containment and remediation if an incident breaks out. This platform frees up response teams to focus on other issues and ensure that data is no longer at risk. And in all, that is what the Egnyte platform does for its users—it helps them lower and manage risk.

About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a principal consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor: