SANS

Analyst Program

Whitepaper

2022 SANS Protects: File Storage

Written by **Matt Bromiley**

March 2022

EGNYTE

Introduction

One of the most important assets of any organization is its data. Data helps drive business and customer decisions and helps organizations reflect on the past and anticipate the future. Simultaneously, data is also a primary target of adversaries—ranging from state-nexus threat actors looking to purloin data, to ransomware threat actors who try to steal data from an environment or lock it up for ransomware and extortion.

Protecting data and files has become a top priority for organizations and security teams alike. File storage security serves as a cornerstone of information security postures and helps drive compliance requirements. Remember, though, that file storage security is not just for protection against outside adversaries. Organizations must also protect their files from within, including from those who already have access and may directly or indirectly let data leak out of the organization.

File storage security *must* protect files and data from multiple types of attacks and data leaks, while simultaneously providing a collaborative and productive environment for employees. In this SANS Protects paper, we look at threats to file storage and ways that your organization can overcome or mitigate them. SANS Protects papers focus on threats and mitigations, helping organizations consider elements of security that they should implement today.

Organizations can simply prop up a file storage solution, whether on-premises or in the cloud, within minutes. However, does that mean they've then secured the data? Does it mean that data is now compliant? We wish all solutions were that simple. However, organizations must ensure that they meet these needs continuously. Other considerations for file storage security include:

- File storage and protection relies on visibility (much like any other security approach). Ensure that you have visibility into your file storage assets, regardless of their "locations."
- Centralized or cloud-based file storage solutions do not immediately remove security concerns. Adversaries still actively hunt and look for data to achieve their goals.
- File storage is often an adversary's goal (not necessarily part of their attack path). So, if we detect at the file level, it might be too late.
- Automated defenses that can detect file changes, abuse, and manipulation are critical to defending against modern adversaries and attacks.

As you work your way through this paper, evaluate the current state of file storage options and security within your own environment. Within this paper, you will find that some of the discussions and suggestions either do or do not apply to your organization specifically. In any case, explore your organization's current deployments and confirm that you are receiving the protections upon which your security team makes its assumptions.

Threats to File Storage

As mentioned in the introduction, an organization's data and files represent a primary target for various adversaries. If we go back years to "typical" advanced persistent threat (APT)-style attacks, we see low-and-slow approaches that had adversaries appropriating gigabytes of data from an organization over a long period of time. Think back to Mandiant's early M-Trends report,[1] which measured dwell time in a matter of months (2014 listed a median of 229 days). These types of espionage or economic-advantage attacks did little to impact the data. Rather, the adversaries preferred to stay hidden in plain sight and hoped for little detection.

Fast forward to the past two years, and we have seen an explosion in ransomware/extortion attacks that do little to remain hidden. Ransomware threat actors do little to remain silent or hidden. To the contrary, ransomware perpetrators count on publicity and notoriety at a certain point in the attack life cycle to help them receive the funds they desire. We examine ransomware in more detail later in this paper.

Of course, adversaries are not the only threats. Some security teams may argue that the greatest threats to their data exist within the organization, in the form of data loss and leakage by employees (intentional or unintentional). Gartner's 2021 Market Guide for Data Loss Prevention (DLP) found that email is still a prevalent source for data loss within organizations and shows little signs of losing that dubious designation.[2]

Security teams may argue that the greatest threats to their data exist in the form of data loss and leakage by employees (intentional or unintentional)—with email being a prevalent source.

Ransomware

Ransomware poses such a significant threat to organizations that it deserves its own focus. For many years, many viewed ransomware as merely a "nuisance" threat. Adversaries had little impact on most organizations, demanded small sums, and the malware was trivial to reverse engineer. Furthermore, many organizations had backups or forensic means to easily restore data. Unfortunately, this is no longer the case.

Over the past few years, adversaries have studied the somewhat easily remediated efforts that their victims could use to reverse during an attack, and they've used that information to quickly ramp up their efforts. Ransomware actors now look for and remove volume shadow copies. Automated scripts identify and target virtual machine hypervisors and backup systems. And, perhaps most relevant, attack patterns heavily target file servers, where the highest value data resides.

Because the effects of ransomware are so wide-reaching, these attacks can quickly go from one system to the entire organization—from both an infection perspective and an impact perspective. This highlights even more the need to implement security controls and protections wherever possible, from entry vectors all the way to file storage solutions.

[1] "Reading the Mandiant M-Trends 2014 Threat Report," https://securityaffairs.co/wordpress/23898/cyber-crime/mandiant-m-trends-2014-report.html

[2] "Market Guide for Data Loss Prevention," www.gartner.com/en/documents/4002997/market-guide-for-data-loss-prevention

Unsecured Cloud Storage

Although not necessarily a "threat" in the traditional sense, cloud storage solutions open an organization to a previously unknown attack vector and potential data leaks or breaches. Of course, that statement contains assumptions—primarily that the storage solutions, such as an Azure Blob or S3 bucket, will be deployed incorrectly or with insecure configurations and so will be accessible to unauthorized parties.

Another reason cloud storage poses considerable security risks is the ease with which someone could spin up a storage resource and add sensitive data to it (all outside the purview of security). In other SANS papers, such as "2022 SANS Survey: Securing Infrastructure Operations,"[3] we discuss the importance of cloud asset visibility to help mitigate risks just like these. Just because cloud resources are easy to create does not mean they are easy to secure—at least not without proper tooling and security controls.

Unauthorized Third-Party Applications

Another consideration for the security team is how authorized users might go about sharing data with others. Despite the best-laid permissions of IT administrators, users often want to get data or a file from one place to another location where it should not be. This is not inherently malicious; the other place could be a separate or home computer, to a user without the correct permissions, or even just a place to print a file.

We'd like to think that most users have good intentions and do not want to harm their organizations or workplaces. Even so, users still must find ways to accomplish their tasks. Their methods may include transferring files to unapproved locations to improve access or to work on a different system. We want to ensure that we enact policies and tooling that can help detect and remediate before data leaks or other breaches.

Despite good intentions, these reasons still pose significant risk to an organization and leave the security team in a tough spot to determine the best protections. Do we prevent the use and connection of all external drives? Can some users request exceptions? Do we regulate printing or require all methods of transfer be approved via IT? Perhaps the most important question: Do we have the staff to support implementations and provide troubleshooting where needed?

Often, these questions and more predict where file storage security policies, procedures, and tooling either succeed or fail. Without proper implementation, training, and usage, a solution can become cumbersome and unused, leading to a false sense of protection.

Weak Authentication

Finally, we look at authorized, legitimate access as another threat to file storage. Such access refers to a scenario in which adversaries obtain legitimate user credentials and subsequently use them to access protected resources. File storage is not alone in this threat; anytime an adversary steals credentials and gains "legitimate" access to resources, it can create a nightmare for the security team. Unfortunately, adversaries who can successfully steal and abuse credentials can hide in plain sight and make detection difficult for security teams.

[3] "2022 SANS Survey: Securing Infrastructure Operations," March 2022, www.sans.org/white-papers/2022-sans-survey-securing-infrastructure-operations/ [Registration required.]

The security concern extends when credentials are the *only* barrier between an adversary and an asset. For example, single-factor authentication, coupled with weak password policies, can create a drastic situation for security teams. Detection can prove difficult, valuable forensic evidence may be little to none, and it may be too late before the security team notices.

Weak authentication is often a key contributor to ransomware breaches, offering a correlative value in security capabilities.

Unfortunately, weak authentication is often a key contributor to ransomware breaches as well. It also often offers a correlative value in security capabilities. Weakly configured storage solutions may give an adversary insight that security is lax in other areas and increase the value or ease of compromise of a target organization. Although this paper does not focus on perimeter security or zero trust policies, these concepts can prove valuable in mitigating file storage risks.

Protecting File Storage

File storage security is not a new concept for organizations. Many security teams have legacy policies and processes in place for protecting files, often in central locations such as on-prem file servers. Perhaps the biggest change in the past several years has been the shift to cloud-based storage. As we analyzed previously, cloud-based storage presents its own set of data challenges.

This section covers some technologies, processes, and implementations that may assist in providing the file storage security requirements that an organization needs. Keep in mind that you may already have the capabilities in these recommendations available to you. We recommend assessing the capabilities of your current tools and see what file storage protections are offered.

One big change in the past several years has been the shift to cloud-based storage, presenting its own set of data challenges.

Malware Detection

The first security implementation we recommend implementing is "simple" malware detection. We say *simple* because to many organizations this exists in the form of an antivirus or is currently available in endpoint detection and response (EDR) capabilities. The importance here is the capability to stave off a ransomware attack as early as possible. Unfortunately, if we wait until the adversary is *encrypting* files, we are too late in the process. In such a case, the adversary has already acquired credentials, moved laterally, and compromised a significant portion of the environment.

Detecting malware as early as possible not only helps protect file storage but also helps prevent myriad attacks from taking place. Ransomware is obviously not the only type of attack that utilizes malware, so the benefits are one-to-many. Organizations can stop multiple types of attacks with simple prevention and detection technologies.

Unauthorized Access and Change Detection

Another security control necessary for any file storage, whether on-prem or cloud, is detection of unauthorized access by a user. This may include:

- Unauthorized access of a file storage resource
- Unauthorized access of a file storage location, such as a folder or drive
- Unauthorized access or change of a file

The reason for this implementation is to identify changes made to files outside the normal expectations. Monitoring for this activity also helps stave off ransomware attacks. However, again, we don't want to wait until adversaries are making changes to files to detect an attack.

Cloud Asset Visibility and Management

One of the easiest ways to work around risks posed by cloud storage assets is to implement cloud asset visibility. Different from normal asset management solutions, cloud asset visibility solutions tie in to various cloud providers and keep track of assets as users deploy them. Asset visibility solutions also help keep track of deployment costs, runtimes, and associated resources. This knowledge proves valuable on its own, let alone for managing file storage solutions.

Case Study: File-Level Ransomware Detection

Our first case study looks at detecting a ransomware attack as it is occurring. However, if you wait until the adversary hits the file server to detect a ransomware attack, you may be too late in the attack to have an impactful response. You can still stave off an adversary in the final stages of the attack, but doing so at that point is not optimal. That said, stopping an attack at 99% completion can still save the organization some data.

When examining ransomware through the file storage lens, remember the various operations that ransomware perform on files: copy, overwrite, encrypt, and/or destroy. All these actions are noisy on a server, especially if they involve numerous files. Each operation creates valuable forensic evidence that, if examined post-activity, can provide a step-by-step look into the attack. If monitored in real time, your security team can use operations to detect potential changes and save the file server.

You can still stave off an adversary in the final stages of the attack, but that is not optimal. That said, stopping an attack at 99% completion can still save the organization some data.

Furthermore, we must also place file backups and backup systems in our threat models—because adversaries place them on their target lists. Once upon a time, ransomware attacks may have encrypted primary data servers but did not reach through networks to discover and wipe backup servers. This provided a unique opportunity to restore the environment from a previously known good version of files, but adversaries quickly caught on. We now see ransomware intrusions actively seek and encrypt backup files and systems.

To mitigate this, organizations can place malware and unauthorized access detections throughout an environment. However, we recommend utilizing the slew of ransomware file operations as detection mechanisms as well. A rapid succession of file changes, including copies, writes, encrypts, and deletions, is often indicative of only a few operations, each of which a security team could confirm as a false positive or not.

With insight into file operations, security teams could write powerful detections to provide unique insight into potential ransomware attacks. However, organizations could also possibly detect other types of attacks with strong detections. Malicious insider actions, such as file wiping or intellectual property (IP) theft, could also throw the same types of actions and be similarly detected.

Case Study: Misconfigured Cloud File Storage

Our second case study looks at an all-too-common scenario: cloud file storage propped up to support a specific organizational need and deployed with minimal to no security implications. We have seen this time and again in various data breaches, and in fact some organizations specialize in locating and responsibly disclosing things such as misconfigured (or "open") file shares or databases. Unfortunately, adversaries do the same.

Misconfigured cloud storage assets also present a multiheaded threat to organizations. The unauthorized access of data represents just tip of the iceberg, although still a considerable threat. One of the last things an organization wants to do is expose its data without an "intrusion" but instead through merely a misconfigured asset that allows access to anyone with knowledge of a URL or IP address and port number. However, a larger concern is whether the security team was even aware of the asset in the first place.

One powerful mitigation for cloud file storage—and cloud assets in general—is to utilize controls that offer visibility and classification into cloud assets.

One powerful mitigation for cloud file storage—and cloud assets in general—is to utilize controls that offer visibility and classification into cloud assets. This can provide the security team with the knowledge they need to successfully inventory and protect an asset. It also allows for an organization to apply security policies at the time of deployment, minimizing risks based on the security team's predefined processes and profiles.

Of course, the other issue at hand is that of Shadow SaaS—employees spinning up resources without the organization's knowledge and thus exposing sensitive files and data outside of visibility and security policies. Employees might not spin up storage resources with malicious intent; often they do it to facilitate a proof of concept (POC) or quick project. However, depending on the sensitivity of the data stored within the solution, it can create a troublesome situation and expand the organization's attack surface.

The same mitigations apply in this situation: Security and development teams must ensure that there is cooperation and an understanding of how rogue assets can impact the organization. Another useful control or point of visibility for security teams is how data moves in and out of the organization. Even if the security team cannot see 100% of the assets, tracking where and how data moves in and out of their monitored assets may provide the insight needed to see data leave an authorized location.

Finally, when it comes to cloud assets, other things beyond just misconfigurations also pose a risk to organizations. Weak credential options, such as single-factor authentication or easily guessed passwords, can open a "secure" file storage to malicious access. We use *secure* lightly in this context because sensitive data should sit behind multifactor authentication (if it can even be directly accessed at all). This creates an opportunity for security teams to rely on more evidence, such as access and authorization audit logs, to determine malicious access to sensitive file storage assets.

Conclusion

Maintaining the integrity, confidentiality, and availability of data is a top priority within many organizations, and so file storage security should always serve as a cornerstone of security postures. In this whitepaper, our first within the SANS Protects series, we looked at threats to file storage options and available technical controls or mitigations for those threats. We also explored implementation options for both new and preexisting file storage solutions.

Note that file storage security is not just a problem for security teams. Depending on data types and methods of storage, organizations may also be subject to various regulations and compliance requirements. Therefore, as we explored, file storage security must straddle at least two lines: keeping an organization's data safe while maintaining ease of access for users and regulatory compliance. Keep this in mind as you consider and implement various security controls. As we said in the paper, look for opportunities to find multiple benefits with one implementation or solution.

Finally, file storage security must also *work*. The data within is far too important. After all, a ransomware attack can cost the business valuable time and resources that it simply does not have. Finding out that your security solution did little to protect your data hardly deserves to be called a security solution. Ensure that, as you implement controls and capabilities within your environment, your security team constantly tests and evaluates to ensure the protection of your organization's data.

Sponsor

SANS would like to thank this paper's sponsor: