

Three Reasons Why You May Be The Next Data Breach Target



In the era of the data breach and ransomware attacks, organizations know they need to protect sensitive data stored in applications and databases. Where too many are failing, though, is in protecting their unstructured data. 80% of an organization's data is now stored in unstructured files, not databases. It's in collaboration portals such as SharePoint, it's stored in NetApp Filers and EMC Isilons, it's on the web in OneDrive and Box, and in truth scattered across the globe. What's truly concerning is the problem is only beginning. The amount of data stored in file servers and NAS devices, collaboration portals, mailboxes and cloud folders is projected to grow 800% in the next five years.

This glut of data also arrives at an intersection where attack methods have shifted and the attack surface has exploded. There's no longer a single network entry point to defend. Instead, people are now the targets. This means defenses must operate in real-time, and be able to identify not only attacks that originate outside the perimeter but also malicious requests from seemingly valid users.

Too many enterprises remain unprepared for how critical securing unstructured data has become. There are three main reasons companies remain unprepared for these changes.

1

Lack of Visibility

Organizations must be able to find sensitive data in order to manage and secure it. That means not only the data in applications and databases, but also managing the creation, download, and upload of unstructured data. Even something as simple as creating a presentation can yield multiple files stored in different locations, or even distributed globally as an email attachment. Any security solution that doesn't involve classifying and protecting unstructured data leaves gaping holes in its coverage and the organization open to data breaches and regulatory penalties for non-compliance.

2

Overpermissioned Users

What happens to a user's permissions when they leave the organization? Or when they switch positions within the company? Too often, they are simply carried forward as much for convenience as anything else. Visualizing the various pathways a user has access to unstructured data can be difficult to manage and control. Ultimately, organizations should seek to normalize permissions across the enterprise. In an age where malicious requests can come from seemingly legitimate users, removing stale permissions is imperative for enterprise security efforts.


3

Lack of Governance

Most unstructured data has no true owner, or in other words no permissions that stop it from being shared. Compliance requirements such as GDPR and CCPA demand least privilege access policies and material changes in how and where organizations store customer data. It's a new level of detail that will catch unprepared organizations flat footed. Ultimately, protecting sensitive data requires an understanding of who should have access, and who shouldn't.

SailPoint Can Help

SailPoint knows unstructured data requires a different approach, one that focuses on identity as the means to protect the enterprise. It's that identity context that empowers business success.



SailPoint IdentityIQ File Access Manager extends identity governance to unstructured data, providing the identity context necessary to protect those files against targeted phishing campaigns, insider threats and other sophisticated attacks.

SailPoint proposes a three pronged approach that serves to embed identity context into data governance decisions and processes. It's an approach that builds security into the very fabric of the enterprise, letting organizations move their security efforts forward in a way that counters both new and existing threats.

Step 1: Identify Risk

The first step in any security program has to be identification of risk. That includes classifying sensitive and exposed data. It also means finding data exposed by open permissions schemes. By discovering and monitoring access to files containing sensitive data such as PII, PHI, and PCI, IdentityIQ File Access Manager minimizes risk exposure to data leakage or breaches.

IdentityIQ File Access Manager gives organizations the power to:

- Quickly scan on-premises and cloud based file stores to find files containing sensitive information via data classification and user activity behavior.
- Clean up permission path headaches by leveraging visual maps of the various ways users have been granted access and may be accessing sensitive files and folders and streamlining their access to one main permission path.
- Manage files stored across hybrid environments by ensuring connectivity and access to Microsoft Windows Servers, Hitachi, EMC, and NetApp devices as well as Microsoft Exchange and Exchange Online, SharePoint and SharePoint Online, OneDrive, Google Drive, Dropbox, and Box.

Step 2: Implement Governance

When data is properly classified, policy violations can be automatically sent to data owners and security staff to end malicious behavior in real time. Organizations who fail to actively assign accountability to data owners to understand who should have access, and just as importantly who actually has access, are leaving themselves open to data breaches and regulatory penalties. IdentityIQ File Access Manager delivers the power to protect business-critical data stored in files by applying consistent administrative processes, policies and controls across systems running on-premises or in the cloud.

In addition, organizations looking to adhere to strict compliance requirements need to strengthen the controls that determine who has access to specific data, and who doesn't. Conversely, removing unwanted and unneeded access to systems, applications, and data is crucial to the success of security efforts.

IdentityIQ File Access Manager helps enterprises implement data governance by:

- Unifying identity and data governance policies by centrally managing access to all files stored on-premises and in the cloud.
- Stopping malicious behavior in its tracks via real-time monitoring of user activity.
- Providing an easy and automated way to prove compliance with required legislative initiatives.
- Detailing data access activity, policy changes, permissions and more via over 100 ready-made reports.

Step 3: Empower the Enterprise

Empowerment means putting decisions into the hands of the business owners who understand the data in its proper context. In traditional “top-down” permissions management approaches, the processes behind managing permissions are detached from the information or resources they should be protecting. Properly balancing the security and risk management needs of the organization with desired business outcomes enables organizations to safely increase collaboration both inside and outside the network.

SailPoint enables a paradigm shift towards a resource/data centric permissions management approach (i.e. normalization) at a pace suitable for administration teams. IdentityIQ File Access Manager improves data security by allowing relevant data owners to control user access and usage via an intuitive and actionable dashboard.

SailPoint IdentityIQ File Access Manager helps organizations meet their business objectives by building a framework of empowerment that:

- Aligns access with business need and provides a strong foundation for governing access throughout a user’s lifecycle.
- Quickly identifies relevant data owners via a proven and innovative crowdsourcing approach.
- Speeds security decisions via intuitive and actionable dashboards to manage access to resources using data security KPIs and real-time risk scoring.
- Enables business data owners to determine and respond to user access requests from their laptop or tablet, keeping productivity flowing.
- Leads to significantly fewer permissions and tighter controls surrounding data resources.



Mature and extend your identity governance efforts to include all your unstructured data.

Having a unified approach to securing access to sensitive data, whether it resides in applications or in files, or on-premises or in the cloud, is a critical component of managing risk and complying with global regulatory requirements. Data security needs identity context for better control. Extending an identity governance platform with data access governance capabilities gives organizations full visibility into “who has access to what,” and insight into how that access is being leveraged. It also gives

enterprises the means to not only meet various compliance and other regulatory requirements, but also to realize an overall improved security posture that allows for security to be built into existing processes and procedures that extend both their value and effectiveness.

IdentityIQ File Access Manager gives organizations the means to mitigate the risk of inappropriate access, improve audit performance and decrease operational costs by centrally managing and controlling user access to sensitive data stored in file folders such as Box, SharePoint, and Google Drive.

**SAILPOINT:
RETHINK
IDENTITY**

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on [Twitter](#) and [LinkedIn](#) and by subscribing to the [SailPoint blog](#).