SailPoint

SOLUTION BRIEF

Mitigating Data Breach Risk with Identity Governance for Files

As data breaches in enterprises have become more frequent and more destructive, the market has turned from an "if breaches happen" to a "when breaches happen" mindset. No longer is being the target of a data breach an uncertainty, but instead an eventuality. Whenever a breach happens, the consequences that come with it are not only financial, but also emotional.

When a breach does occur, its end goal is usually the procurement of data that the enterprise holds. The first "knee jerk" reaction may be to completely shut down access across the board, but this only causes more problems than it solves by preventing the employees from doing their daily jobs. Breaches can take 229 days to be found[1], and in all likelihood, the hacker is already long gone by the time the breach is discovered. If you have not governed access to your organization's data well, it will take even more time before you will be able to find the source and shut down any more leaked information.

Considering that organizations today have 80% of their corporate data in unstructured stores, it is an obvious source of sensitive information that is more than likely not well-protected. Imagine how much personal information on both employees and customers may be sitting in text documents. Or financial information in spreadsheets and PDFs.

The best way to prevent extraneous risk and mitigate how much data is exposed during a breach is to comprehensively secure access to all users, applications, and data stored in files.

Securing Access to Your Sensitive Data Stored in Files

While the need to protect your organization's sensitive data is clearly an important piece of your security processes, just how to protect it may not be as easy to determine. There are three basic steps – locating sensitive data, ensuring the appropriate access, and assigning data owners – that will set you down the right path to mitigate the risk of a data breach by securing access to your data stored in files.

[1] *2016 Cost of a Data Breach,* Ponemon Institute

1

Step 1: Find Where Sensitive Data Exists

The first step in securing your unstructured data is to find where your sensitive information resides. The sheer volume of unstructured data can make this an extremely difficult task, especially if you plan on tackling it manually. Enterprises can easily have hundreds of millions of files across their file servers, networked drives, collaboration portals such as SharePoint, cloud storage, etc. and cataloguing all that data can be a tall order, much less identifying and securing it. Employing a comprehensive identity governance solution that extends to data stored in files can help identify and classify your sensitive data.

2

Step 2: Identify Who Has Access

Once you have identified all your data and determined what is and isn't sensitive, you must then be able to answer the question "who has access to what?" The goal of your identity governance program is to ensure that your users have the right access to the right applications & files at the right time.

With a holistic solution in place, you can easily determine who has access to your data, and by which means (individual or group permissions, stale authentication from a previous position in the company, etc.). This visibility will give you a greater insight into how access is granted/terminated within your organization so that you can manage it properly. You will then be able to create the appropriate policies and procedures, as well as clean up the current permissions granted within the organization and maintain it in the future.

3

Step 3: Elect the Right Data Owners

In order to drive better governance you should identify and empower data owners who have the most intelligence about the data. While organizations traditionally assign business owners to specific applications, the same cannot be said for data stored in files, and finding the appropriate owners can be challenging without the right methods.

Rather than try to take an over-simplified approach to assume who is the right data owner based on the most active user, you should instead employ a crowd-sourced approach to ask those who use the data the most who should own it. Without the proper owners, data can easily become stale, permissions can be excessively granted, and other security problems can ensue.

Moving Foward

When all three steps have been initially completed, it is then time to begin automation of your processes. Your identity governance approach must be able to automate access certifications, streamline access requests through self-service tools, as well as locate and track new sensitive data as it is created and provision the proper access to it. All this needs to happen with as little required oversight from IT while still giving them the tools to have a 360-degree view of the data, and what they are doing with that access.

SailPoint Can Help

To fully address today's modern data security needs, organizations are moving beyond traditional data access governance solutions, and incorporating sensitive data stored in files and folders as part of their comprehensive identity governance program. By taking this approach, organizations will reduce their risk of breach by 60%[2].

Visibility

In order to protect access to sensitive data, you must have a holistic view across your entire infrastructure. If your IT team or business owners are unaware of where sensitive data resides, cannot see all the permissions a user has, or how this access is being used, they simply cannot make the right access decisions are unaware of where sensitive data resides, to mitigate security and compliance risks.

IdentityIQ File Access Manager helps answer these essential questions:

- Where is your sensitive information?
- Who has access to it and is that access too broad?
- What are those users doing with their access, and do these actions violate your security policy?
- Can you prove all this to an auditor?

Control

Accurately identifying data owners is a key step towards effectively controling and securing your organization's data. Organizations who fail to actively assign accountability to data owners who are most knowledgeable about who should and shouldn't have access, are leaving themselves open to data breaches and regulatory penalties.

Once the owners have been elected from those who actually use the data on a regular basis, you must then enable them to manage their data via user-friendly tools that ultimately save them time.

IdentityIQ File Access Manager allows data owners to:

- Get visibility over the data they own.
- Self-configure alerts that are brought directly to their attention.
- Create a task list to keep owners on track.
- Provide controlled access through self-service access requests.
- Give IT oversight and compliance through periodic entitlement reviews.
- Add access and remove high-risk access through actionable intelligence.

[2]*Gartner Identity & Access Summit,* Las Vegas, 2017

Compliance

Organizations in a regulated industry will always be concerned withmaintaining compliance. But even those in less-regulated industries still need to understand that the data they possess needs to be protected. The security of this sensitive information and compliance with any regulations is imperative.

IdentityIQ File Access Manager helps compliance efforts by providing:

- Visibility into the location of sensitive documents.
- Validation that sensitive documents are only accessible on a need-to-know basis.
- Activity monitoring to ensure that only the proper identities are accessing the data.

Conclusion

Rather than hope a breach never occurs in your enterprise, it is a better idea to mitigate as much risk as possible. Planning ahead and helping to secure as much of the organization as possible before a breach is attempted is the best way to secure your organization's data whether it is stored on-premises or in the cloud. SailPoint can help to ensure you are secure now, tomorrow and in the future.

SB1021-1903