SailPoint

SOLUTION BRIEF

Protecting Intellectual Property with Data Access Governance

Intellectual property (IP) is what separates one enterprise from another and provides a competitive advantage in the market. Securing IP and ensuring that only the right people have access to it – and nothing more – is of paramount importance. In order to protect IP in your organization, you must know where it resides, who has access to it and what those users are doing with their access.

Finding Your Sensitive Information

The first challenge that most organizations find themselves struggling with is locating where sensitive data resides. This task is difficult because IP-related data can be stored in applications and files that can be difficult to track; while many organizations have visibility and control over access to data in applications, identifying which files contain sensitive data is a much more difficult task. For example, if an employee exports financial data from SAP into a spreadsheet, that data will now reside in files that are not in a structured database. This unstructured data – along with the unstructured data the rest of the enterprise is creating – does not follow the normal schema and can be difficult to identify as sensitive.

While your organization's policies may tell your users where to store sensitive data, including IP assets, the unfortunate reality is that your users may or may not follow those rules. This causes multiple problems, including making securing sensitive information nearly impossible since you don't know where it is.

This is the first area in which a data access governance solution can help: it can automatically scan your systems where files are stored and search for specific keywords, patterns and behaviors to identify any files which might contain potentially sensitive information. With this first step complete, you can then determine who has access to your organization's important data – including your IP.

Determining Who Can Access Your IP

The next step in protecting file-based sensitive IP, including text documents, presentations, e-mails, etc., is to determine who has access and how that access is granted (directly through an account or entitlement or indirectly through a

membership in a directory group). This is a key step in the process since a few extra people having access to the next holiday party location won't pose a threat or make you fail an audit, but the same cannot be said for unauthorized users having access to financial or customer data.

The simple fact is that you can't protect your sensitive data if you don't know who has access to it and how they got that access. A data access governance solution can identify all the direct and indirect permissions that allow a user to have access to a certain file or folder, enabling you to reduce excess permissions or terminate access entirely. Without this visibility and control, users may continue to have access to sensitive data even after attempts have been made to remove it since access can be granted by multiple paths.

Another important aspect of controlling access to unstructured data is by assigning data owners. Without someone to oversee the relationships between users and sensitive data, your organization can be quickly put at risk of a data breech as new users and data arrive. Additionally, data can become stale, excess permissions can be granted, and the general health of the data can deteriorate. By leveraging a data access governance solution that can assist you in finding the right owners, you can add valuable oversight and control. One approach is to use activity to determine the most likely owner, but it is much more effective to ask your users – the ones who use the data on a regular basis – to elect your data owners. This guarantees that you leverage the person most familiar with the data and its contents to control access.

Automation & Planning for Growth

Once you have determined which files contain sensitive data, who has access to them and who owns them, you need to find out what those users are doing with that access. Some of the most damaging data breaches have occurred when a user has appropriate access to certain files, but they are using that access inappropriately. For example, a user could download entire volumes of sensitive information – customer lists or financial data – right before leaving the company. Understanding appropriate usage patterns and alerting security administrators when something looks suspicious is the best way to mitigate the risk of IP loss.

A data access governance solution can help keep the massive volume of your organization's unstructured data in check. While manually sourcing all this information – where sensitive information resides and who has access to it – can be done, it is a time-consuming and error-prone process when your organization could easily have 100 million files (or many more). Finding all that you need to know about every file simply isn't possible with manual processes.

Automating key controls to secure your unstructured data is the best option. Streamlining onboarding processes for new users – including provisioning and de-provisioning of access – ensures that users get the access they need to be productive, but no more than is necessary. Additionally, implementing self-service

access requests and real-time event monitoring for suspicious behavior means that not only can you secure the unstructured data you currently possess, but you can be prepared as the amount of data your organization possesses continues to grow in the future. As a final measure of prevention, regular review of access to unstructured data should be integrated into your automated control framework. This works as both a security backstop and validates for your auditors that you are taking the necessary steps to protect sensitive data.

SailPoint Can Help

At SailPoint, we know how to secure an organization's users – its identities – including how (or if) they access your data. In order for your organization to be secure, you need both identity governance and data access governance solutions to ensure you have full visibility, control and compliance over all your data – structured or unstructured.

Visibility

In order to govern users' access to data, you must have a holistic view across your entire infrastructure. If your IT team or business owners cannot see all the permissions a user has, they simply cannot make the right decisions about who should have access to what to avoid complications from over-entitlement and separation-of-duty (SoD).

IdentityIQ File Access Manager helps answer these essential questions:

- Where is your sensitive information, including your intellectual property?
- 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

Before you can effectively control and secure your organization's data, you must first identify its owners. While structured data stores have generally been assigned business owners, unstructured data usually do not have a complementary owner. Without proper data owners, unstructured data in files can be easily overlooked, incorrectly classified and improperly managed in terms of who has access.

Organizations who fail to actively assign accountability to data owners to understand who should have access and who does have access to sensitive data in the enterprise are leaving themselves open to data breaches and regulatory penalties. For instance, if a public company has its financial data leaked and its stock price falls as a result, its investors are negatively affected and the company is now in violation of the Sarbanes-Oxley (SOX) regulations.

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.

Compliance

Organizations in a regulated industry will always be concerned with staying within 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 aren't being leaked outside of protected areas.
- Activity monitoring to ensure that only the proper identities are accessing the data.

Conclusion

Protecting your organization's IP is and always will be a major part of your security program. SailPoint can help you identify where sensitive files reside, determine who has access to them, elect the right data owners, and keep this important information secure both now and in the future.

SB1022-1903