SailPoint

SOLUTION BRIEF

When Identity **Meets Data**

Data. It's the foundation for business in the modern world, and the lifeblood of every organization regardless of its business or location. In today's connected world, data exists in many places: in data centers, on corporate desktop systems, in email and even on users' personal mobile devices. Data allows us to store and share information about a wide range of corporate activities, including business plans, financial results, trade secrets, employee programs and many more. It's how employees, contractors, business partners and vendors communicate with one another every day. Data can take many forms and can be stored in a variety of locations. But if it's not protected, your business can be irreparably harmed – both financially and with its reputation.

Not all data is created equal. Some data – corporate financials, intellectual property, highly regulated data (personally identifiable information) – requires special handling in order to mitigate the risk of a data breach and the resulting ramifications of the data being used inappropriately in or out of the organization. And since data can be stored in a wide variety of locations, this makes protecting access to data, especially sensitive data, a daunting task. Sensitive data, can be particularly challenging, and deserves special attention because of its importance to the organization.

Hidden Gaps in Data Protection

Unfortunately, protecting sensitive data can't be achieved with physical security alone. In order for data to be valuable within an organization, it must be accessible, but only by the right people. Therefore, managing access to data is a critical component in protecting it from those trying to steal it or use it in malicious or inappropriate ways. In the past, sensitive data such as financial information or customer data could be locked away in structured applications such as mainframes, ERPs or databases where access can be strictly controlled.

Unfortunately, structured systems are not the only place sensitive data is stored. Unstructured data, or data that is generally stored in files outside of structured applications and databases, is a growing problem for organizations around the world. In many cases, unstructured data started out as structured data in an application, but was then moved by an end user into a format more convenient for their task at hand.

Think about how many times sensitive financial or customer data in your company has been transferred to a spreadsheet or document so that the information could be easily shared with other employees, business partners or contractors. It's easy to see how quickly data can move from secure, controlled environments to convenient, but unsecured locations.

Most enterprises now store so much unstructured data on file servers and NAS devices, on SharePoint sites, and in cloud storage systems that they have no effective way of determining what they possess, where it is stored, or who has access to it. The inability to effectively govern access to unstructured data presents serious and growing risks, including brand damage as well as regulatory and legal exposure.

Closing the Gaps – Governing Access to All Data

So what can be done to better protect sensitive data? The answer lies in taking a comprehensive approach to governing access to all data, structured or unstructured, in the enterprise no matter where the data exists: in applications or files, in the data center or in the cloud. This is where traditional identity and access management solutions fall short. They focus on securing access to applications (which is, of course, important), but they don't address sensitive data stored in unstructured files.

Only an identity governance solution which spans applications and data will secure access whether the data is stored in structured applications and databases or unstructured files. Additionally, the identity governance solution must also take into account where the sensitive data is stored and how access to it is granted. Taking a comprehensive perspective gives organizations the visibility to who has access to what, while also supporting the preventive and detective controls needed to restrict access to data and identify and remediate security issues, and also addressing a growing number of regulatory requirements, including SOX and GDPR.

Finding Your Sensitive Data

The first challenge organizations face in securing access to sensitive data is knowing where it is stored. Applications and databases are the obvious place to start since they are well-understood repositories of data in the organization. They generally have both business and technical owners who can be interviewed to understand what type of data is generated or stored within their boundaries. The challenge comes when users move data from a structured system into another format to make it easier to share the information with other users. 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.

Identifying where unstructured data is stored is much more challenging. First, it can be stored in a wide variety of locations inside the data center (e.g., file shares, NAS devices, SharePoint) or in the cloud (e.g., Box, Google Drive, SharePoint Online). Second, unlike structured applications where changes to data are tightly controlled and monitored by the application owners, unstructured data can be created, modified and deleted by almost anyone in the organization. This makes it vastly more difficult to identify the specific locations where unstructured data resides at any specific moment in time. The only realistic way to find and keep track of sensitive data stored in files is to leverage an automated solution that can scan systems in the data center and cloud where users store files.

Once you have located where sensitive data is stored in both structured systems and unstructured file stores, you can begin taking steps to proactively govern access to it. Next, address issues with how access is granted to the systems and files themselves. This can be a complicated task, especially where groups or roles are used to abstract users from the underlying access models. However, ensuring you understand and correct any issues in how access is granted is a critical step in the governance process.

Designing Preventive Controls for Real-time Governance

After locating where sensitive data exists and making sure it is stored in the right place and with the right access model, the first priority is putting appropriate preventive controls in place to ensure only the right people gain access to it. Access to sensitive data should be highly restricted, and users should have access to only the applications and files needed to perform their jobs. This may sound straightforward, but do you know what data is sensitive and what access privileges are appropriate for any given job function within your organization?

An identity governance program spanning applications and data stored in files can help find sensitive data across the enterprise and by collecting and analyzing permissions show "who has access to what." It can also help ensure that user access conforms to policy and job roles as access changes throughout a user's lifecycle within the organization. Key preventive controls for ensuring users have the right access to the right data include real-time policy enforcement during access requests or automated provision events and built-in approvals by business managers, data owners or application owners. By leveraging a single approach for granting access, while concurrently enforcing policies in real-time, organizations can streamline delivery of access to the business while also improving their security posture.

Implementing Detective Controls to Cover All Your Bases

Organizations also need detective controls to review and monitor user access and activity for anomalies that need investigation. In other words, it's not enough to simply define access controls and forget about them. Too many factors in the environment are constantly changing (users, applications, directories, etc.), and sometimes policies and procedures are not followed to the letter. Detective controls allow organizations to identify and rectify problems before they lead to a catastrophic breach. Examples of detective controls include periodic review of access by supervisors and data owners and monitoring of user activity affecting sensitive data. Every organization will benefit from detection of dangerous situations such as a fired employee who still has access to cloud storage or a user who has downloaded large volumes of sensitive data on multiple occasions.

Similar to preventive controls, a consistent, uniform approach to implementing detective controls is an important aspect of an effective identity governance program – especially one that is designed to govern access to sensitive data stored in applications, databases and files.

Summary

Protecting sensitive data can feel particularly daunting given the challenges outlined. Fortunately, there is a solution – identity governance – that allows organizations to address the growing amount of sensitive data in the enterprise and align it with the users who need access to it.

Balancing security and convenience is the key to success.

Business is driven on easy, real-time access to the information it needs to succeed. But that convenience has to be checked with strong controls that ensure data is safe from prying eyes. By leveraging a comprehensive approach to governing access, you can mitigate risk and secure your organization.

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%[1].

By laying the foundation for effective governance across all identity activities, and providing a complete framework for centralizing identity data, SailPoint can help organizations establish controls that ensure users have the right access to the right systems and data at the right time.

The SailPoint solution provides a single view of a user and their accounts, entitlements and associated risk across all applications, as well as structured and unstructured resources for "big picture" visibility and control. It also transforms technical identity data scattered across multiple enterprise systems into easily-understood and business-relevant information through intuitive reporting and dashboards. With the SailPoint platform, organizations can more quickly identify risks, spot compliance issues and make the right decisions to strengthen controls.

SailPoint, a Gartner Magic Quadrant Leader, built our business on the foundational principle that identity is everything.

It's your data. You own it.
But hackers are hard at work to get it.
How will you protect it?

Learn more at sailpoint.com/data

[1]Gartner Identity & Access Summit, Las Vegas, 2017

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SB1016-1809