One Identity

Six Steps to Achieving Data Access Governance

Abstract

Data is an organization's most valuable asset, consisting of anything from intellectual property to customer information. Often, this data is found on a number of platforms: Microsoft® Windows® file servers, NAS devices, SharePoint® sites and more. Unfortunately, many organizations cannot adequately control access to that data, or even reliably assess who currently has access.

Nevertheless, organizations need to satisfy compliance requirements and be able to quickly address security threats—or, ideally, prevent them from arising at all. They need to centralize the access request process and put an end to ambiguity about who has access to what. They need automated, multi-platform data access governance. This white paper outlines six steps to achieving that data access governance.

Introduction

Organizations know that controlling access to data is vital: security breaches, mistakes and leaks of sensitive enterprise data can lead to loss of intellectual property (IP), system downtime, frustrated users, lost productivity, fines for failing to comply with external regulations, and organizational embarrassment. But the processes at many organizations today to achieve that control are tedious, time-consuming and error-prone. Administrators try to monitor group changes in Active Directory®; data loss on file servers and NAS devices; and SharePoint activity, but all too often these approaches simply address current symptoms but fail to permanently fix the root cause of problems. Moreover, all that manual work and reporting distracts administrators from working on other projects.

Can your IT department even answer whether or not you should have the access you have?

A warm breeze swirls up a deserted main street as a tumbleweed blows past two men about to face one another in a draw: it's the Wild West – a great analogy for the state of data in most organizations today. You've got your disputes over who owns what, your band of outlaws trying to steal what's yours, and usually an outgunned security team who is doing its best to keep the peace.

Also remember that the Wild West was a time of growth (mostly uncontrolled growth), with new towns popping up and population increasing – very much like the data in your environment. You have new data being created and saved on platforms from Windows file servers to NAS devices, and you even have SharePoint sites popping up. More than likely, your employees are constantly using new devices, such as iPads®, to access, create and alter data as well.

Your IT department is acting as sheriff, doing its best to keep up and keep the peace, but today's outlaws are no longer the obvious tall dark stranger in the black trench coat who elicits a frightened gasp as he walks into the saloon. You face myriad threats to your data, and you have multiple compliance regulations and internal policies to adhere to. You need automated, multi-platform data access governance.

The problems with current practices

What exactly are the problems with current data access control methods? Inefficiency, ineffectiveness and a lack of agility.

Inefficiency

Securing and controlling access to data in your infrastructures is a tedious, repetitive, time-consuming process. In your environment today, how long would it take your IT team to discover what you have access to, and how you gained that access? How would they go about doing it across all the platforms in your entire organization?

The bottom line: Current practices are inefficient, whether you are manually assessing all of the unstructured data across your widely diverse environment, uncovering data loss on file servers and NAS devices, or inventorying what's available on SharePoint. And that inefficiency keeps administrators from working on other projects.

Ineffectiveness

Here's a big issue that most organizations never address: Can your IT department even answer whether or not you should have the access you have? Unless you are in a very small company, the answer is no. IT can't possibly know whether your role should be permitted to access certain files or folders; that's a business decision, not a technical choice. But most organizations do place IT in the role of gatekeeper to monitor and secure access to data, which leads to users having access that the business would say they shouldn't have. Additionally, you will inevitably be left with unstructured and orphaned data—no one knows who it belongs to, whether it's still valid, and so on.

Lack of agility

Today's environment is reactionary – problems arise and you react to them. Of course, there's always going to be a need for solutions that can help you react to problems, but if all you do is fix things at this moment in time, with no thought of what happens down the road for the future, then you can't be very agile. For example, you might be able to assign an owner to each piece of data you have today, but what happens tomorrow when an employee resigns, new people are hired, and your company acquires another smaller company? You need a process in place to centralize access requests and put an end to the ambiguity of who has access to the data, and, more important, who should have access to the data.

Solutions exist to address some of these problems, such as discovery, control and automation. However only one vendor

offers a holistic approach that can deliver end-to-end data access governance that is poised to take you into the future.

The new frontier: data access governance

Step out of the Wild West and into the new frontier! Often people feel that the only viable approach to data security is to go to an extreme and lock everything down as if it were Fort Knox, but that approach can cripple the productivity of your employees, who have legitimate needs for data access.

Fortunately, there is a civilized process that you can use to address the challenges of data access governance. By implementing a comprehensive data access governance strategy, you can regain control of your data. The figure below shows the six steps in this strategy; you can insert yourself at any step depending on where your organization is with respect to tackling these challenges.

The six steps

1. **Discover users and resources.**
   If you're just starting down the path, the first step involves taking an inventory of your infrastructure. Who are your users, what resources (such as file shares) do you have in your environment? You'll also need to discover and document the extent of SharePoint, and identify any unstructured or orphaned data. This will give you a full picture of what you are dealing with.

2. **Classify data and access rights.**
   Once you have a sense of what is in your environment, you need to classify it to identify whether it's confidential, whether it is affected by any regulations (for example, credit card numbers need to be handled in accordance with PCI), and whether it is still relevant or should be archived. Determine who the business owners of data should be, and assess your identity and access management policies. You are working towards establishing an access model that is based on established and consistent policy and on existing identity infrastructure.

Fortunately, there is a civilized process that you can use to address the challenges of data access governance. By implementing a comprehensive data access governance strategy, you can regain control of your data.

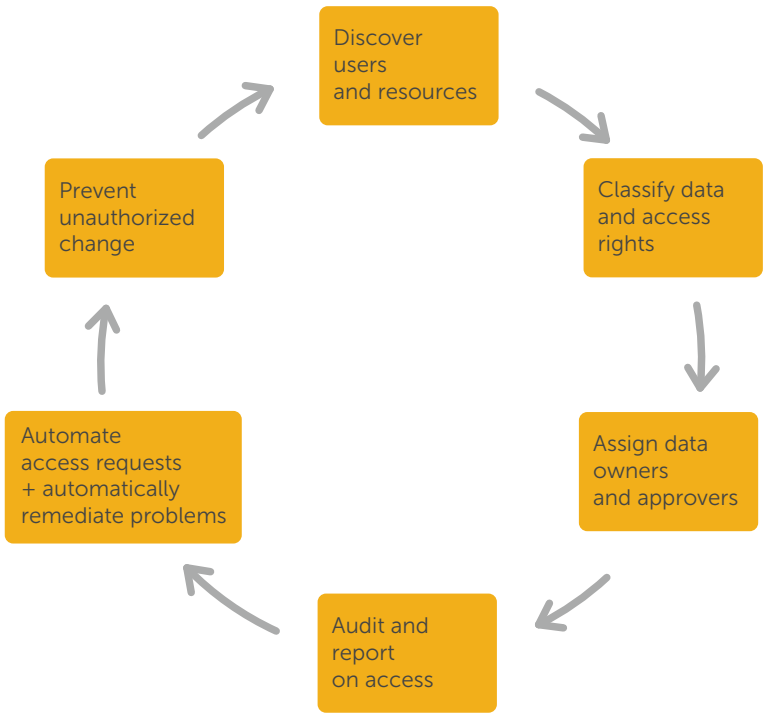

Figure 1. The six steps in an effective data access governance strategy

Controlling data today can seem like the Wild West.

3. **Assign data owners and approvers.** Here the rubber starts to hit the road: You're now assigning the appropriate business owners of data based on their roles, locations or other attributes. Going forward, the business owner will be the one to grant access, not IT. During this phase, it's important to perform the necessary checks for compliance to ensure separation of duties (e.g., the requestor can't also be the approver). The final part of this step is to establish an automated work-flow process for future requests so you won't have to go back to the drawing board when changes are requested down the road.

4. **Audit and report on access.** Since data in your environment is constantly evolving, it's crucial to schedule regular business-level attestation of access to ensure accuracy and security. You can then generate detailed reports for auditors to prove adherence to regulations.

   The attestation process must be efficient and take into account that it is the business owners who have the knowledge to do the attestation. You want to replace current inefficient processes in which reports are gathered by IT, passed to the business, interpreted, and handed back to IT to implement changes. Enabling the business to do it all themselves improves data access governance.

5. **Automate access requests and automatically remediate problems.** For security, your process must grant access only based on the requester's role within the organization. One approach is to use an access request portal: Users can request access resources and appropriate personnel can review the access to validate that the process is working as intended. It's also important to implement automated responses that remediate any deviations from the rules that you have worked so hard to establish.

6. **Prevent unauthorized change.** There are always going to be certain data, groups or access rights that you'll want to secure from ever being altered. So lock those down and set up a real-time alert to notify you if a change attempt is made. It is also best practice to log all changes in a secure depository that can't be altered, separate from standard event logs, for any forensic analysis later. But simply knowing "a change" was made isn't going to tell you much down the road, so it's equally important that your logs record and show you what change was made, with the before and after values.

Conclusion

Controlling data today can seem like the Wild West: You must deal with constant threats, declining enforcement budgets, rapid growth and constant change. But while addressing the challenges of data access governance is neither quick nor easy, it doesn't need to be insanely complex, either. Using the holistic approach outlined in this paper, you can get your environment in order now and address the root of the problem so that it continues to stay in order in the future.

One Identity solutions can help you establish complete 360-degree visibility into user access in your organization, including extending the security you already have through Active Directory to your non-Windows systems, applications and data. Our data access governance solutions enable organizations to discover, assess and assign ownership with scheduled attestation for maintenance across a multi-platform environment. One Identity solutions also deliver change monitoring and compliance reporting to close the loop on the governance process for ongoing security. This approach ensures efficiency, effectiveness and agility for the future.

To learn more, please visit: software.dell.com/solutions/access-governance.

For More Information

About One Identity

The One Identity family of identity and access management (IAM) solutions, truly offers IAM for the real world including business-centric, modular and integrated, and future ready solutions for identity governance, access management, and privileged management.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.