Mitigating Risk by Governing Access to Unstructured Data

Governing access to mission-critical data within file-based, unstructured data is imperative for data protection and privacy compliance. Historically, the focus of data access was concentrated on application repositories associated with IAM systems. Unauthorized access of unstructured data is a risk that analysts, legislatures, CSOs, and compliance officers must address.

Basis

Data Access Governance is all about the right people having the right access to the right data at the right time. When that doesn't happen, one of two bad things occur. First, when the wrong people have access to key data, your organization is at risk. Second, when the right people don't have access to the data they need, the organization is operating at less than efficient levels and people go out of band to share data, which can inherently put the data at risk.

If you aren't effectively governing access to your data, you can't meet the compliance requirements your organization might be facing, and you will have challenges fulfilling audit requests or attestation needs. In addition, you won't be able to adapt to emerging and constantly evolving privacy compliance requirements.

Leading analyst firms have identified a convergence with the Data Access Governance (DAG), Identity and Access Management (IAM), and Identity Governance and Administration (IGA) market segments. Without going into a detailed definition of each market segment, it's sufficient to say that what the analysts have determined is that a data access governance strategy ultimately comes down to individual users, their roles in organizations, and their access to data based on their roles.

Traditionally, leading IAM/IGA products have focused on governing data access to applications and the data housed and controlled by those applications. But what about the data outside the scope of applications? Analysts have concluded that the elephant in the room is the lack of governance for organizations' unstructured data, that is, file-based data that makes up more than 80 percent of organizations' total data.

Recent news stories have demonstrated the devastation that can happen when hackers or other unauthorized individuals gain access to personal and sensitive information located within the unstructured data located on storage devices on the network. That's why everyone from Chief Privacy and Data Protection Officers, to IAM/IGA developers, to CSOs are now making unstructured data a focus of their data access governance and data privacy compliance strategies.

Implementing Effective Data Access Governance for Privacy Compliance

The elements of an effective DAG solution for privacy compliance are simple but challenging. Here are a few strategic considerations:

- A key first step to getting control over data sprawl is to implement data discovery, to understand what data and risk the organization is holding. Voltage Data Discovery identifies, analyzes, and classifies unstructured data
- Identifying data location, value, and risk, provides the insight to enable effective action on data—whether for defensible deletion, protection, or data access governance
- The next step is to perform some level of permissions cleanup on high value target areas. The entropy factor of security in unstructured data is typically high, especially in large, complex organizations with storage environments that have evolved over a long period of time or one in which management turnover has occurred.
- Second, the ability to apply policy automatically to data is critical. Again, identity and role are a central driver here, so the ability to drive security to data though identity is imperative.
- Next, you need to monitor security to key data areas and take appropriate action. This could involve notifying data owners of changes to security or remediating changes in certain situations.
- Last, periodic certification of access to data is required. It is vital that the business-level data owners who understand the access needs of individuals and are ultimately responsible for the stewardship of the data conduct these certification reviews.

Solution

Fortunately, CyberRes long ago recognized the risks inherent in storing unstructured data and developed industry-recognized tools for identifying what data you are storing, who has access to it, and an automated means of remediating access permissions, moving data, and even disposing of it as specified by regulations or policies.

CyberRes is addressing the challenges of the larger Data Access Governance market with a set of integrated products with proven technology.

File Analysis Suite

CyberRes Voltage File Analysis Suite controls access to data stored in the network file system according to identity and role. With Voltage FAS, organizations are equipped to extend identity-based security and access management to the largest and oftentimes most vulnerable data segment—unstructured data. Voltage FAS automates access assignments and remediation, prevents unauthorized access, mitigates risk, and helps to meet attestation for unstructured data access compliance.

Voltage File Analysis Suite is governed by Identity-Driven policies that you define. User home folders and group folders can be provisioned automatically with the access permissions that are specified in the policy.

Auxiliary storage policies can be the means of provisioning and protecting files with personally identifiable information (PII) from users who should not have access to that information. For example, when John Taylor joins the organization and is provisioned a network home folder through an Identity-Driven policy, an Auxiliary Storage policy will create a separate John Taylor folder in the H.R. Department share where files containing PII can be stored safely and accessed only by members of the H.R. group.

In addition to Identity-Driven policies, Target- Driven policies can be set for any network folder or share. Target-Driven policies can provide additional risk mitigation through data location remediation, data access restrictions, recovery after data loss or corruption, and automated data owner notification when access permissions have changed.

Many organizations must comply with security regulations that require vigilance in user access to areas of the network containing personal data or other restricted or sensitive information, so being notified of any changes to access permissions can be critical. Security Notification policies let you specify the shares or folders to be analyzed, the frequency of this analysis through scheduled scans, and the data owners who are to be notified when changes in access permissions take place.

Security Notification policies notify data owners of:

- Direct or indirect changes involving who can access designated data
- The details of those changes

Direct access changes involve permissions modification while indirect changes might involve changes in role in the identity system itself. Both of these levels ultimately impact who can access the data and the data owner might want to know about these changes.

Lockdown policies restrict access permissions to a specific set of individual users either through direct assignments or group memberships. Fencing policies set access permissions to authorized users and groups based on roles that can change over time.

Reporting

CyberRes Voltage File Analysis Suite provides comprehensive reporting and analysis of user access to data stored on the network file system. With Voltage FAS, administrators can determine quickly if their organization is in compliance with regulations pertaining to security and access to unstructured data.

Voltage FAS reports on:

- Assigned user permissions for all folders and subfolders from a specified file system path
- All users who can access a specific network folder
- All of the network folders that a particular user can access
- Files containing personal or sensitive information
- The owners of individual files
- And much more

In the process, Voltage FAS mitigates the risk of unauthorized access, noncompliance, and data breaches.

These capabilities enable organizations to meet both internal and external security goals and quickly and efficiently respond to audit and attestation challenges.

Voltage Data Privacy and Protection

Voltage File Analysis Suite is a file analysis solution enables organizations to reduce information risk, ensure data privacy, analyze, optimize and secure employee access to critical data that drive and protect the business quickly and efficiently. Voltage FAS ensures data protection and data preservation while mitigating the risk associated with managing sensitive data. Voltage FAS drives operational excellence initiatives improving data visibility, data minimization efforts,

CyberRes recognized the risks inherent in storing unstructured data and has developed industry-recognized tools for identifying what data you are storing, who has access to it, and the automated means of remediating access permissions, moving data, and even disposing of it as specified by regulations or policies.

Contact us at **CyberRes.com**
Like what you read? Share it.

data privacy readiness, and data protection while addressing long-term preservation for high-value data (e.g., contracts, intellectual property, patents, etc.) and sensitive data (e.g., PI/ PII, PCI, PHI, etc.).

Learn more at **www.microfocus.com/en-us/cyberres/data-privacy-protection/data-access**

CyberRes
A Micro Focus Line of Business