opentext™ | Cybersecurity

Ten Reasons for Deploying Voltage Data Access Governance

Data Access Governance (DAG) is a market segment that focuses on identifying and addressing malicious and non-malicious threats coming from unauthorized access to sensitive and valuable unstructured data. Voltage Data Access Governance includes File Reporter and File Dynamics that, together, not only address DAG objectives, but deliver additional powerful data management capabilities that data and security officers are in need of today.

Anyone familiar with data storage has undoubtedly heard the term "exponential" data growth. A thesaurus offers synonyms such as "aggressive" or "epidemic," but the word's origin is "exponent"—meaning a positive number raised to a power. So, while today's IT department employees describe their stored data in the "petabytes," they're really talking about 1,024 terabytes or 1015 bytes. Chances are, your handheld calculator can't display that number without using scientific notation. The bottom line is, managing very large data (and in this example, 1,000,000,000,000,000 bytes) is incredibly challenging!

That's why Chief Data Officers (CDOs), Data Privacy Officers (DPOs), and Chief Security Officers (CSOs) are looking for tools such as Voltage Data Access Governance to help Identify the data they have, learn who has access to it, determine if it is secure, determine if it is relevant, and then take automated remediating actions to address these findings.

Voltage Data Access Governance by OpenText™ provides an extensive set of data reporting and management capabilities to address the needs of CDOs, DPOs, and CSOs. Here are ten:

1. **Identifies data and where it's located.** Identify what files are being stored across your entire enterprise, including files stored in Microsoft 365 cloud libraries. Learn which files are relevant and which files should be archived or deleted. Determine if sensitive and high-value files are being stored in secure locations.

2. **Identifies who has access to data.** Determine all users who can access your sensitive and high-value data storage shares and folders, their specific access permissions, and how their access is derived.

3. **Corrects access permissions.** Security policies restrict access to locations storing sensitive and high-value data to only authorized users. If a network administrator mistakenly alters these access permissions, the changes are automatically revoked.

4. **Cleans up data.** Policy settings and grooming rules not only remove ROT (redundant, obsolete, and trivial files), but can archive or delete files that haven't been accessed for a set amount of time, files that meet or exceed a specific size, files with specific file extensions, and other specifications.

Voltage Data Access Governance comprises our OpenText™ File Reporter and OpenText™ File Dynamics products and provides:

- Reporting on Microsoft network- and Microsoft 365-stored data
- Permissions reporting for individual network users or file shares and folders
- Graphical analytics for quickly identifying data storage issues
- Built-in and custom-query reporting
- Identity-driven policies for managing the lifecycle of user and group storage
- Target-driven policies for managing individual file shares and folders
- Security policies that prevent unauthorized access
- And much more

CDOs, DPOs, and CSOs are looking for tools like Voltage Data Access Governance to help identify the data they have, learn who has access to it, determine if it is secure, determine if it is relevant, and then take automated remediating actions to address these findings.

Connect with Us
www.opentext.com

5. **Determines data storage costs.** Storage cost reports display calculated storage costs according to charges you establish per MB, GB, or TB. You can use these reports to determine which users or groups are costing you the most through their storage use.

6. **Prevents certain file types from being stored.** Restrict your network storage areas from being a storage repository for personal photos, music, videos, or other non-work files by removing them through a grooming operation.

7. **Migrates data.** Easily migrate shares, folders, or all of the files stored on a server to a new location on your network by simply changing the target path in the policy and then initiating the migration.

8. **Performs load balancing.** Automatically balance the amount of stored data for policy-managed data across multiple servers through load distribution settings.

9. **Helps you understand your network's growth.** Trending reports can show the rate at which content on network shares is growing. You can then address this growth by determining when you will need to purchase additional network storage or by cleaning up old data through automated policies.

10. **Identifies duplicate files.** A principal objective for any organization that is determined to reduce stored network data is to eliminate duplicate versions of files. Two types of duplicate file reports, including one conducted through content-based hashes, indicate duplicate versions of files and their locations.

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

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.