Voltage Fusion Data Monitoring: Improving Data Security and Privacy Posture

In today's data-driven world, organizations face increasing challenges in protecting their sensitive information from unauthorized access, ensuring compliance with global data privacy regulations, and maintaining a robust data security posture. Monitoring access, permissions, and data use is critical to help mitigate the risk associated with these challenges.

By implementing effective strategies for data access governance and employing robust database activity monitoring solutions, businesses can enhance their data security, achieve regulatory compliance, improve data quality, streamline operations, and reduce business risks. Both data access governance and database activity monitoring play a critical role in managing data securely and augmenting an organization's overall data security posture.

Benefits of Data Access Governance

Data access governance involves managing and controlling access to sensitive data within an organization. By implementing robust data access governance practices, businesses can enjoy several key benefits:

- **Enhanced Data Security:** Effective data access governance ensures that only authorized personnel can access sensitive information. Organizations can significantly reduce the risk of data breaches and unauthorized data exposure by implementing granular access controls, role-based permissions, and robust authentication mechanisms.
- **Improved Regulatory Compliance:** Data access governance is crucial in meeting regulatory requirements, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). Organizations can demonstrate compliance by enforcing data access policies, tracking data usage, maintaining audit trails, and avoiding fines and reputational damage.
- **Better Data Quality and Integrity:** With data access governance, organizations can establish data stewardship practices and ensure data accuracy, completeness, and consistency. Businesses can maintain high-quality data by defining data ownership, implementing data validation checks, and monitoring data usage, enabling informed decision-making and operational efficiency.

Importance of Data Access Governance

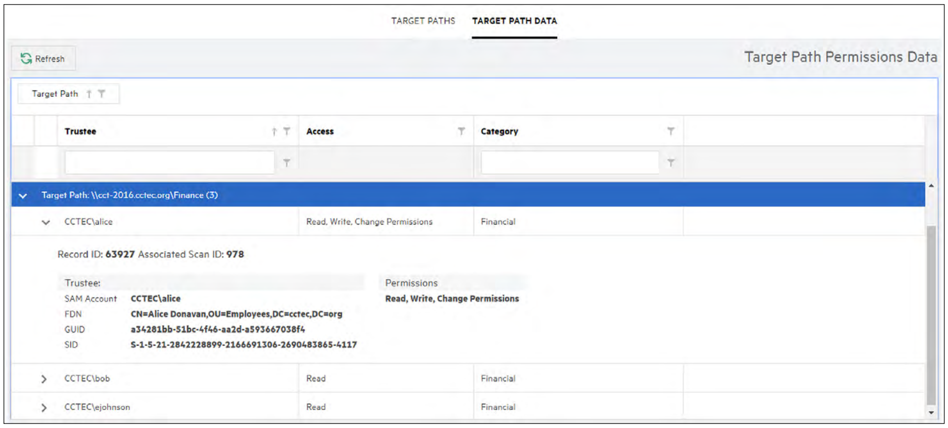
Data access governance is vital for organizations due to the following reasons:

- **Protection against Internal Threats:** Insider threats, intentional or unintentional, pose significant risks to an organization's data security. Data access governance allows organizations to mitigate these risks by implementing controls that restrict access to sensitive data based on user roles, responsibilities, and business needs. By monitoring user activities and access privileges, organizations can detect and prevent unauthorized data access or misuse of rights, minimizing the risk of internal data breaches.
- **Safeguarding Sensitive Information:** Organizations deal with a vast amount of sensitive data, including customer information, financial records, and intellectual property. Data access governance ensures that only authorized individuals can access and modify this critical information, reducing the risk of data leaks, fraud, and unauthorized disclosure. By implementing stringent access controls, organizations can strongly defend against external and internal threats to sensitive data.
- **Reporting and Analytics:** Effective data access governance requires the ability to identify what is being stored across the enterprise, who has access to it, and when necessary, perform detailed analytics on this data.
- **Effective data management practices:** Unstructured data sprawl adds to the complexity of managing sensitive data across a vast enterprise. Data access governance helps organizations manage file shares, reduce the risk of exposed files, and remediate access to orphan files that pose potential data loss and breach risks.

Benefits of Database Activity Monitoring

Similarly, in the structured data world, database activity monitoring involves real-time monitoring and analysis of database activities to identify potential security threats, policy violations, and suspicious behavior. The benefits of implementing database activity monitoring include the following:

- **Early Threat Detection:** Database activity monitoring provides real-time visibility into database activities, allowing organizations to promptly detect and respond to potential security threats. Organizations can identify unauthorized access attempts, data breaches, or misuse of privileged accounts by analyzing patterns, abnormal behavior, and access anomalies. Early threat detection enables proactive measures to mitigate risks, preventing the loss of sensitive data and potential financial and reputational damage.
- **Compliance and Auditing:** Database activity monitoring facilitates compliance with regulatory requirements by providing detailed audit logs and reports. Organizations can demonstrate compliance with industry standards and regulations by monitoring and reporting on user activities, data access, and modifications. Database activity monitoring solutions often offer built-in reporting functionalities, simplifying the generation of compliance reports and reducing the effort required for audits.
- **Incident Response and Forensic Analysis:** In the event of a security incident, database activity monitoring aids in incident response and forensic analysis. The ability to monitor and record all database activities allows organizations to reconstruct events, identify the root cause of a breach, and understand the scope of the incident. This information is invaluable for conducting thorough investigations, remediation efforts, and implementing measures to prevent similar incidents in the future.



	Trustee	Access	Category
Target Path: \\cct-2016.cctec.org\Finance (3)			
	CCTEC\alice	Read, Write, Change Permissions	Financial
	CCTEC\bob	Read	Financial
	CCTEC\ejohnson	Read	Financial

Record ID: **63927** Associated Scan ID: **978**

Trustee:		Permissions
SAM Account	**CCTEC\alice**	**Read, Write, Change Permissions**
FDN	**CN=Alice Donavan,OU=Employees,DC=cctec,DC=org**	
GUID	**a34281bb-51bc-4f46-aa2d-a593667038f4**	
SID	**S-1-5-21-2842228899-2166691306-2690483865-4117**	

Figure 1. Voltage Fusion DAG Target Path Data

- **Insider Threat Detection:** Database activity monitoring plays a crucial role in identifying and mitigating insider threats. Organizations can detect unusual or suspicious behavior by monitoring user activities and database interactions, such as unauthorized data access, unauthorized privilege escalations, or data exfiltration attempts. Prompt detection and response to insider threats can prevent significant data breaches and protect sensitive information from malicious insiders.
- **Operational Efficiency and Performance Optimization:** Database activity monitoring also offers benefits beyond security. It provides insights into database usage, performance metrics, and query optimization opportunities. Organizations can identify and address performance bottlenecks by analyzing database activity, optimizing resource utilization, and enhancing overall system efficiency, improving application performance and user experience.

Importance of Database Activity Monitoring

Database activity monitoring holds significant importance for organizations due to the following reasons:

- **Proactive Threat Detection and Response:** In today's rapidly evolving threat landscape, organizations must adopt proactive measures to detect and respond to threats. Monitoring provides real-time visibility into database activities, enabling the detection of unauthorized access attempts, data breaches, or suspicious behavior. By monitoring database activities, organizations can take immediate action to mitigate risks, minimize the impact of security incidents, and prevent further compromise of sensitive data.
- **Compliance and Regulatory Requirements:** Compliance with industry standards and regulatory requirements is critical for businesses operating in various sectors. Database activity monitoring plays a pivotal role in meeting compliance obligations by providing detailed audit logs and reports on database activities. It enables organizations to demonstrate adherence to regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), or other industry-specific compliance frameworks. Organizations can ensure they meet security and data privacy requirements by continuously monitoring and auditing database activities.
- **Insider Threat Mitigation**: Insider threats pose significant risks to organizations, as employees or authorized individuals with access to sensitive data may intentionally or unintentionally misuse or compromise it.

Database activity monitoring helps identify potential insider threats by monitoring user activities and detecting unauthorized or suspicious behavior. By promptly detecting such threats, organizations can initiate appropriate response measures, investigate the root causes, and take preventive actions to mitigate the risks associated with insider threats.

- **Forensic Analysis and Investigation:** Detailed information about database activities is crucial for practical forensic analysis and investigation in a security incident or data breach. Database activity monitoring provides a comprehensive record of all interactions with the database, allowing security teams to reconstruct events, trace the origin of the incident, and identify the extent of the impact. This information is invaluable for understanding the scope of the breach, assisting law enforcement agencies, and taking measures to prevent similar incidents in the future.
- **Continuous Improvement and Optimization:** Database activity monitoring offers insights into database performance, usage patterns, and query optimization opportunities. By analyzing the monitored activities, organizations can identify areas for improvement, optimize database configurations, and fine-tune query execution plans. These insights lead to enhanced operational efficiency, reduced response times, and improved overall database performance, ultimately benefiting the organization's productivity and customer experience.

Organizations can proactively address security threats, maintain compliance, mitigate insider risks, conduct effective investigations, and optimize their database environments by emphasizing the importance of database activity monitoring.

Voltage Fusion Data Monitoring Solutions

Data security posture management is critical to any organization's cybersecurity strategy. Voltage Fusion by OpenText, Voltage Data Access Governance by OpenText and Database Activity Monitoring play integral roles in helping customers improve their data security posture. Our solutions ensure that sensitive data remains secure, compliant, and protected, reducing the risk of data breach, ensuring regulatory compliance, and driving operational efficiencies. Moreover, Voltage Fusion by OpenText™ establishes a strong foundation for a robust data security framework by discovering and classifying sensitive data, safeguarding sensitive and personal information, and enabling secure information sharing. By embracing these practices, businesses can bolster their security posture, protect their valuable assets, and instill trust among customers and stakeholders in an increasingly data-centric world.

Voltage Fusion Data Security Platform

Voltage Fusion enables organizations to quickly find, classify, and protect sensitive and high-value data. Voltage Fusion provides complete visibility and insight across structured and unstructured data silos, helps contain data management costs while delivering actionable analytics that improve efficiency, data quality, and data privacy compliance. Contextually aware, AI-driven grammars reduce false positives and quickly identify high-value assets (e.g., contracts, intellectual property, patents, etc.) personal and sensitive data types (e.g., PI/ PII, PCI, PHI, etc.). Voltage Fusion supports data masking/ anonymization, 3rd party tagging including Microsoft Information Protection (MIP) for data protection along with litigation hold and long-term retention management to meet data preservation requirements.

Voltage Fusion Data Access Governance

Voltage Fusion Data Access Governance (DAG) is a solution that adopts an identity-centric approach to safeguarding sensitive unstructured data. With Voltage DAG, organizations can establish access policies that align with specific roles, guaranteeing that only authorized users with appropriate roles can access data when needed. Voltage DAG offers a comprehensive set of features including change notifications, lifecycle management, security lockdown, and security fencing. Voltage DAG includes reporting capabilities enabling network administrators to easily identify enterprise data that needs to moved, secured, retired, and more.

Connect with Us
www.opentext.com

Voltage Fusion Database Activity Monitoring

Voltage Fusion Database Activity Monitoring (VDAM) is a powerful solution that monitors all database activities within an organization. VDAM actively monitors in real-time and generates alerts for any policy violations. VDAM works with Oracle DB, Microsoft SQL, IBM DB2, MongoDB, MySQL, and many more. VDAM's monitoring capabilities encompass a wide range of activities, including database administrator actions and application transactions such as data manipulation, schema modifications, access control changes, and transaction control. With VDAM, organizations can enable faster IT modernization and contain costs by retiring dormant data, improve privacy posture through insights into applications interacting with sensitive data, and support green-IT and sustainability efforts.

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

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.

761-000113-002 | O | 10/23 | © 2023 Open Text