Shadow Access to Your Data: What It Is and Why It's Dangerous

As organizations invest heavily in data infrastructure to fuel innovation and decision-making, a growing concern emerges—shadow access to data. As more users and applications seek connectivity to databases, data warehouses and data lakes, challenges arise due to the frequent lack of native IAM integration for privileged users and use of service accounts by applications. This presents a formidable obstacle for organizations striving to monitor, comprehend, and control data access at its foundational layer. In this white paper, we dissect the nature of shadow access, outline its risks, and advocate for a comprehensive solution to address this challenge.

Understanding Shadow Access

Shadow access refers to invisible interactions with an underlying service, often occurring outside the purview of central IT and security controls. In the modern data stack, shadow access can arise for both users and applications.

Shadow Access by Direct Users

Direct users refers to anyone with privileged or restricted access to the data repository using a username and password. They could be accessing the repository using a command line interface or a thick client (e.g. DBeaver) or a web client (e.g. PgAdmin).

The core issue in this case is that a majority of databases lack native SAML or OIDC support. As a consequence, organizations usually give database and data warehouse access to users using one of the two following approaches:

1. **Shared accounts:** an account gets created in the database, and its credentials get stored in a PAM (Privileged Access Management) tool. Users then grab those credentials from PAM when needed, using some organization-specific workflow.

This scenario results in the shadow access problem - since attributing a given command to its corresponding user is complex and requires looking through multiple different logs and traces. Also, implementing any specific access privileges is challenging because that account can be used by multiple people.

2. **Ad-hoc user accounts:** In this case the team members go through the toil of creating and maintaining individual user accounts for database access. This quickly becomes untenable and results in the joiners-movers-leavers problem - keeping the accounts and their privileges updated often falls out of sync as the organization evolves creating security and compliance risks.

Shadow Access by Application Users

Application user refers to anyone consuming data through a visualization tool (e.g. Looker), a computational application (e.g. notebook) or a home grown tool. In this case the user may authenticate into the app (using for instance SSO), and the app then accesses the data repository using credentials for a service account on their behalf. The app users essentially impersonate the app when running commands against the data repository.

This is a common scenario for shadow access. Historically this was less significant because only a limited number of users accessed data through BI tools which ran in very constrained environments. However, with the paradigm shift towards data-driven organizations, the user base has expanded significantly and they use cloud-based applications to access data.

> A particularly egregious case of shadow access for application users is someone using application credentials to directly access the data repository. This is more common than one would expect - application credentials are often available within the application or some configuration file in plaintext, and are easily accessible to the developers or administrators of the application. In our experience working with security leaders in the financial services sector, this is often a key area of concern for them.

Challenges Resulting from Shadow Access

The prevalence of shadow access in data repositories introduces technical hurdles that translate into the following risks for organizations:

- **Security Blind Spots:** Shadow access creates unmonitored points of entry into a service, leading to security blind spots where unauthorized access can go undetected. This is particularly concerning given the critical nature of data repositories.
- **Audit Risks:** In the absence of clear visibility and monitoring mechanisms, audit trails become incomplete or unreliable. This introduces audit risks, making it challenging for organizations to provide accurate and comprehensive records of data interactions, potentially leading to compliance issues.
- **Inability to Provide Least Privilege:** The lack of identity-based controls and oversight complicates the implementation of the principle of least privilege. Organizations struggle to ensure that users and applications have the minimal access necessary for their roles, heightening the risk of data exposure and misuse.
- **Lack of Assurance:** With shadow access, there is a notable absence of assurance regarding the authenticity of data requests. This has the potential to erode trust amongst customers, not only for B2B businesses but also B2C businesses.
- **Increased Attack Surface:** Unregulated access points contribute to an expanded attack surface. This enlarges the avenues for malicious actors to exploit vulnerabilities, making it imperative for organizations to address shadow access to reduce their susceptibility to cyber threats.

Shadow Access Renders Existing Solutions Ineffective

Contemporary security programs increasingly incorporate a dedicated data security component. This component, comprising one or more of Data Activity Monitoring (DAM), Data Security Posture Management (DSPM), and Data Activity Governance (DAG), forms a critical bulwark against unauthorized access and data breaches. However, shadow access introduces serious challenges for these integral components.

Database Activity Monitoring

DAM solutions provide continuous monitoring and analysis of all user actions, queries, and transactions within the data infrastructure, flagging potential threats, unauthorized access, and anomalous behaviors. DAM solutions play a critical role in maintaining data integrity, ensuring compliance with industry regulations, and fortifying defenses against evolving cyber threats.

Shadow access undermines DAMs by preventing precise monitoring and creating blind spots. This compromises the system's ability to detect unauthorized or unusual activities promptly.

Data Security Posture Management

DSPM products help organizations protect their data by providing visibility into where sensitive data is stored, who has access to it, and how it is being used. DSPM products also help organizations identify and remediate security risks, comply with data privacy regulations, and ensure that their data is protected from unauthorized access, modification, or deletion.

Shadow access introduces significant hurdles to the efficacy of DSPM which relies on comprehensive visibility into access privileges, and usage to ensure robust protection.Shadow access not only creates blind spots but also renders privilege inspection meaningless when it comes to shared accounts and service accounts.

Data Access Governance

DAG products help organizations manage and control access to their data by providing a centralized platform for managing user access permissions, tracking data usage, and enforcing data security policies. The concept is very broadly applicable, but often focused on data products that connect to data warehouses and data lakes for reporting.

The effectiveness of DAG products, designed to centralize control over data access, faces a substantial challenge with shadow access which creates gaps in the centralized control model. It disrupts the accurate tracking of who accesses data and how it is utilized, compromising the essence of DAG's role.

About

Cyral provides controls for privacy, compliance, governance and protection thereby reducing risk, complexity, and cost for managing structured data. The Cyral platform discovers data, unifies access controls for users and applications, enables fine-grained authorization policies and provides complete monitoring and reporting. This comprehensive coverage enables risk-based governance, limits the blast radius of data-related incidents and reduces overhead and costs. Cyral's technology allows customers to implement data security controls using their existing, centralized entitlements, thereby simplifying administration and automating remediation. Customers use Cyral to accomplish least privilege, data minimization, spillage prevention and Zero Trust.

For more information, visit **www.cyral.com** or follow **@CyralInc** on X.