It’s Time for Universal Data Authorization Standards

Data-driven organizations face the challenge of managing extensive data volumes dispersed across diverse data stores. The rapid transition to cloud computing has exacerbated this challenge, making data more accessible to a wider audience. As a result, companies are increasingly leveraging their enterprise data platforms to extract valuable insights. These insights, in turn, play a pivotal role in enhancing decision-making processes, optimizing customer interactions, and enriching employee experiences.

However, many of these companies struggle to answer a critical security question: “Who has access to my data, and how did they get it?” Each data store has its own authorization model, and until the various data sources used by enterprises share a common approach when it comes to authorization, companies struggle to maintain authorized access across their databases, data warehouses, and data lakes, placing sensitive data at risk.

As the breadth and complexity of data grows, so does a company’s vulnerability. Even enterprises with robust data security and compliance practices in place are falling short when it comes to data access and authorization. Considering that three-quarters of all breaches are linked to a human element (including privilege misuse), who can access what data (and for how long) remains a central, often overlooked issue.

A universal data authorization standard would make a big impact.

Why is a universal data authorization standard needed?
Standards are nothing new when it comes to data and technology. W3C standards define aspects of the web, search engines, and website development. Matter is an open-source connectivity standard for smart home and Internet of Things (IoT) devices, which aims to improve compatibility and security. ISO/IEC 27701 is the first international standard for privacy information management.

Similarly, a universal data authorization standard would make retrieving and using data more accessible for those with the appropriate authorization, while safeguarding sensitive data.

Specifically, a universal data authorization standard would:

Enable interoperability between different systems. When data is stored and accessed using a consistent protocol, it is easier for various components of an organization’s technology ecosystem to communicate and share information.
Maintain data consistency and integrity. A universal data authorization standard that includes guidelines for how data is structured, stored, and accessed ensures that data is accurate, complete, consistent, and error-free. This is essential for making informed decisions and conducting meaningful analysis.
Ensure compliance. Lack of proper authorization puts companies at risk of non-compliance with data privacy laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). A universal data authorization standard helps organizations comply with various industry and government regulations, avoiding audits, legal issues, and potential fines.
Better protect sensitive data. Clear, enforced guidelines on who should have access to what prevents unauthorized access and reduces the risk of breach. Recently, two former Tesla employees

maliciously shared sensitive data on over 75,000 people with a German newspaper in a whistleblowing attempt. Proper data authorization standards could have prevented this. By minimizing the risk of security incidents, a universal data authorization standard also makes security awareness training easier and leads to cost savings in terms of prevention and remediation.
Improve efficiency and scalability. Developers and data analysts work more effectively with clear guidelines for accessing and manipulating data, leading to faster development cycles and improved productivity. As your organization grows and adds more systems and data sources, adherence to a standard ensures that new components easily integrate with existing ones.
How do we get there?
In an ideal world, all data vendors would come together and create a universal data authorization standard, recognizing it is in their customers' (the enterprise) best interest.

However, this just isn't realistic. For starters, standardization on the technical level is too complex. While they may draw inspiration from common access concepts like role-based attribute controls (RBAC), vendors implement these differently. Snowflake's implementation is different from BigQuery's, which is different from Redshift's, and so forth. It's also not in the best interest of the data vendors' bottom line – the amount of time, effort, and money it would take to converge is prohibitive.

More realistically, market forces or policy will drive a universal authorization standard. Ultimately, the increased regulations around compliance and customers' demands for data privacy will eventually push the needle.

What steps can enterprises take in the meantime?
Until the industry embraces the critical importance of establishing a universal standard for data authorization, here are a few suggestions for what enterprises can do now, on their own:

Identify your organization's most suitable access controls by aligning them with your daily business operations and objectives. Invest in automated tools so you're not burdened with manually granting and revoking access. Incorporate time-sensitive authorization restrictions and dynamic data masking techniques to restrict data exposure to authorized personnel within defined timeframes. Enhance security further by introducing role-based access controls (RBAC) and attribute-based access controls (ABAC), enabling precise data authorization based on user attributes and contextual information.
Reference known data security and compliance standards. When creating your data authorization standards, it's important to reference available data security and compliance standards. Various organizations have developed data security standards, including the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST). There are also several data compliance standards that organizations need to comply with, depending on their location and industry. When used together with strong data access controls, these frameworks prevent unauthorized access and misuse of sensitive data and improve enterprise security practices.
Take inspiration from others. Several industries have taken steps to integrate data authorization standards into their organizations, notably government and higher ed. A visit to the CDC, EPA, Boston University, and Johns Hopkins can give you an idea of how organizations define and enforce their data access rules.
Inform your organization. Human error remains a leading cause of sensitive data misuse, as does a lack of awareness around corporate policies about handling data. Educating executives and your most junior employees about data authorization and security policies will help them stay aware.