veza

The Anatomy of a Data Breach

Protect your data by shifting the focus to authorization

Data breaches happen when sensitive data like PII or valuable proprietary information is exfiltrated from an organization's systems and networks. While breaches are usually instigated by cybercriminals, insider threats — even if only due to inadvertent privilege abuse — can also occur. Regardless of the cause, a data breach can result in non-compliance with security and privacy regulations, financial loss, and damage to your company's reputation.

A growing risk, but why now?

In modern, cloud-centric enterprises, the data substrate has shifted from on-prem to cloud. The attack surface is no longer shielded by a traditional security perimeter, which has left corporate assets increasingly exposed. The growing prevalence of attacks focused exclusively on data, such as ransomware, have heightened the need for enterprises to rethink how they approach data security. However, the tools built to secure on-prem data are no match for the challenges of a multi-cloud ecosystem spread across identity, apps, data systems, and cloud services, as they provide zero visibility into cloud-native data and do not address the proliferation of identities, such as employees, partners, contractors, service accounts, and others.

Leading causes of data breaches.

According to Verizon, privilege abuse has been a leading data breach vector for several years, with 61% of breaches attributed to the misuse of credentials. Key risk factors include:

- **Privilege abuse/over-privileged Identities**
  Giving users unneeded authorization to access and interact with data for which they have no use.

  If, via phishing or other forms of social engineering, attackers gain the credentials of a user having unnecessary privileges, they can easily get into systems and wreak havoc.

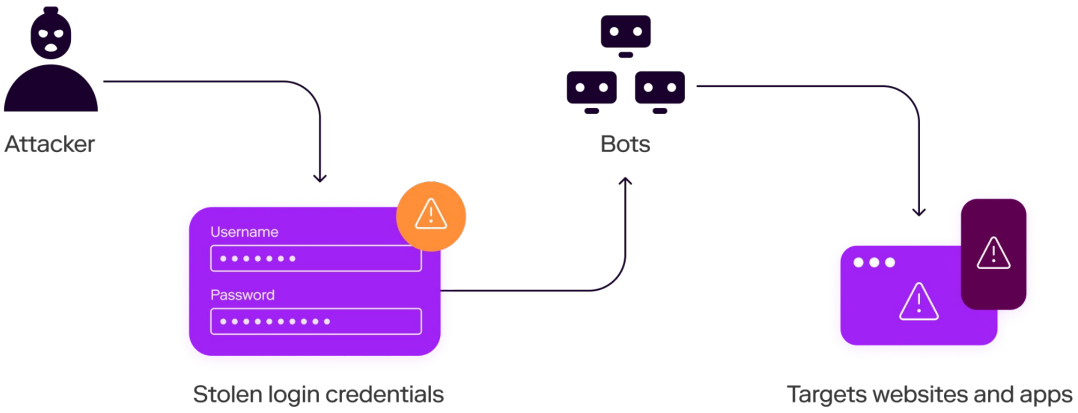
- **Complex cloud identity & access management (IAM) frameworks**
  Whether it's Amazon Web Services, Google Cloud, or Microsoft Azure, the authorization structures (users, groups, roles, permissions) for cloud IAM are extremely complex, making it challenging to keep track of various access permissions across resources.

- **Orphaned/dormant accounts**
  User accounts sometimes remain open after a user has left the company or moved to another position. If bad actors gain access to active, but unmonitored accounts, they might be able to move about the enterprise unobserved.

- **Weak or undefined data access controls/poor data governance**
  Cloud misconfigurations and lack of visibility and control over authorization; specifically effective permissions to data for each enterprise identity may contribute to data breaches.

- **Insider threats**
  Employees may steal or accidentally expose data, users sharing personal info at unsecured locations may unwittingly reveal credentials, and stolen or lost laptops and phones can leave a door open to enterprise resources.

How breaches unfold, step by step.



Infiltration/Research/Asset Targeting

Scanning for vulnerabilities and researching how to exploit them, the attacker's mission is to discover what the target has of value and how to attack. Spam can be used to deliver malware and/or include links to phishing websites for credential harvesting and internet-facing surfaces (e.g., RDP) can be exploited for network-based, backdoor intrusions and SQL injections.

Reconnaissance/Network Traversal

Once infiltration is established on a device, attackers search for systems containing valuable data. Domain controllers are a key target, as they contain a directory of user accounts and passwords. Databases are also highly sought after as they often hold sensitive customer and employee data (e.g., Social Security numbers, PII). Attackers will search for ways to compromise privileged administrator accounts and move laterally throughout the company to access a database of usernames and passwords, and then stealthily traverse the network appearing as legitimate local admins.

Exploitation/Privilege Elevation/Persistence

At this stage, the attackers are in and have likely breached the directory of user accounts and passwords. With that info they can launch brute force attacks on all admin accounts,create new ones, and up-level access permissions to get into file shares,applications, and data.

Data Exfiltration

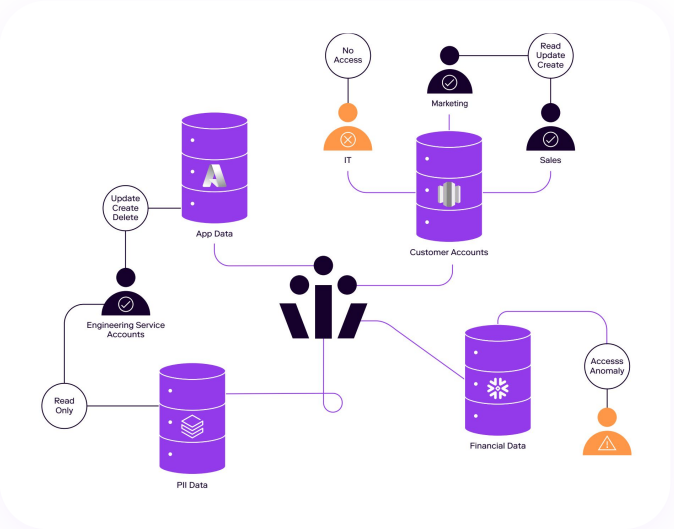
Everything is set. All the systems required to download and export data are ready to go either via FTP, email, or by moving the data to another server already under the attacker's control.

Shift your focus to authorization to limit exposure

Many organizations only place importance on securing authentication — validating user credentials through solutions like single sign-on and multi-factor authentication. However, to truly secure your data sources requires managing authorization and controlling the specific actions users can take on the data. To mitigate data breach risk, here are some steps you can take to incorporate strong data security into your strategy:

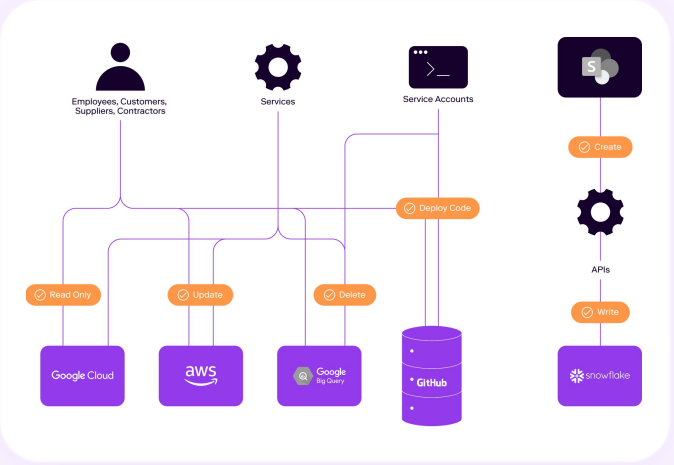
Strong Data Access Controls

Authentication is just a first step. To truly protect against data breach, you need to understand who can take action on actual data. When authorization to cloud data is scattered across disparate systems, access is either insecure or inefficient — or both. Monitoring access isn't sufficient. An identity-to-data relationship map, including non-human identities (service accounts) and granular access controls are required to enable IT and security to securely supply, manage, and remediate effective permissions on data sources. A platform-centric approach will give your teams the centralized tools needed to confidently provide or withdraw access to data sources based on enterprise rules and security protocols.



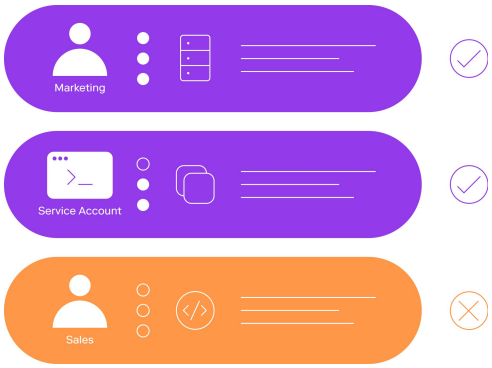
Least Privilege for Data

Implement a solution based on the least privilege principle, which limits individual user privileges only to data that is essential for fulfilling their function — the helpdesk does not need access to HR data, nor does sales need to access source code. Control authorization on a need-to-know basis to minimize access to sensitive data and place stringent controls on highly privileged administrative accounts. Consolidate permissions as much as possible based on user roles and identities.



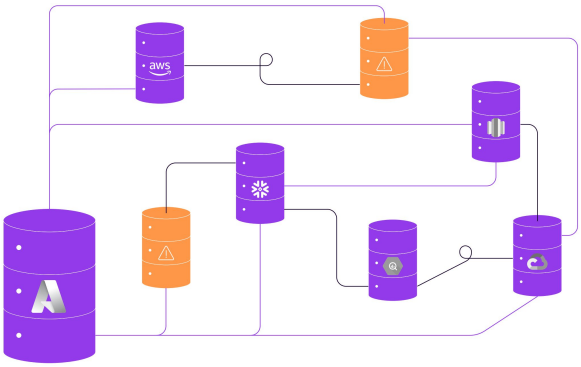
Access & Entitlement Reviews

Examine log activities and conduct audits to see who has access to specific data resources (i.e., tables/columns in Snowflake and libraries in SharePoint) and how frequently they access these resources. Manage access for human and non-human identities (service accounts and principals) and limit the number of users with administrative privileges to data. Search for, investigate, and eliminate orphaned and unused accounts and accounts that may have been created stealthily by intruders.



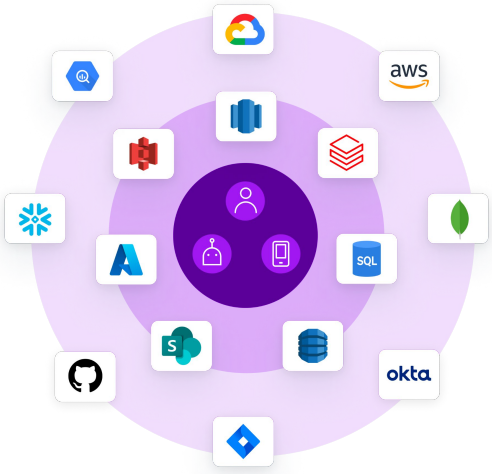
Data Governance

Implement a solution that enables you to consistently manage data access across the entire enterprise, including establishing standards for data distribution/sharing policies. A strong governance program leads to reliable and repeatable data security practices, and enables the streamlining of audits and documentation required to comply with privacy regulations and global compliance standards.



Visibility/Data Discovery & Classification

Implement a solution that provides visibility over where your data resides and who is authorized to take action on it. Traditional security solutions weren't built for the massive scale of multi-cloud data, resulting in blind spots that make it difficult to identify what needs to be protected.

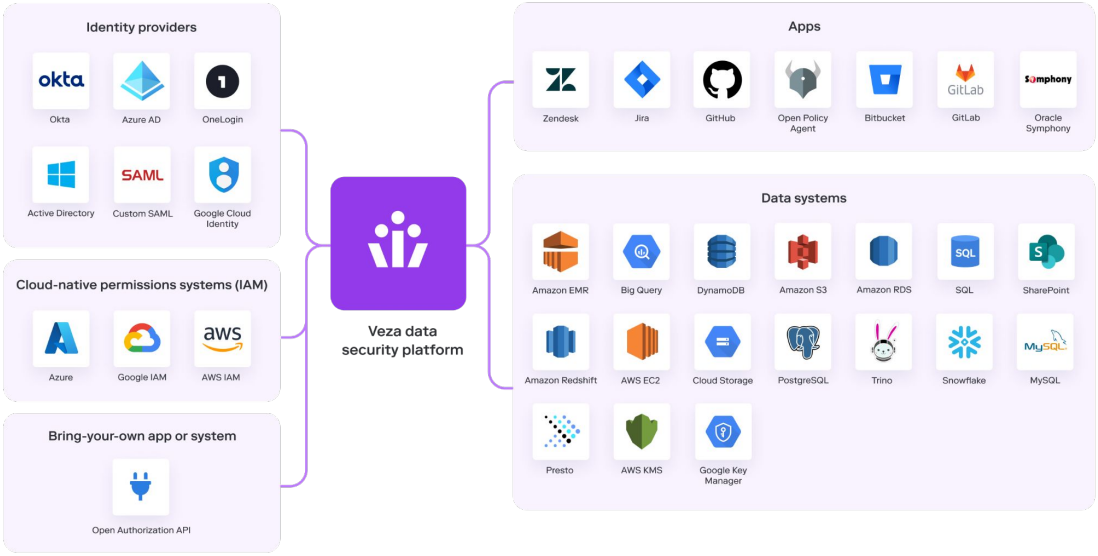


Veza - data security built on the power of authorization

In today's multi-cloud era, organizations face significant data security challenges, including implementing least privilege principles, conducting access and entitlement reviews, and managing data governance. Veza empowers organizations to understand and control who can and should take action on what data, bringing the power of authorization to data security — in effect, redefining zero trust security through data. Our data security platform helps you manage authorization for any enterprise identity — human or nonhuman — to any resource, be it data, applications, or cloud services.

Veza integrates with key identity providers (Okta, Azure AD), cloud IAMs (AWS, GCP, Azure RBAC), apps (Github, JIRA, Bitbucket, etc.), and data systems (Snowflake, Redshift, Google BigQuery, Presto, Trino, and more). Our agentless solution translates highly complex, system-specific authorization structures into a common language of effective permissions — all delivered through a CRUD (Create, Read, Update, Delete) interface in a single control plane. Think of it as a unified data authorization graph.

While there are innumerable data security solutions available today, only Veza can answer the fundamental question of who can and should take what action on what data, which is the key to curbing privilege abuse and achieving least privilege and effective cloud data governance.



To learn more about how Veza fits into your data security initiatives, visit us at www.veza.com.

• sign up for a free trial

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the modern era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.