veza

Authorization - The Missing Piece of Ransomware Protection

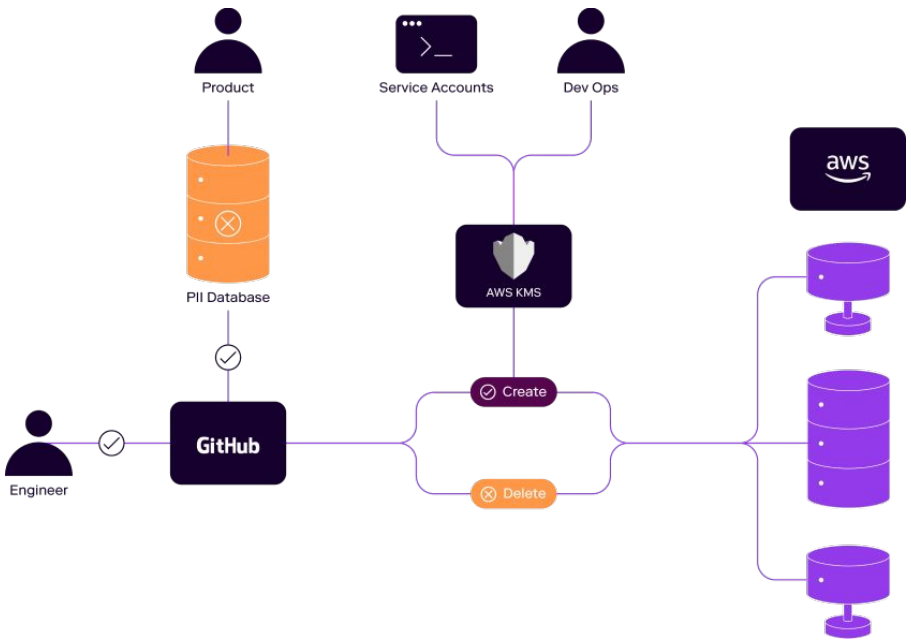
Tackle ransomware head-on by enforcing least privilege access to data

The eruption of ransomware is hardly a recent development—it's been nearly a decade since CryptoLocker injected the term into the vocabulary of cybersecurity. Yet even with cumulative global cybersecurity spending expected to reach $1.75 trillion from 2021–2025, the impact of ransomware continues to grow.

The fact is, any defense is only as strong as its weakest point. While organizations invest heavily in measures such as antivirus software, multi factor authentication (MFA), and vulnerability management, they often overlook a critical element: the data permissions granted to their own user accounts.

From misconfigured or dormant identities, to over-permissioned accounts, hackers depend on lapses and blind spots in their victims' data security practices to achieve their objectives.

Without clear visibility and control over enterprise-wide data authorization—which identities can take what actions on what data—companies remain all too vulnerable to a devastating breach.



Why ransomware works—and why most security strategies don't

Ransomware has soared in popularity among cybercriminals for good reason. With the growing sophistication of malware and the rise of ransomware-as-a-service, these attacks become easier and more effective to launch every day. They're also highly profitable. Even a partial restoration of compromised data from a backup can be a lengthy and costly process, and a full recovery can be difficult or impossible to achieve.

With the clock ticking, and business damage already mounting, victims often choose to pay up. And as hackers are fully aware, most enterprises are simply not well enough protected against ransomware. Even multi-layered security strategies fail to focus on the right measures and controls, leaving confidential data exposed to risk.

It's not that organizations neglect or fail to prioritize ransomware protection—in fact, this is a top priority for every CISO.

Common preventative measures include:

- Antivirus software to screen and quarantine suspected malware
- Endpoint detection and response (EDR) technologies to monitor for suspicious activity
- Adaptive access, paired with multi-factor authentication (MFA), to counter credential theft and tailor privileges to the device type and network connection being used
- Regular software updates and security patches to close known vulnerabilities
- User training on email security, password hygiene, and phishing prevention
- Identity security software to to discover abnormal and risky behavior by users based on user and entity behavior analytics (UEBA)

During an attack, a victim can take steps such as removing infected devices from the network and shutting down external access. Recovery efforts focus on restoring data from backups—if they are available.

Yet even with all these strategies and precautions in place, ransomware attacks remain a pervasive and growing threat. Consider:

- Ransomware attacks in the U.S. and around the world doubled in 2021
- More than one-third of global organizations were the victim of ransomware in 2021
- Global ransomware damage costs are projected to exceed $265 billion by 2031

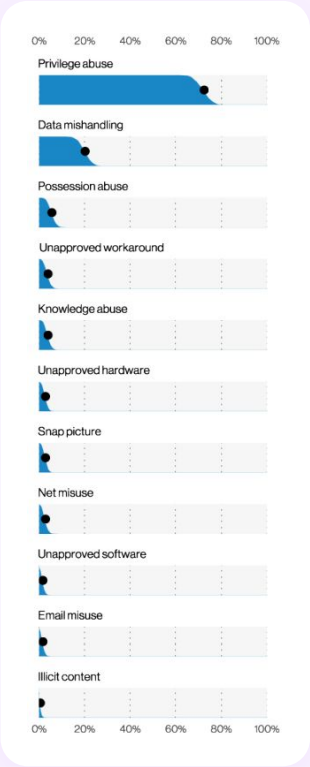
The ransomware security puzzle clearly has missing a piece.

Veza's approach to combat ransomware: the power of authorization

While organizations are working overtime to prevent ransomware from entering their environment—a losing battle, in many cases—they overlook one simple point: In order for an attack to succeed, the threat actor needs to use a compromised user account to move through the network and access its target data. Without this access, the ransomware group behind the attack is unable to achieve its goal and the attempted extortion falls flat.

The bad news is that even when access to sensitive information is limited to a subset of accounts, most organizations don't actually know which accounts these are, or which data they have what level of permissions for. This makes it impossible to effectively enforce the principle of least privilege—a critical element of ransomware protection. Simply put, **you can't protect what you can't see.**

Veza closes the authorization gap by helping organizations understand who has access to what data, with what privileges. With Veza's data security platform, built on the power of authorization, organizations can:



2021 Verizon Data Breach Investigations Report - privilege abuse is the #1 misuse variety in breaches

Gain complete visibility into identity-to-data relationships

Organizations can easily understand exactly what accounts can take what actions across all their data systems, on-prem and in the cloud. For example, an Okta admin may have read-only permissions in Snowflake, but full access to delete code repositories in GitHub. With Veza, organizations can identify the full chain of authorization for any account, human or non-human. Having identified accounts with legitimate privileged access, the organization can use this visibility to prioritize and plan protections to reduce their associated risk.

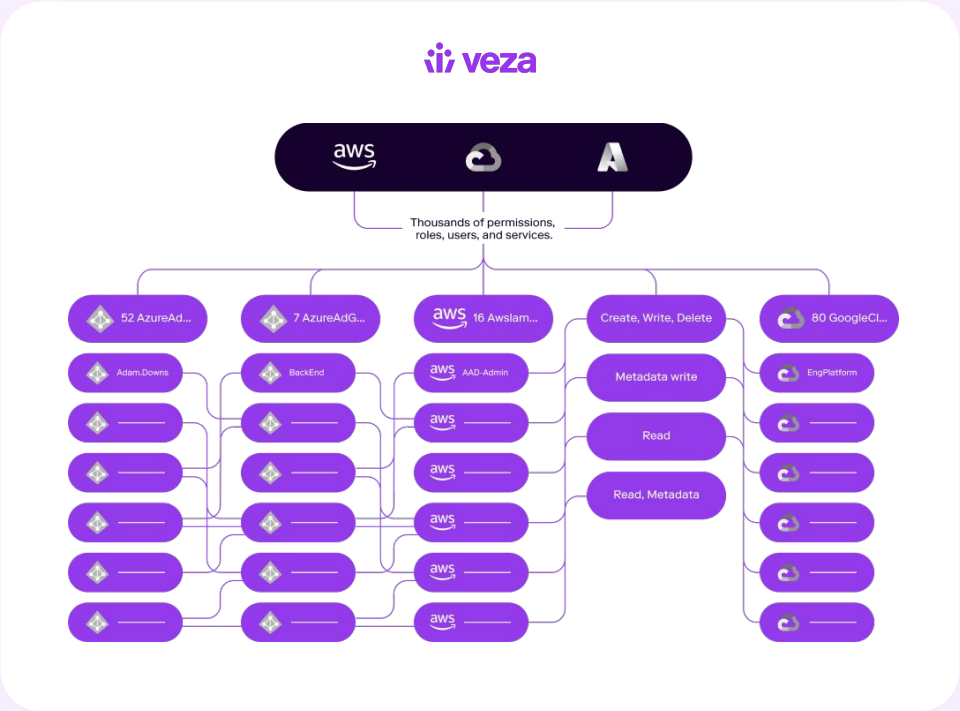
Enable least privilege to data

With the visibility and insight provided by Veza, organizations can ensure that each account has only the minimum privileges on data required—create, read, update, or delete—for a user's job or a service account's function. Veza platform also provides recommendations on how to remediate access violations in the environment, including specific steps for specific systems such as AWS IAM.

Identify cloud IAM and data store misconfigurations

To further limit the blast radius of any breach, companies can flag users with high-risk permissions such as programmatic access to services, or AWS roles with AssumeRole lateral movement. Undersecured data stores such as S3 buckets that are unencrypted or allow public access can also be easily identified.

By bringing new visibility and insight into data permissions throughout the environment, Veza helps organizations understand and reduce their exposure to ransomware risk.



Making ransomware history

As long as ransomware attacks work, cybercriminals will keep launching them. The best anti-ransomware strategy is to protect what matters—the data itself—and keep from falling victim in the first place. By leveraging the power of authorization to prevent the malicious encryption of their data, organizations can render ransomware both ineffective and unprofitable. And never have to worry about ransom demands again.

Learn more about how data security plays a critical role in protecting against ransomware at Modernize Data Security to Protect Against Ransomware.

- 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.