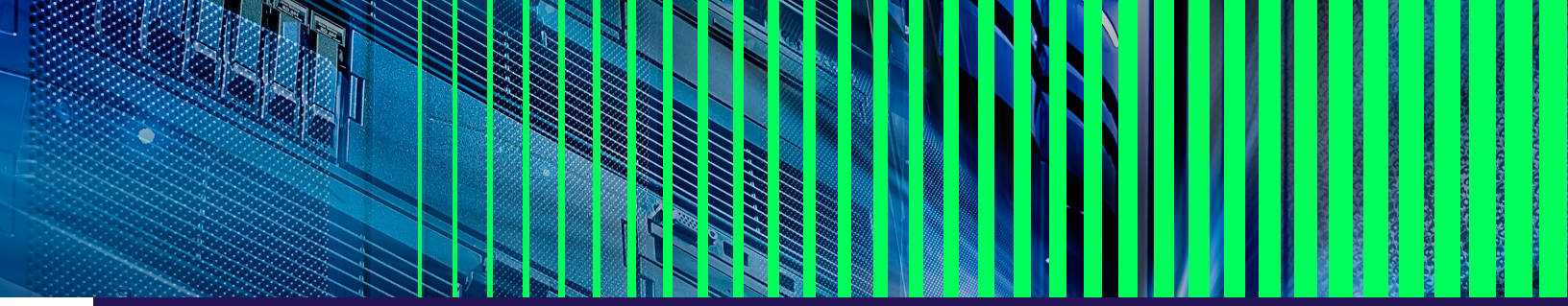

Delinea

Automated Access Management for Databases Eliminates Friction and Mitigates Risk

> Insider threats are among the most common causes of database security breaches and are often the result of allowing too many employees to hold privileged user access credentials."
>
> → IBM

Rise of cloud-hosted databases

Organizations are rapidly adopting cloud databases. Cloud databases are available on a pay-as-you-go basis so you can avoid capital investments and maintenance resources. In addition to scalable infrastructure, the cloud also offers services.

Your databases may include IaaS cloud resources, essentially an abstracted version of a traditional, on-prem database. You may also partner with cloud providers for Database-as-a-Service offerings, which provide benefits such as data outsourcing, multi-tenancy, and resource sharing. Cloud databases allow developers to t create applications without the hassle of infrastructure-related issues. A single organization may have multiple databases used for storage, application development, and data processing.

Database security challenges

When a small group of database administrators ran databases, you knew who they were and could enforce central security policies. Now, more people throughout the organization are accessing critical resources and sensitive information.. People accessing database resources are often remote and include direct hires, temporary contractors, and outsourced development teams. They want immediate access to databases to debug issues and answer questions.

Security teams must make it possible for people to be self-sufficient and access the databases they need to do their work without delay. At the same time, you must ensure mitigating controls are in place, such as an appropriate level of access, authorization, and approvals. To meet compliance requirements for security as well as data privacy, you must ensure a detailed audit log of database access.

Database security is often at odds with database usability. "The more accessible and usable the database, the more vulnerable it is to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use." (IBM)

Access is often provided to an entire resource or "package," meaning an entire database, to make debugging or other work easier. With this type of approach, you don't know what code, data, or processes are inside the database and you can't track activity or changes at a granular level. Your cloud databases may be from multiple vendors—Microsoft, Amazon, Google, Oracle, and IBM—which makes a consistent security and access model challenging to implement.

Keys to Database PAM

With Delinea's Database Access Controller you can minimize risk by providing database access to the right people at the right time.

1 LIMIT THE PEOPLE WHO KNOW YOUR DATABASE ADDRESS

Database Access Controller helps you avoid sharing the location of a database with more people than necessary. Proxy functionality means the IP address of the resource as well as the password are never shown to users. Even third-party contractors can access and work on a database without needing to see a specific IP address.

2 CONFIRM PEOPLE WHO ACCESS YOUR DATABASE ARE WHO THEY SAY THEY ARE

With Database Access Controller you can implement multi-factor authentication to confirm identity of database users. You can do this with authentication mechanisms such as email, Yubikey, or biometrics such as fingerprints.

3 SET LIMITS ON DATABASE USER ACCESS

Database Access Controller helps you avoid sharing the location of a database with more people than necessary. Proxy functionality means the IP address of the resource and the password are never shown to users. Even third-party contractors can access and work on a database without needing to see a specific IP address.

With Database Access Controller you can implement multi-factor authentication to confirm the identities of database users. You can do this with authentication mechanisms such as email, Yubikey, or biometrics such as fingerprints.

To censure Separation of Duties, you can control who can access which databases and set up automated workflows and approvals to provide granular access. You can even eliminate standing credentials and set up time-bound access that ends when projects are over or expires automatically after a certain period. You'll always have a data log to demonstrate security and privacy compliance.

Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**