Delinea

Multi-Directory Brokering

Many organizations are embarking on cloud migration projects that require new Windows and Linux instances in one or multiple Infrastructure-as-a-Service (IaaS) platforms. A big concern for them is how to leverage their existing on-premise or cloud-based Identity and Access Management (IAM) infrastructure to enable administrators, developers, and operations teams to access those systems securely, without massive incremental cost, effort, and complexity.

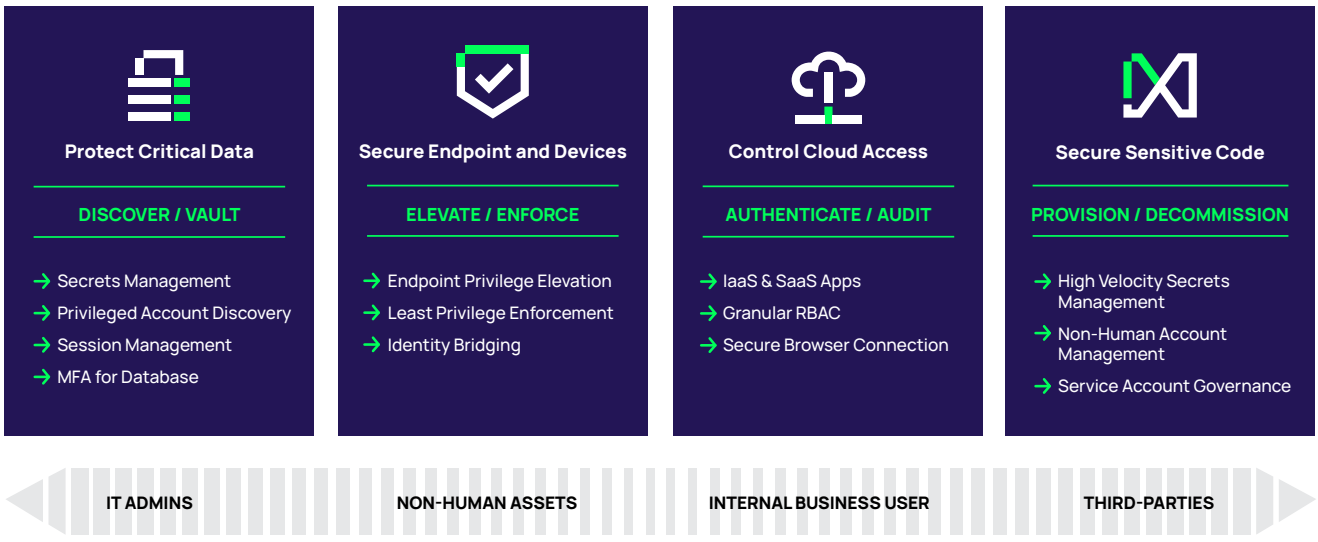
Organizations are replicating IAM infrastructure in multiple VPCs and clouds resulting in complicated directory trust models and additional firewall ports that introduce risk and threaten compliance.

This solution brief introduces Multi-Directory Brokering, designed to overcome these challenges. It is a capability of Delinea's Server PAM solutions.

Over the years, Delinea's Server PAM capabilities have grown into a rich framework extending PAM to address modern hybrid cloud use cases.

Although we'll use Amazon® Web Services (AWS) in our discussion, the challenge and solutions apply equally to other IaaS providers such as Microsoft® Azure and Google® Cloud.

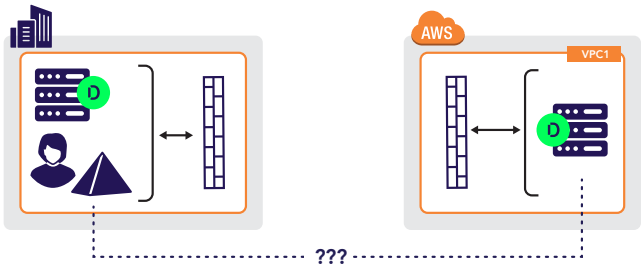
PAM Solutions Portfolio



Example Use Case

Let's assume you're starting a small proof of concept by standing up a few Windows and Linux Elastic Compute Cloud (EC2) instances in AWS. Developers work on these systems directly, as do the operations team and the system administrators. They all use local accounts to log in since that's quick and easy for a proof of concept.

Fast forward — the proof of concept is a success, and now they must secure and scale this environment for production. Per company security policy, these production systems must now be brought under centralized Delinea PAM security management like their on-premise servers. This means deleting or disabling all the local accounts and joining the servers to Active Directory. Users will then log in with their individual low-privilege corporate Active Directory account and use Delinea Server PAM's privilege elevation to run administrative tasks only when required, in a time-boxed fashion.

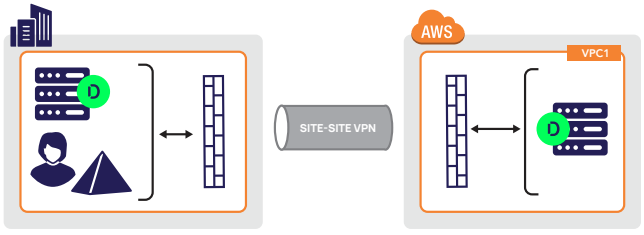


A big challenge is these new instances have no line of sight to Active Directory to validate the users' credentials.

Solution

You have several options. Let's briefly summarize the main ones.

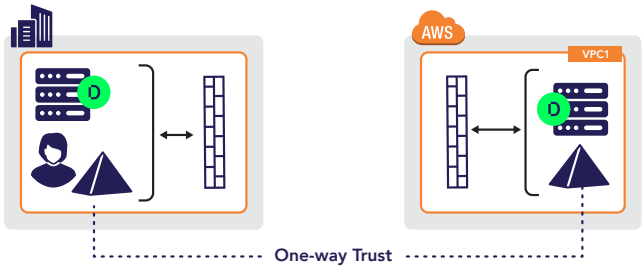
VPN Connection



Multiple options exist for the various IaaS providers. For example, Amazon provides Amazon Direct Connect and Amazon Hardware VPN. As dedicated site-to-site solutions, they can get expensive, and they may not be available in every geography.

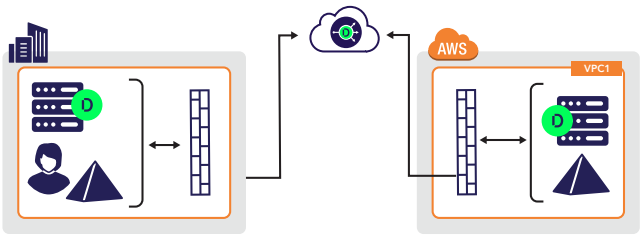
A security disadvantage is having to open all Active Directory ports, which increases the attack surface as an AWS EC2 instance in the VPC can now communicate openly with the corporate Active Directory.

Extend On-Premises Active Directory to the Cloud



Alternatively, various Active Directory configurations are possible that involve replicating the corporate forest or creating a new forest in AWS, each with varying pros and cons.

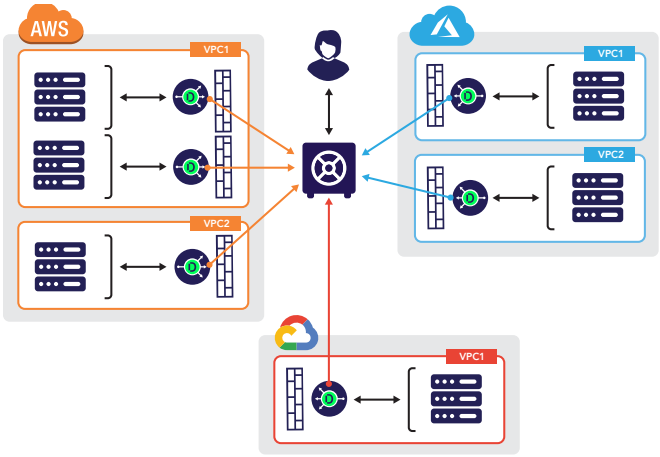
A best practice would be establishing a new Active Directory resource forest in AWS with a one-way trust back to the corporate forest. That adds quite a bit of complexity and additional infrastructure, cost, and maintenance, not to mention extra firewall ports that increase the attack surface.



Delinea Server PAM Clients for Linux and Windows include a modern Multi-Directory Brokering Service to satisfy this hybrid IT use case, focusing on speed, agility, low cost, robust security, and integration with existing on-premise infrastructure and PAM security controls. It involves the Delinea Client, Delinea Platform, and Delinea Connector.

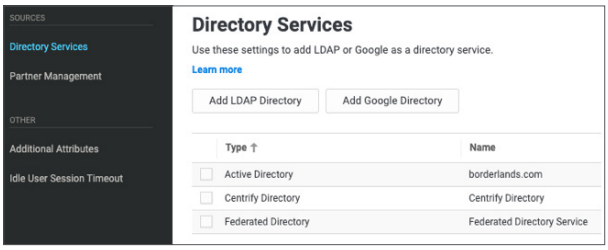
This approach obviates the need for your EC2 instances to join directly to Active Directory for user authentication. Even Windows EC2 instances don't have to be domain-joined. Instead, the EC2 instances enroll with the Delinea SaaS platform, where its multi-directory brokering service figures out where and how to access the appropriate enterprise user directory for credential validation. With this configuration, users can now log into Windows or Linux EC2 instances using

their corporate account without the instances needing direct visibility to the enterprise directory. This method is not only quick and easy but more secure than the alternatives. Since Delinea Server PAM in your VPCs maintains a persistent outbound connection to the Delinea Platform, there's no need to poke additional holes in your firewall.



We also designed this solution to scale in support of modern hybrid use cases. If you distribute your applications and services across multiple VPCs/VNets or even across multiple IaaS platforms, traditional password vaults would need to be replicated along with all the supporting infrastructure necessary to synchronize across the systems. However, due to its modern hub-and-spoke design, and since the Delinea Platform is a true SaaS service, it is accessible from any DMZ, any VPC/VNet, any IaaS provider.

One final benefit — if you happen to maintain administrator accounts in multiple enterprise directories — for example, internal IT in Active Directory and outsourced or third-party identities in LDAP, the Delinea Authentication Service has you covered since it can validate user credentials against Active Directory, LDAP, Google Cloud Platform Directory, Delinea's own Cloud Directory, or even a directory from a third-party identity provider, such as Okta Universal Directory.

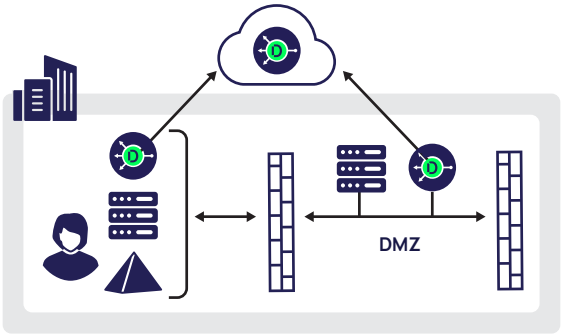


The net-net is that you can eliminate local privileged accounts and enable users — administrators, operations team, developers — to log into IaaS instances using their least privilege enterprise identity without IT having to replicate enterprise directory infrastructure and without these instances joining to a corporate directory domain controller. Even the Windows instances can be standalone.

Bonus — DMZ Use Cases

Many customers stand up Windows or Linux boxes on-premise in their DMZ for applications such as Web servers. They don't want the inherent risk of extending Active Directory into the DMZ to enable Active Directory-based login, so they use local accounts for user login. Sound familiar?

The solution described above for the cloud-based use case works identically for this use case as well. The servers in the DMZ don't need to join to Active Directory. They instead join the Delinea Platform, which in turn securely bridges to Active Directory inside the corporate network or the other directories mentioned earlier.



So, this is a prime example of Delinea evolving to solve modern hybrid use cases that legacy PAM solutions are simply not designed to accommodate, but in the process, satisfying an existing security challenge that plagues many customers today.

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**