

Delinea

Software and Services

For G-Cloud Clients

Contents

Contents.....	2
Executive Summary.....	6
Company Overview.....	7
Secret Server	8
Summary	8
Secret Server Architecture.....	9
Overview.....	9
Deployment Options	9
Cloud Architecture	9
Secret Server Cloud Architecture	10
Cloud System Pre-Requisites.....	10
On Prem Architecture	11
Single-Site Architecture.....	11
Multi-Site High Level Architecture	12
Architectural Assumptions	12
System Pre-Requisites	13
Architecture Component Description.....	14
Local and Global Load Balancers.....	14
Web Server Layer	14
Database Server Layer	14
RabbitMQ Server Layer	15
Distributed Engine Layer.....	15
Features description	16
Vaulting and Encryption.....	16
Access Control.....	16
Auditing and Monitoring.....	17
Session recording	17
Metadata capturing	18
Password Management	19

Session Flow Description	20
Session Flow – Agent Based Launching from the WebUI	20
Session Flow – Agent Less Launching from the WebUI	21
Session Flow – Agent Less SSH Terminal	21
Session Management.....	22
Secure Remote Access to Infrastructure without a VPN	22
Privilege Manager	23
Get complete visibility	23
Implement Least Privilege Enforcement	23
Control Your Applications	23
Application Elevation	24
Provide the right level of security and flexibility for your organisation	24
Warning.....	24
Justification	24
Approval	25
Privileged Behavior Analytics.....	26
PBA Key Features	27
Connection Manager	29
The challenge	29
Secret Server integration:	29
The solution – Connection Manager	29
Key Features.....	30
Delinea for Active Directory Bridging	31
AD Bridging Architecture	31
Prerequisites.....	32
Connector machine configuration:	33
AD Bridging Features	34
Identity Consolidation	34
Unique Zone Technology	34
Enforce Separation of Duties	36
Centralize User Profiles	36
Delegate Access.....	36

Ensure Separation of Duties.....	36
Least privilege Access & Privilege Elevation.....	37
Complexity in the Many Flavors of Linux *and* AD	39
Restricted Shell	41
Beyond Authentication	41
Supportability Over Time	41
Deployment Options and Services.....	42
Account Lifecycle Manager	43
Service Account – Full Lifecycle Management	43
ALM Architecture	44
Cloud Architecture	44
Functionality	45
Establish Workflows.....	45
Delegate Ownership.....	45
Provision Accounts.....	45
Enforce Governance.....	45
Decommission Accounts	45
DevOps Secrets Vault.....	46
The challenge	46
The solution	46
Integrations.....	46
Integration with Secret Server	47
Architecture	47
Delinea Support	48
Support Portal.....	48
Support SLA Summary	49
Standard Support	49
Premium Support.....	49
Premium+ Support.....	49
Delinea Training	50
Delinea Training Methodology & Framework	50
Delinea’s Instructor-led training.....	50
Delivery	50

Sample Schedule	51
Delinea’s E-learning	52
Project Overview	53
Professional Services Team.....	53
Implementation Approach.....	54
Project Governance	55
Project Team	55
Delinea Project Team	55
G-Cloud Clients Project Team	56
Implementation Approach & Key Deliverables	57
Project Communication Plan	58

Executive Summary

Cyber Incidents have evolved and have become the #1 risk for organizations and businesses in the world¹. Also privilege account are the primary target for hackers as they represent the “Keys to the Kingdom”. Protecting and securing these critical accounts has become a top priority for organization and PAM has become the #1 security priority for CISO's².

Indeed, we have seen that 80% of breaches will involve Privileged Accounts³, 85% of Cyber Attacks are done through compromised endpoint⁴ and finally that 96% of critical vulnerabilities in Windows can be mitigated by removing Local Administrative rights on endpoints⁵.

Privilege Accounts are present everywhere, in every system and can easily exceed 3 to 5 times the number of employees. They also exist beyond IT, such as in Social Medias where misused of account can lead to catastrophic impact on the organization's reputation.

This document provides an overview of the solutions available from Delinea and the PAM solution proposed by Delinea for G-Cloud Clients. This response provides an overview of the products as well as detailed response to the request for proposal and sets out the specifications, requirements, options, and indicative general terms covering the services G-Cloud Clients require.

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide, including over half of the Fortune 100. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. For more information, please visit <https://delinea.com/>

¹ Source: Allianz Risk Barometer 2021

² Source: Gartner

³ Source: SANS

⁴ Source: Forrester

⁵ Source: Microsoft

Company Overview

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide, including over half of the Fortune 100. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. For more information, please visit our website <https://delinea.com/>

Delinea was formed in 2022 with the merger of Centrify Corp incorporated in 2004 and Thycotic Software founded in 1996 and incorporated in 2000 in the USA as Thycotic Software LLC, a Delaware registered company.

With the release of our Privileged Account Management product, Secret Server in 2005 we saw amazing growth year on year, recently reaching 75% CAGR, and by investing 16% of revenue in R&D we are now recognised as an industry innovator and leader by many independent bodies including Gartner, KuppingerCole & Forrester.

Having been acquired by TPG Capital in 2021 and undergoing a merger with Centrify, rebranding as **Delinea**, we have seen great growth and investment in our solutions and company, expanding our portfolio, personnel and presence globally. For more information, please see <https://delinea.com/news/thycoticcentrify-is-now-delinea> and <https://delinea.com/news>.

Delinea is a private limited company with over 850 employees. Now headquartered in Redwood, California and Washington DC, Delinea operates worldwide with offices in the UK, Germany, Spain, Singapore, and Australia. For more information, please <https://delinea.com/> and <https://delinea.com/contact-us>

We are a channel software sales organisation that is structured around customer success and customer feedback. This means that departments are structured for cross functional feedback and improvement to rapidly deliver updates to our products to maintain high levels of customer satisfaction. With 95% customer satisfaction and 97% retention rate, Thycotic were named a Gartner Peer Insights Customers' Choice for PAM in Jan2021.

We are ISO27001 and SOC2 certified, GDPR and EU/US Privacy Shield compliant. Our Software is Common Criteria certified, NIST-compliant, FEDRAMP certified and CSA STAR certified. We also have FEDRAMP. With this level of assurance our products are currently being used by many Fortune listed companies across all industry sectors including Government, Energy & Utilities, Financial services, IT & Security, Healthcare & Pharmaceuticals, Education, Manufacturing, Commercial and Retail. Our customers include over half of the Fortune 100 companies and some of the largest companies in the world.

Secret Server

Delinea provide a range of solutions within a PAM platform to meet every aspect of privileged account security. Secret Server is the cornerstone of the platform and provides vaulting, discovery, session management and a range of additional functionality to meet the needs of organizations looking to secure privilege accounts.

Summary

Delinea provides security solutions to over 17,500 organizations and are a leading provider of privileged account management solutions, some of our key differentiators are listed below:

- Fastest growing PAM company over the last 5 years
- Full SaaS solution since 2017 (more than 1,200 customers deployed in the cloud)
- Functional parity with the Cloud and on-premise version
- Flexible launching model – a dynamic approach designed to save PMI money by leveraging client-side processing (decreasing the server infrastructure required for the solution)
- Best UI/UX – ensure users adopt the solution with an easy-to-use, unified interface
- Rapid deployment, allowing the solution to become used and provide security quickly and effectively
- Low or zero down time upgrades – allowing no service interruption for upgrading the PAM platform
- Extensibility, with APIs and integration abilities available right out-of-the-box for easy use with no vendor professional services
- 34 Net Promoter Score from customers – 14% above industry average
- More 5-star Gartner Peer reviews than any other PAM vendor
- Certifications: ISO 27001, SOC 2, Common Criteria, EU GDPR compliance, PCI-DSS, SOX, SAS70, FERC, NERC, COBIT, and HIPAA

Secret Server Architecture

Overview

Delinea Secret Server is a PAM solution comprised of two main components, A front end web application that is hosted within Microsoft IIS and a backend database hosted within Microsoft SQL Server. The solution can be hosted on physical or virtual infrastructure with no differences between system requirements.

The solution can be made highly available to provide active/active or active/passive failover. Based on G-Cloud Clients requirements, a proposed high-level architecture has been proposed. If successful, Delinea will work with G-Cloud Clients to validate and refine this architecture.

Deployment Options

Delinea Secret Server is available in the following deployment formats:

- **On-Premise** – Deploy Secret Server into on-premise, physical, or virtual infrastructure or into a private cloud tenant.
- **Cloud** – Access the same functionality as a service with Secret Server cloud, a full SaaS PAM offering

Cloud Architecture

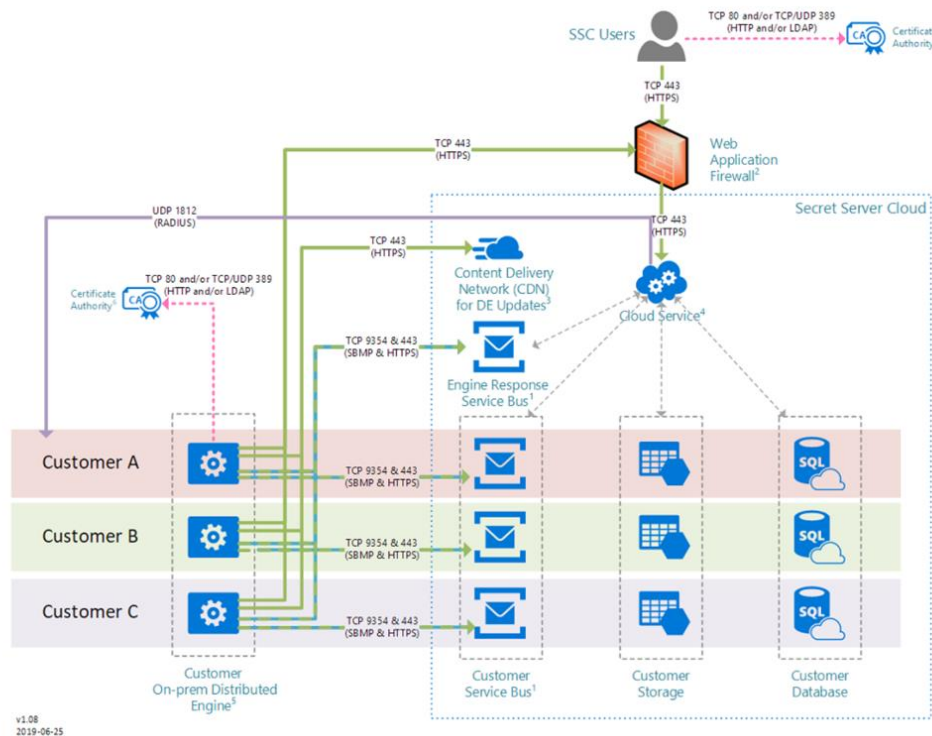
Delinea Secret Server cloud is a PAM solution hosted by Delinea as a SaaS service. An on-prem component, a Distributed Engine, provides connectivity and performs local tasks such as password rotations, heartbeats, account discovery and proxying of connections as necessary. If successful, Delinea will work with G-Cloud Clients to validate and refine this architecture.

Delinea Secret Server Cloud is hosted in Microsoft Azure with 100% isolation and data encryption. Delinea provide the following Azure locations: US East, Canada, Singapore, Germany Central and Australia Central. Customers can choose whichever region they wish to use at initial provisioning, typically choosing the closest location or if they have a specific requirement for where data reside.

For Secret Server Cloud in Europe, we use Azure datacentres based in Germany; Frankfurt (Germany Central) and Magdeburg for failover (Germany Northeast).

Secret Server Cloud Architecture

Secret Server Cloud Multi-Tenant Architecture Reference



Cloud System Pre-Requisites

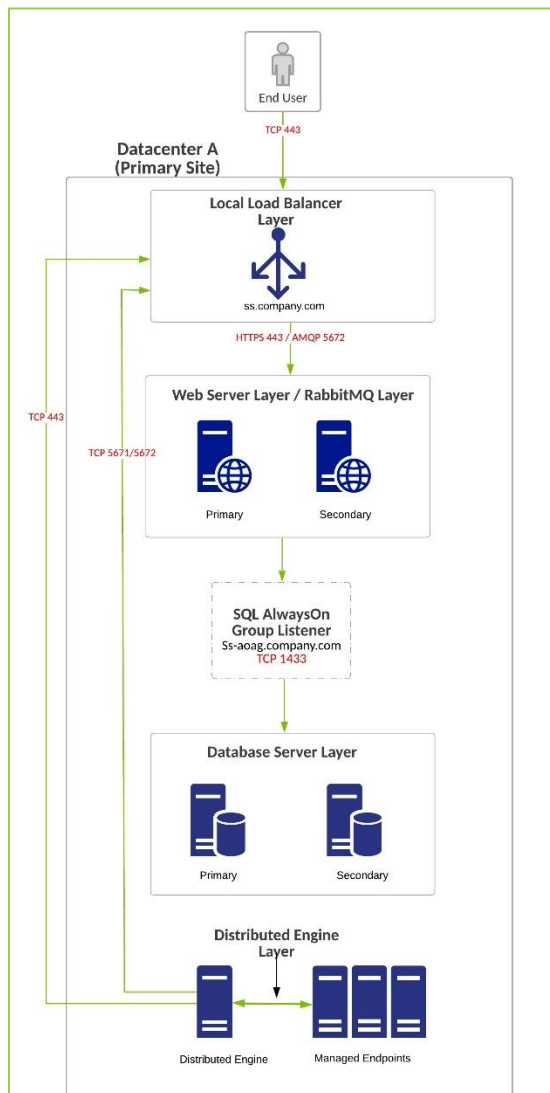
Below are the system prerequisites to implement the proposed architecture:

Role	Operating System	# CPUs (≥ 2GHz)	RAM (GB)	Minimum Storage (GB)
Distributed Engine	Windows Server 2012 or higher	4	4	100

On Prem Architecture

Single-Site Architecture

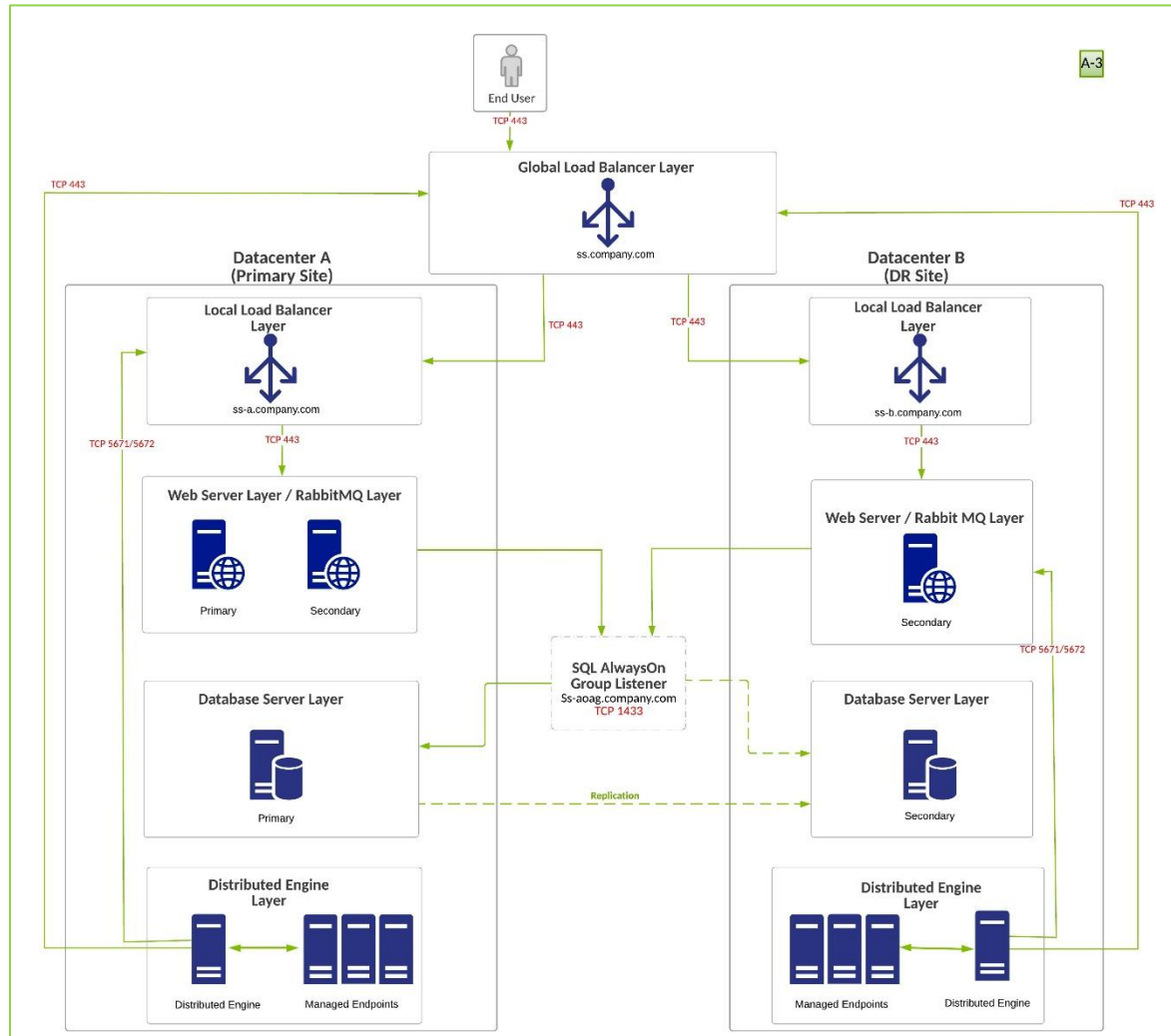
The following high level design identifies how Secret Server can be deployed in a highly available configuration within a single deployment location.



The above high-level design of the architecture is proposed as a Conceptual Design to present the different component involved in a Secret Server deployment. Each component of this architecture is described further below in this document, and it has been built to provide high availability and to G-Cloud Clients requirements.

Multi-Site High Level Architecture

The following high level design identifies how Secret Server can be deployed in a highly available configuration across two deployment locations.



The above high-level design of the architecture is proposed as a Conceptual Design to present the different component involved in a Secret Server deployment. Each component of this architecture is described further below in this document, and it has been built to provide high availability and to G-Cloud Clients requirements

Architectural Assumptions

The solution will be installed within required datacenters and will provide **Active/Active** with **high availability on each and every component** of the architecture to guarantee maximum resiliency and the best performance for G-Cloud Clients.

Delinea will deliver a detailed Low Level Design (for Delinea component) during the project

System Pre-Requisites

Below are the system prerequisites to implement the proposed architecture:

Datacenter	Role	# CPUs (≥ 2 GHz)	RAM (GB)	Minimum Storage (GB)
Primary	Frontend WEB	8	16	500
Primary	Frontend WEB	8	16	500
Primary	Database	8	16	1000
Primary	Database (optional)	8	16	1000
Primary	Site Connector	2	4	100
Primary	Site Connector (optional)	2	4	100
Primary	Distributed Engine (optional)	4	8	100
Secondary (DR)	Frontend WEB	8	16	500
Secondary (DR)	Database	8	16	1000
Secondary (DR)	Site Connector	2	4	100
Secondary (DR)	Distributed Engine (optional)	4	8	100

Architecture Component Description

Local and Global Load Balancers

The load balancers are deployed at the frontend of the solution and direct traffic appropriately depending on a wide variety of dynamic configuration options. The load balancers themselves are generally considered to be a part of the *environment* as opposed to the solution and are hence not provided as part of Secret Server itself. The load balancers that can be deployed at each layer must be capable of X-forwarding and carrying TLS traffic over port 443 to the required servers.

This diagram specifically details the split between the local and the global load balancers, however any such configuration can be defined and deployed depending on the specifics of the network into which the solution is being placed.

Web Server Layer

The frontend for Secret Server is built on a Web Cluster formed of multiple Windows IIS ASP.NET frontend servers to provide the solution interface both for users and API-based transactions. As well as providing the interface, the servers also perform various working functions such as processing password changes, performing discovery, running scripts, compiling reports, and creating Secrets in the backend database. These actions are closely tied to the message queue as describe in the 'RabbitMQ Server Layer'.

Multiple web servers can be run side by side, either in an active-active configuration or in an active-passive configuration. The web servers act in a cluster which is self-maintaining and can be made up of as many web servers as is required to meet the customers locational and availability requirements. Additionally, different servers in the cluster can be assigned to different types of processing actions depending on the requirements of a specific geography, datacenter, or "Site". "Sites" are simply virtual groupings of devices within Secret Server.

Database Server Layer

Secret Server features a wide variety of High Availability deployment options. The backend database, built on Microsoft's SQL platform, can be implemented in a highly available way using Microsoft SQL AlwaysOn Availability Groups.

In this architectural example, the database is set as an AlwaysOn Availability group spanning two data centres and provides intra datacenter as well as inter datacenter resilience.

With respect to database security, Secret Server uses Advanced Encryption Standards (AES) 256-bit encryption to secure all privileged accounts. Each privileged account has its own unique AES 256bit encryption key, and is encrypted, salted, and hashed when stored. AES 256 encryption is subset of the Rijndael algorithm, provides unsurpassed security for sensitive enterprise passwords. All sensitive information in the database is encrypted using the master encryption key for the service. Additional Transparent Data Encryption (TDE) can be enabled which protects the entirety of the database with Microsoft standard database encryption.

RabbitMQ Server Layer

Actions within Secret Server such as password changes, discovery, and many more, are stored as messages in the message queue before being transacted by the selected Web Server or Distributed Engine. The message queue is powered by RabbitMQ which in this architectural pattern is instantiated as a Cluster spanning across two datacenters to provide resilience of the queue.

Messages are securely transmitted to and from the message queue via TLS over 443.

Distributed Engine Layer

Secret Server features inbuilt tools such as the 'Distributed Engine' which allows for process offloading (for very large, process intensive estates) and also allows administrators to easily extend the reach of Secret Server across geographically disperse estates – particularly infrastructures that feature high levels of network segregation. The Distributed Engine(s) can be set to perform actions such as password validation (heartbeats), password changing, directory integration, session proxy and discovery locally in a specific environment (such as a DMZ) to avoid the need to have to open up a wide variety of firewall rules into these environments to grant the PAM solution access.

For Secret server cloud the Distributed engine also connects your environment to you Secret Server cloud and is the only component that would be installed within your environment.

Features description

Secret Server session flow is built to be the less disruptive for the architecture yet providing a very secure way of protecting privilege accounts, control the access to these accounts and auditing and monitoring their usage.

Accounts stored into the Secret Server will benefit from the below controls:

Vaulting and Encryption

Credentials that are stored in the database are protected by unique AES256 bit encryption keys that are generated for each and every privileged account within the solution. The sensitive parts of these credentials (the password, for example) are protected via encryption, hashing and salting.

A copy of the master encryption key is triple encrypted (once via symmetric obfuscation, once via the DPAPI key of the server and then once via the EFS key of the domain service account that is running the Application Pool on the server) on each web application server, and this provides access for the web server in question to then unlock the sensitive components of a privileged credential in a highly authenticated and rigorously enforced manner. It is worth noting that, if available, the master encryption key can be offloaded to an HSM (Hardware Security Module) for storage and dynamic access, where available.

Access Control

Ensuring that users will have access only to accounts that they are allowed to. Implementing Role Based Access Control (RBAC) will allow granular permission granting to access information within the solution. Access policies can be defined based on user attributes in LDAP (Active Directory) or locally defined.

On top of RBAC, Workflows are available to allow further control over the access to accounts. These workflows are:

- i. **Request for approval:** The user's access to privileged account must be granted by one or multiple approvers with the ability to define multiple level or approvals
- ii. **Request for comment or ticket number:** leveraging an integration with a ticketing system solution, the user can be asked to provide a reason as well as a valid incident or change ticket number before accessing a privileged account.
- iii. **Checkout:** Making the access to an account exclusive to a user for a defined time. This will allow organization to enforce accountability, especially with shared account. It is also possible to rotate the password every time the user is done using the account.

Auditing and Monitoring

Secret Server keeps track of every user integration with a system: every access to an account, change of configuration, view of a session recording, etc. This way, we can provide a full audit trails to admins and auditors regarding the solution. These logs can then be sent to an external SIEM solution.

Additionally, Session Recording is also available to provide additional visibility during the session using privileged accounts:

Session recording

Secret Server can record full session-based activity. This includes visual, screen activity, and keystroke logging, from the moment a user launches a session from our platform, right through to its termination. This data is lightweight and stored securely. Each session is indexed with key metadata including associated user, timeframes, relevant folder, sub folder, session/launcher type, etc, to ensure the most intuitive and user-friendly experience available.

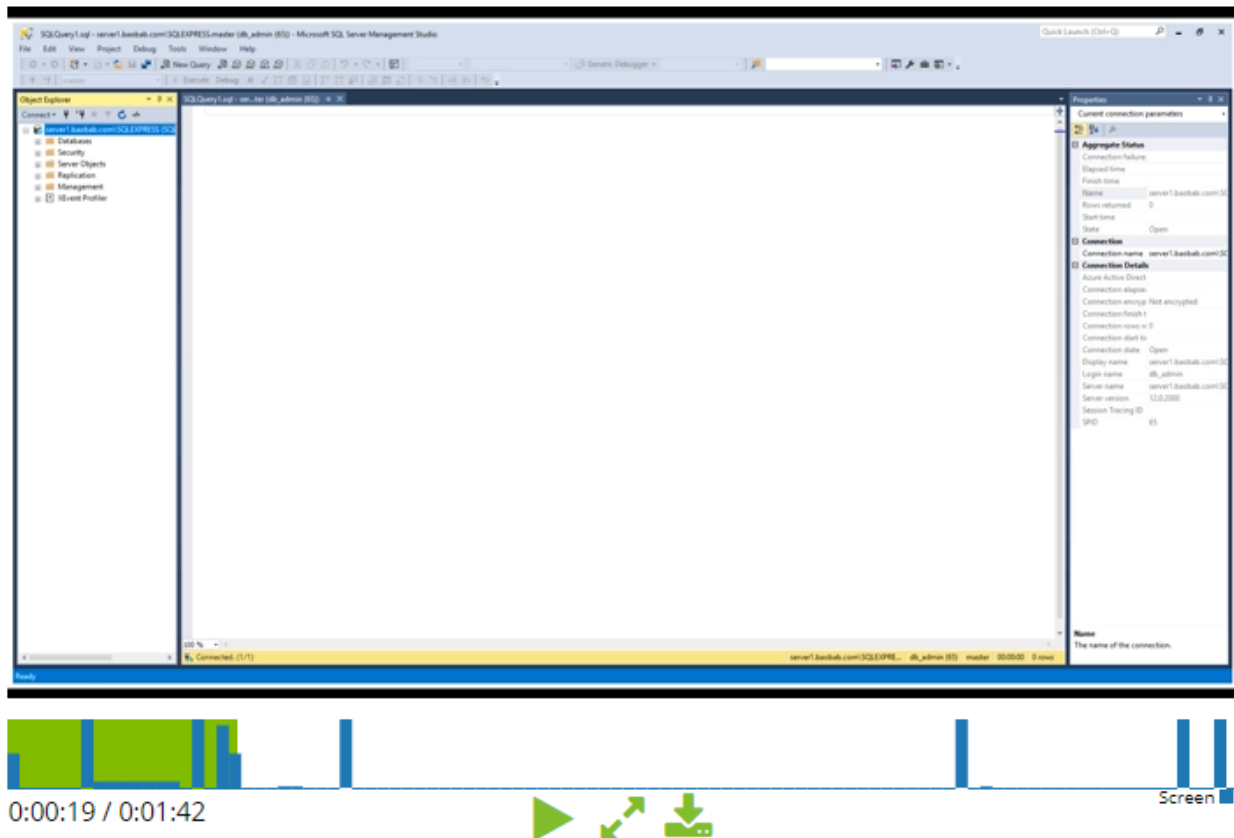
Full live session viewing is also available. Alerts can be set up to alert pre-configured admins when a suspect user logs in - enabling them to quickly begin live monitoring of users. Admins also have the option for a "live sessions" widget on their landing page - helping them keep track of live sessions. Admins with sufficient privilege can terminate live sessions immediately and require that the user request for access or use 2FA to log back in. All of this associated activity is marked and stored in the Secret Server audit trails. All sessions are recorded sequentially and can be played back in full, with keyword searches allowing the administrator to quickly identify and view a certain behaviour or keystroke entry.

When recording a session, Secret Server always records the user activity with it. Which means that inactivity during the session can be detected and skipped by the auditors when viewing the session, saving them time. Below is an example of an SQL based session recording where we can see the user activity below video to help the auditors focusing their attention on when the user was active during the session:

Session Recording is available for

- RDP Sessions
- SSH Sessions
- Web Sessions
- Custom Applications

Session recording provides full colour video of user activity as well as session metadata (keystrokes logged by the user during the session and application launches)



Note: This is available for any application that is being recorded

Metadata capturing

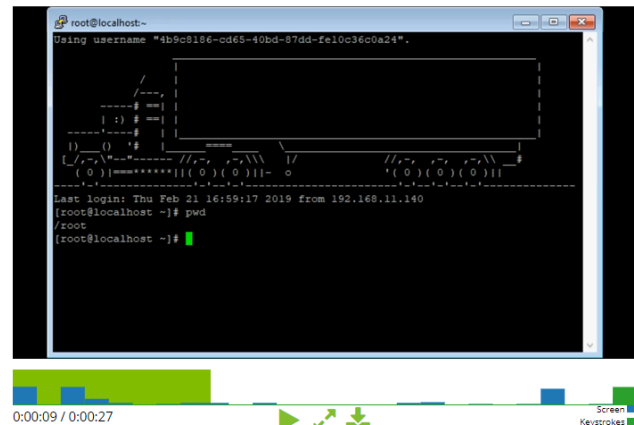
Capture of metadata (i.e. Key Logging, Processes, Screen Activity, and full video output. etc) is supported Client & Server side. The metadata for sessions is captured either directly (in the case of **SSH**) by the frontend web server (or Distributed Engine) that is brokering the connection and stored securely within the solution for auditing purposes. For **RDP**, the session metadata is captured by proxying sessions via the Secret Server or Distributed Engine RDP proxy or with the one-time installation of the Advanced Session Recording Agent on the target device that collects the keystroke data in real-time and sends it securely back to the platform. This data is then fully cross-searchable and accessible through granular auditing controls.

Search Session Activity

Activity Type: Keystroke Keyword:

Elapsed	Type	Activity	Jump To
07:20:52		pwd	
07:20:52		ls	
07:20:52		cd ..	
07:20:52		l	
07:20:52		ls	
07:20:52		cd etc	
07:20:52		pwd	
07:20:52		exit	

[View entire SSH Session Log](#)



In the case of SSH, the session log is also capture as a text file and be download separately from the video.

Password Management

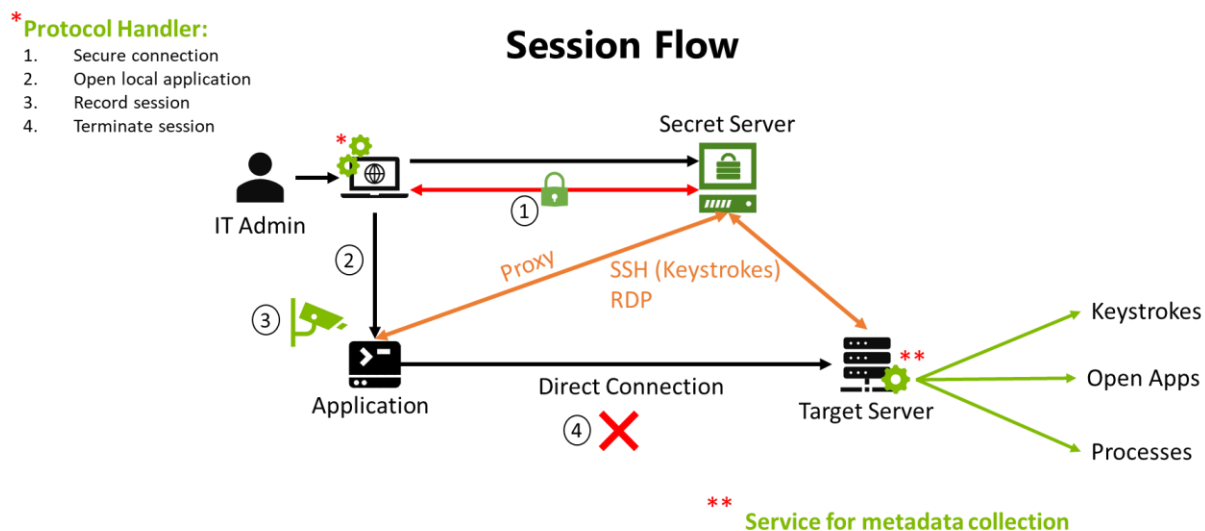
Secret Server can seamlessly manage privileged account credentials and rotate them automatically on a defined scheduled. Password can be hidden to the users to enforce confidentiality and “break the glass” mode is available if needed to provide access to all password for specific users.

Password policies can be defined for each type of accounts with customizable complexity.

Session Flow Description

In this section, we will describe the various method of launching session using Delinea Secret Server. As presented below, these various methods allow our customer to deploy and use Secret Server in the way that best fits their requirements. For instance, Delinea Secret Server is the only PAM solution that allows users to launch session either directly from their own machine or using a jump server with feature parity.

Session Flow – Agent Based Launching from the WebUI

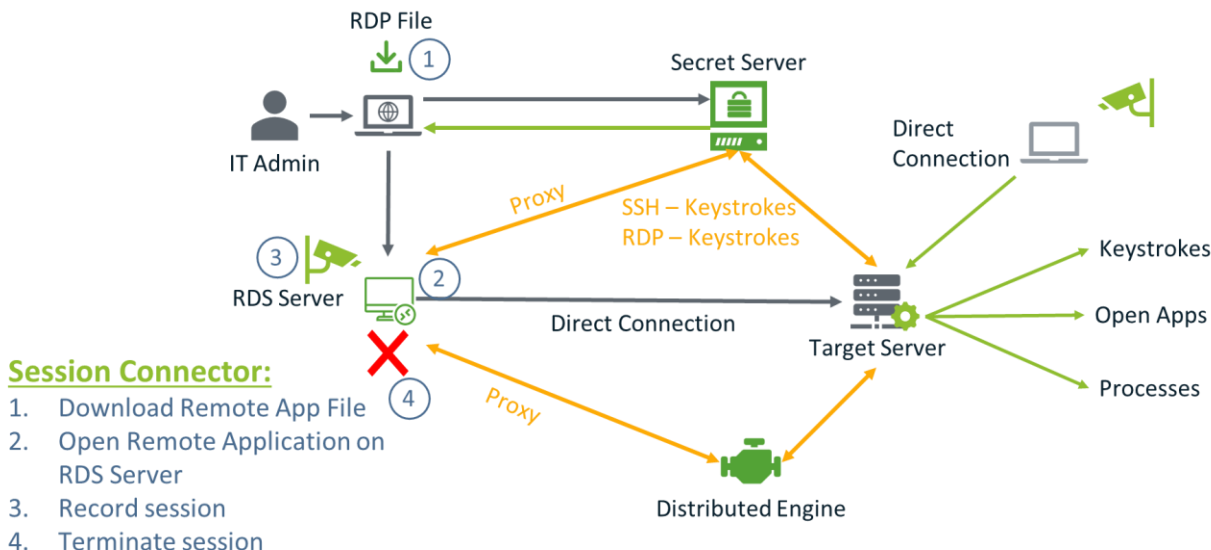


Delinea Secret Server features full privileged session management whereby privileged users can launch sessions in to target servers or applications and utilise privileged credentials without knowing the password to these credentials.

Sessions are launched from within the Secret Server web interface. These sessions can be built out of any application that is required, everything from PuTTY, to RDP, to FileZilla, to PowerShell, Telnet, VNC, HTTPS, depending on the type of privilege that is to be used. Once a session is launched the client device either connects directly to the session or application or, in the case of SSH and RDP, the session can be proxied through Secret Server - either one of its frontend web servers or Distributed Engines. Custom launchers can be instantiated to launch any required application. Both the SSH and RDP protocols can be proxied (and tunnelled through SSH) to the target device.

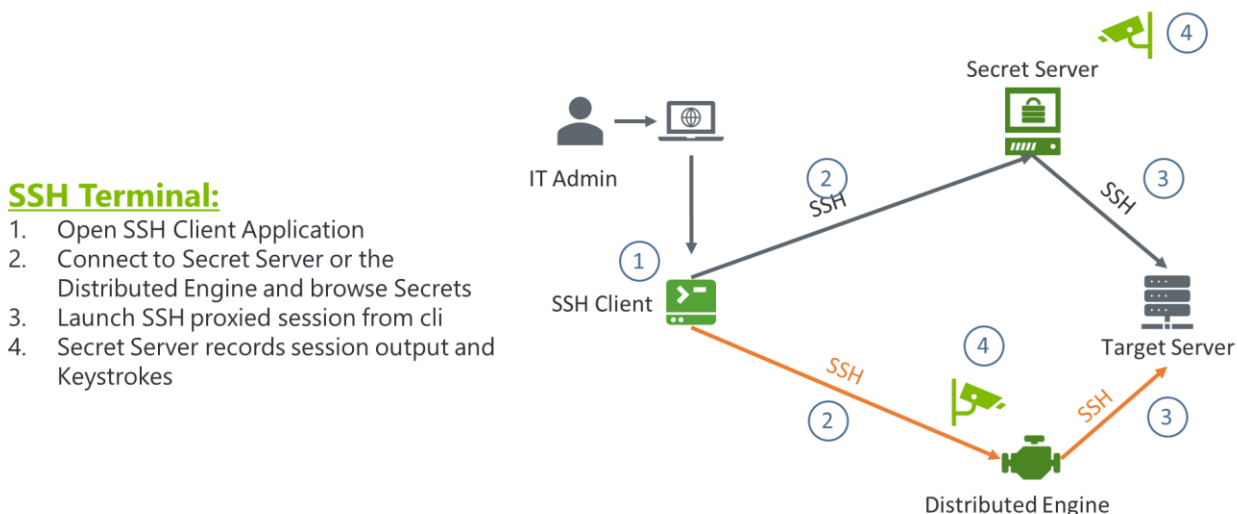
Direct launching in to privileged sessions is fully supported using Secret Server (removing the necessity for a Jump Server or Bastion Host), however, the solution can be easily integrated with an existing Jump Server, where required.

Session Flow – Agent Less Launching from the WebUI



In the above flow, the main difference with the previous one is that the launched application will be launched for a Jump Server called Session Connector. With Secret Server Session Connector (SSSC) installed on a Remote Desktop Services (RDS) server, anyone who can download and launch a standard Remote Desktop Protocol (RDP) shortcut file can have the same experience. The RDS server itself runs a special Secret Server Protocol Handler (SSPH) for RDS—SSPH (RDS) as a remote app to record the sessions, so end-users do not need to install any additional software.

Session Flow – Agent Less SSH Terminal



The above describe the SSH Terminal capability of Delinea's Secret Server that allow users to launch SSH session from any SSH client or Operating System, to target systems through Secret Server. It is also possible to launch your session directly to the target system using our Native SSH proxy feature and command using this syntax:

```
ssh <user>@<ss_ip> -t launch <secret_id>
```

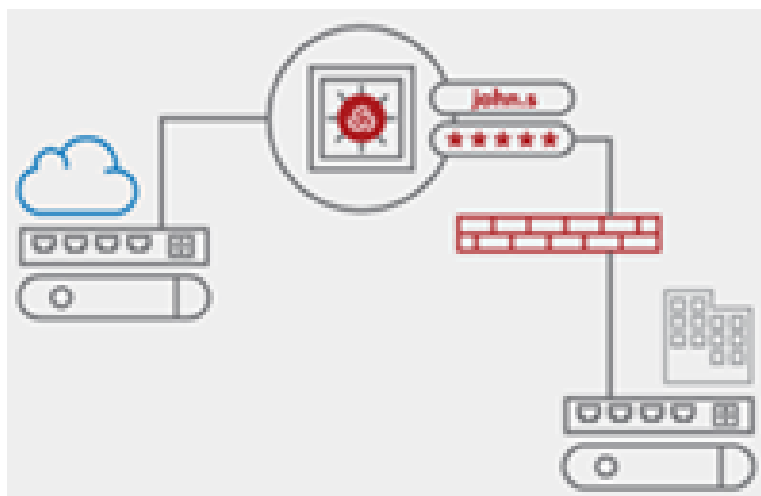
Session Management

Delinea Secret Server provides a very easy to launch session using application clients. The main requirement to launch an application is that it has to be installed on the machine that is used to connect to Secret Server: it can be the client machine or a jump server.

Below are the different level of integration with client application that Secret Server supports and their requirements:

1. **Full Integration:** Secret Server can launch the application from command line and pass on the parameters in the process. For example, for SAP GUI, the command to launch the applications from command line is: `./sapshcut.exe -sysname=<SYSTEM ID> -client=<CLIENT NUMBER> -user=<USERNAME> -pw=<PASSWORD>`
2. **Batch File integration:** If the application doesn't accept parameters in the process as described in option 1, a batch file to open the application and feed in the credentials can be potentially created, if supported the application. In this case, video recording will not be available and will require a Jump Server on which the application will be installed.
3. **Minimal:** if none of the above options are available or more information is needed to define the integration level, Secret Server can always launch the application from Secret Server and let the user copy paste the credentials in the application, that way we can record the activity.
4. **Web Password Filler:** For web application, the Web Password Filler will fill the username and password fields and login the user directly into the application. Secret Server now fully supports session recording for web sessions.

Secure Remote Access to Infrastructure without a VPN



Provide remote administrators, outsourced IT, and third-party vendors with secure access to the specific servers and network equipment they manage — on-premises and in the cloud. Context-aware multi-factor authentication combined with VPN-less access and a choice of deployment models deliver the robust security your hybrid IT environment demands. This allows for seamless access to only the appropriate resources without opening network wide access, thus increasing the attack surface.

Privilege Manager

Privilege Manager provides a best-in-class solution for managing local Windows and MacOS privileged accounts. Organisations commonly find themselves stuck between the security benefits of removing local administrative rights and productivity impact that this may bring. Privilege Manager provides the functionality to quickly and easily remove admin rights from users while elevating specific applications that may need elevation, without impacting user productivity.

Get complete visibility

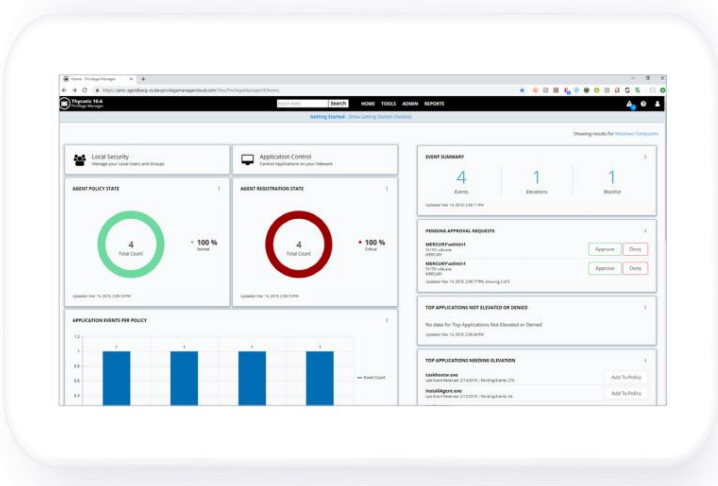
As soon as the Privilege Manager agent is deployed, all local users, groups and privileges are inventoried and can be viewed and reported within the central, administrative console. This gives organizations immediate visibility of local privilege environment, right across the organization.

Implement Least Privilege Enforcement

Remove excess privileges and permanently control which accounts are members of any local group. Continuously discover endpoints, applications, and processes tied to privileged accounts. Check policies and execute application control 24/7. View actionable reporting through a single, streamlined dashboard.

Control Your Applications

Create granular application control policies for Allowing, Blocking, Elevating, Restricting or just Monitoring applications, without requiring admin credentials or IT support to allow people to use applications and controls they need to do their jobs, without requiring local admin rights.



Easy To Support. Seamless For Users.

- Manage Local Groups and Accounts
- Deploy a Single Agent
- Define Flexible Policies
- Elevate, Allow, and Block Applications
- Improve Productivity and Reduce Helpdesk Tickets

Application Elevation

Privilege Manager allows organisations to completely remove administrative privileges while targeting and elevating applications that need admin rights to function. Applications can be targeted intelligently and securely to ensure pin-point accuracy of policies. Examples of secure application targeting methods are provided below:

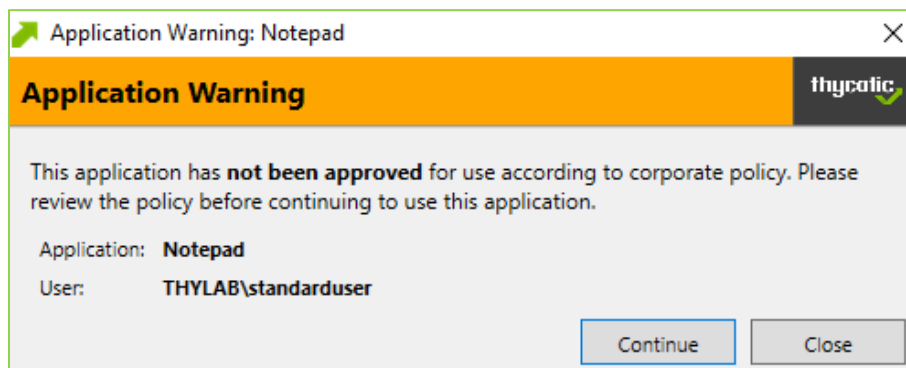
- Digital Certificate targeting
- Internal filename
- Command line matching
- Version
- Hash
- And many more

Provide the right level of security and flexibility for your organisation

Applications can be completely controlled so that users can only elevate or even execute applications that have been explicitly approved. Applications can also be gated so that users will see a customised message before execution or elevation is possible.

Warning

Ensure users are warned when running or elevating specific applications with a customisable message:



Justification

Prompt users to provide a justification as to why they need to elevate or execute a given application. The data collected from user justification can then be used to further refine and enhance policies:

Application Elevation: Notepad

Application Elevation thycotic

Please provide a reason as to why you require this application to be run with elevated rights.

Application: **Notepad**

User: **THYLAB\standarduser**

Type a brief explanation describing why this application is necessary. This explanation **will be recorded** and may be reviewed by the IT staff for consideration into corporate policy.

Reason (required):

Continue Cancel

Approval

an approval workflow so that users are unable to elevate or execute specific applications without getting approval to do so from a support team or line manager:

Application Notice: Notepad

Application Notice thycotic

This application has **not been approved**. Please discontinue use or enter your justification to continue.

Application: **Notepad**

User: **THYLAB\standarduser**

Type a brief explanation describing why this application is necessary. This explanation will form part of the request and will be reviewed by IT staff in consideration of this request.

Reason (required):

Continue Cancel

Privileged Behavior Analytics

Privileged Behavior Analytics (PBA) empowers IT and Security administrators to prevent, detect and stop breaches by continually analysing privileged activity across the organizations to identify early signs of data breach or insider threat. PBA is a cloud product built on the Amazon Web Services (AWS) platform, using machine learning to provide analytics to help administrators monitor and detect behaviours by aggregating and visualising audit and meta data from both Secret Server and Privilege Manager. PBA is available as an add on to Delinea Secret Server or is included with Secret Server Platinum Edition and Privilege Manager Cloud.



PBA connects directly with an on-premises or cloud installation of Secret Server and ingests all secret and user activity from Secret Server in order to detect anomalous behaviours leveraging machine learning algorithms and enables administrators to analyse privileged access using data visualization tools and intuitive dashboards.

PBA also connects to Privilege Manager Cloud and ingests data on users accessing applications, enabling administrator visualization and analysis.

Delinea provide AWS locations for PBA EU-central-1 or USA east-1 depending on the choice of the customer. In Europe the AWS location is based in Frankfurt Germany with DR site based in Ireland (EU-west-1).

PBA Key Features

Dashboards

PBA offers Flexible data visualizations & dashboards. The PBA dashboard contains multiple widgets that provide at-a-glance data on what is happening in your Secret Server environment. The page automatically cycles through views of your widgets from the last day, week, and month. You may pause the cycling by simply clicking on “Day”, “Week,” or “Month.” The widgets can be activated or deactivated by clicking on their corresponding symbols on the left side of the page. The Dashboard Assistant gives guidance to users on where they should focus their attention. It shows recent events and allows the user to go to those events in Privileged Behavior Analytics by clicking the event title. In addition, users may click the downward facing arrow icons on each event to receive more information about why the event matters and what they may do about it.



Cloud-based deployment

Privileged Behavior Analytics is deployed on AWS, selected due to its scalability and power to rapidly process and analyze large amounts of data. There is no installation required, simply connect your Secret Server and/or Privilege Manager Cloud installation to the cloud platform, and Privilege Behavior Analytics will begin working right away.

Machine learning / behavior baselines

Users access Secret Server in a number of different ways, but each individual person typically has a behaviour pattern. Privileged Behavior Analytics learns the behaviours of each individual user in order to create a behavior baseline, so that when the user perform activities outside of this normal behaviour, the system can alert the security team.

Threat scoring

Privilege Behavior Analytics applies a threat scoring algorithm to determine the severity of anomalous behaviours. This threat scoring takes into account factors such as the time of day a secret is accessed, the level of sensitivity of a specific secret, whether the secret is shared with a number of users, and their history of access to that secret

Manual sensitivity adjustments

For secrets and users that need to be monitored more closely, administrators can override the threat score to force the system to be more sensitive to that secret or user and the corresponding activity.

Secret access intelligence & graph

Analyse a number of different views of privileged behaviour across the system such as most active secrets, most active users, time of day access, extended secret access details, and extended user details. The Secret Access Graph can be used to explore the behaviours of Secret Server users at a glance. PBA for Privilege Manager also has an Application Clock, Graph, IP Map, and Most Active and details pages to show patterns of users accessing applications, using endpoints, and triggering policies.

Privileged Behavior Alerts

The Privileged Behavior Alerts page allows you to see any events that have occurred in Secret Server that were outside normal observed behavior. In addition, you can receive alerts under customizable circumstances whenever these abnormal events occur. Receive email alerts to be instantly notified the moment that unusual activity is occurring on your system, 24 hours a day, 7 days a week. Always have eyes monitoring the access of your system. Alerts provide details on the risk factor, such as who access the secret and at what time and allows the administrator to quickly click through to more details.

User Watch List

The User Watch List page provides a convenient location to track users of interest and easily access information about each. By default, the Privileged Behavior Analytics (PBA) System adds to the Watch List users with active alerts and warnings and new users.

Alert Actions

Privileged Behavior Analytics, PBA, provides three different automated actions that it can take in response to an Alert Event.

(1) The Challenge-response can be configured to automatically impose additional controls on a Secret Server User if their actions cause PBA to generate an alert that meets or exceeds the Alert Threshold.

(2) The Webhook response can be configured to integrate with external systems by sending an HTTP post when PBA has a user alert event.

(3) The Code Hook response can be configured to integrate with external systems by executing a user-provided script when Privileged Behavior Analytics has a user alert event.

Connection Manager

One of the biggest challenges to a successful PAM project is the acceptance of users and the perceived change to the ways in which users work. Delinea aim to provide a flexible range of options to minimise the change to user experience and therefore drive user adoption of a secure, easy to use platform.

The challenge

- Users in large, complex environments often have **multiple sessions** active at the same time (e.g., 30 simultaneous sessions for busy admin). Admins need to **quickly switch between sessions** to efficiently manage them.

Secret Server integration:

- Most managed sessions will be to secure resources requiring privileged access. They must be able to retrieve necessary privileged credentials from a secure vault.
- Users of SS can launch secure sessions, but they are not manageable within a **single interface**.
- Users do not want to log in to a SS interface to launch sessions. It **interrupts their workflow**. They want to use a session manager and have the necessary credentials automatically injected into their sessions.

The solution – Connection Manager

Connection Manager is a solution that provides a unified environment for management of and interaction with multiple remote sessions, for both Remote Desktop (RDP) and SSH. Integration with Secret Server provides the credentials needed for remote sessions and supports the various authentication and credential access mechanisms available through Secret Server. Integration with Secret Server is done via the REST API, which is included in Professional and Platinum editions.

Key Features

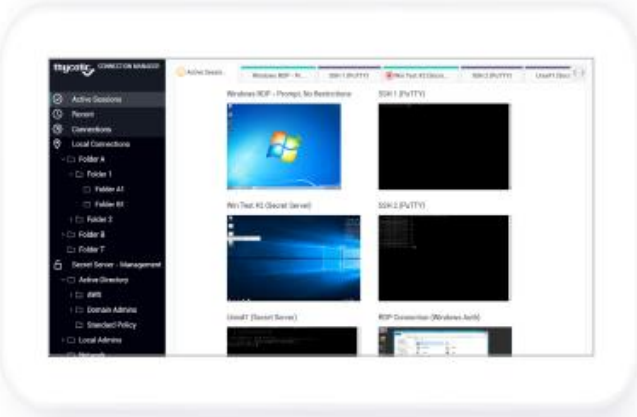
Remote Access: With Connection Manager users can launch and configure sessions across multiple environments without having to manage each separately. Connection Manager is tightly integrated with Secret Server and all details are encrypted. You can use Secrets to launch remote sessions on demand and the credentials and environmental details from Secret Server are automatically injected into sessions as needed. Saved Secret Server connections are displayed in the left-hand navigation. You can also make “Local” connections to environments not managed by Secret Server. These connections can be saved and managed locally and are listed separately.

Session Management: Standard RDP/SSH session controls are available. Sessions will open as a Tab and can be viewed this way or expanded to Full Screen depending on your preference. You have the option to define screen size and resolution for each connection.

Centralized Control: All of this is done through a single interface to manage and interact with sessions. Current sessions are viewed under “Active Connections”, or you can select the session tab. Selecting a connection in the main window will display its details. Recent connections are saved, and search is available to look for your Secrets or connection names.

Session Recording: Creating an end-to-end record of privileged user access is important for compliance mandates. With Connection Manager, you can record sessions when you see an indicator by the secret configuration in Secret Server – You see it is indicated with the Launcher icon in the Properties panel UI whether or not the session will be recorded.

Tracking and Auditing: You can record any access (launch/edit/view) of Secrets data and send that information to the Secret Server Audit logs. This provides an audit trail to prove compliance.



Streamline Control over Sessions
Connection Manager saves you time and lowers your privileged user risk

Remote Access: Launch and configure sessions across multiple environments

Session Management: Automatically inject credentials into sessions

Centralized Control: Access a single interface to manage and interact with sessions.

Session Recording: Create an end to end record of privileged user access

Tracking and Auditing: Provide an audit trail to demonstrate compliance

Delinea for Active Directory Bridging

Active Directory provides a central point of administration within Windows. But for Linux and UNIX, user identities may reside on individual servers or in separate identity silos, complicating operations and compromising security. Delinea unifies your IT infrastructure by centralizing identity and access management for non-Windows systems, devices, and apps within your existing Active Directory infrastructure.

Delinea Authentication Services (AD Bridging) is a software-based solution that can be deployed using on-prem virtual environment with simple requirements and scalable model.

Authentication Service simplifies cross-platform authentication and access control. Privilege Elevation Service grants elevated or restricted access to computers and accounts.

On Windows, Delinea includes management consoles and services to simplify the management and integration of Linux and UNIX computers and users into Active Directory.

The key components for Windows that you use in deployment are:

- Delinea Access Manager console
- Delinea Zone Provisioning Agent configuration panel and Windows service

There are several additional Windows components available for you to use, depending on the version of Delinea software you install and the requirements of your environment. For example, Delinea offers extensions for working with NIS maps and Active Directory group policies, as well as components to support a multi-tier architecture for auditing activity in user sessions and the Delinea Network Information Service to support agentless authentication service.

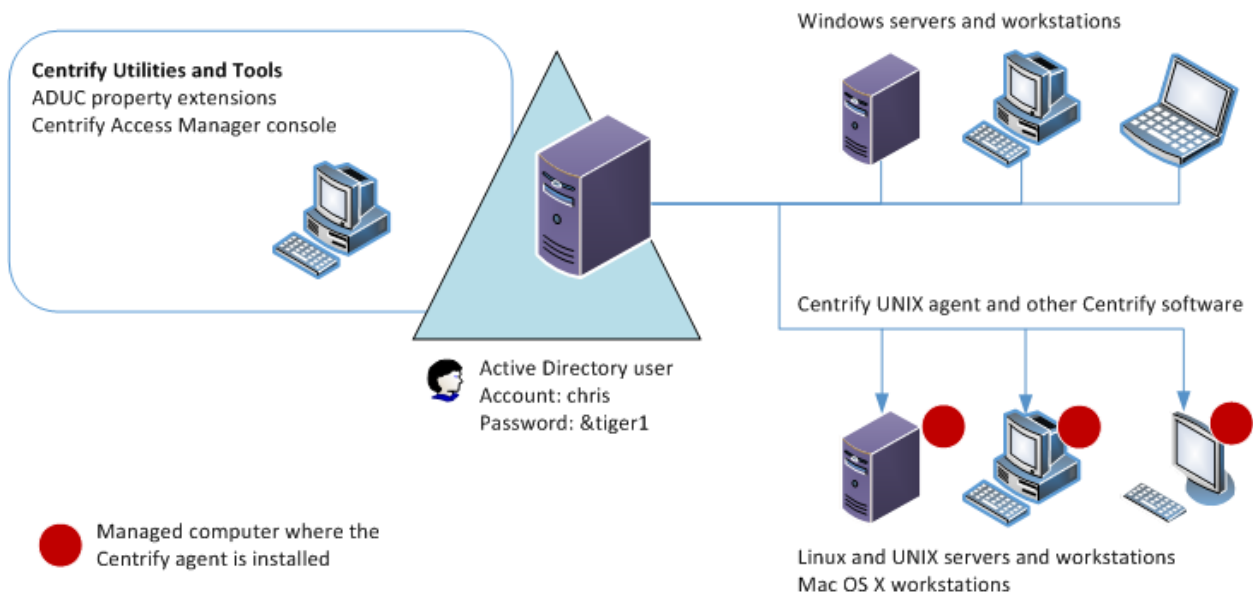
AD Bridging Architecture

On non-Windows computers, Delinea software consists of the core Delinea agent (adclient), related libraries, and optional tools. The Delinea agent enables the local host computer—most commonly a Linux or UNIX computer—to join an Active Directory domain.

After the agent is deployed on a server or workstation, that computer is considered a **managed computer** and it can join any Active Directory domain you choose.

When a Centrify-managed computer joins an Active Directory domain, it essentially becomes an Active Directory client and relies on Active Directory to provide authentication, authorization, policy management, and directory services. The interaction between the agent on the local computer and Active Directory is like the interaction between a Windows workstation and its Active Directory domain controller, including failover to a backup domain controller if the managed computer is unable to connect to its primary domain controller.

The following figure provides a simplified view of the integration between Windows and non-Windows computers through Delinea software.



Prerequisites

The below table summarizes the minimum software and hardware requirements for deploying Delinea Authentication Service. Requirements may vary based on your scale out and performance needs.

Component	Introduction	Specs	Qty	Comments
Delinea Management Node	Delinea Access Manager Server	windows server 2016 /2019 - Minimum Specs	1	
Delinea PAS	PAS Portal to service connectors (jump box)	windows server 2016 /2019 6 GB RAM 100 GB free disk space 2 Cores CPU	2 for HA	Failover cluster
Delinea Connector	Proxy sessions (Secure Remote Access)	windows server 2016 /2019 32 GB RAM 200 GB free disk space 6 Cores CPU	2 for HA	
Delinea Audit Nodes	Delinea Audit Collector Server	windows server 2016 6 cores CPU 32 GB RAM 200 GB of free Disk Space	2 for HA	
Audit Store	Database to store & archive audited sessions	Microsoft SQL Server 1 TB GB of storage		
for Node above	Computer clock set to synchronize with a known accurate time source. Microsoft .NET Framework updated to version 4.8			

Connector machine configuration:

Connectors could be installed on physical or virtual machines.

The machine requirements could be classified into the following sizes:

- Small: 2 Core 8 GB RAM, 500GB disk
- Medium: 4 Core, 16 GB RAM, 500GB disk
- Large: 6 Core, 32 GB RAM, 1TB disk

Note: All sizes should be served by 1 GB Ethernet.

AD Bridging Features

Identity Consolidation

Centrify enables you to consolidate user accounts and groups into Active Directory and enforce separation of administrative duties. Eliminate multiple identities and ensure a "one user, one identity" framework that strengthens security, lowers IT costs, and streamlines your organization.

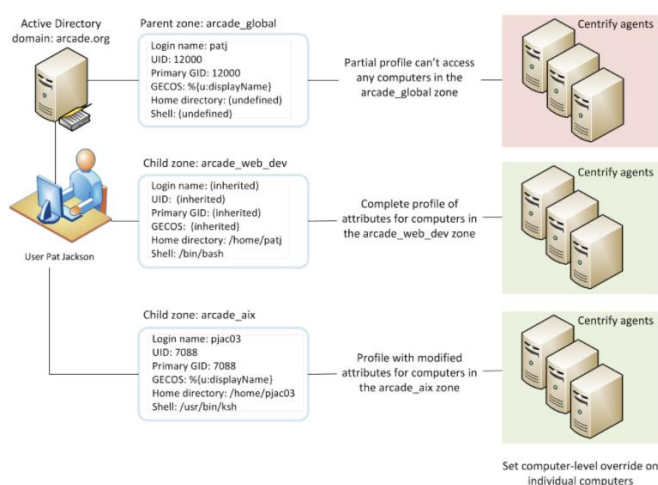
With Centrify, you can natively join Linux and UNIX systems to Active Directory, turning the host system into a client. Secure systems using the same authentication and Group Policy services currently deployed for Windows systems.

Unique Zone Technology

Whether you need to manage a few workstations or tens of thousands of Windows, Linux, and UNIX servers, Centrify's patented Zone technology enables you to quickly centralize management of these resources within Active Directory while not compromising on security or manageability. Delinea Zones provide:

- The fastest and most efficient means of consolidating a set of complex and disparate non-Windows identities into Active Directory.
- The most flexible solution for creating least-access and least-privilege security models for a diverse set of users, systems and roles across Windows, Linux, and UNIX systems
- The most secure means of managing user privileges in a highly granular manner.

How Zones Work



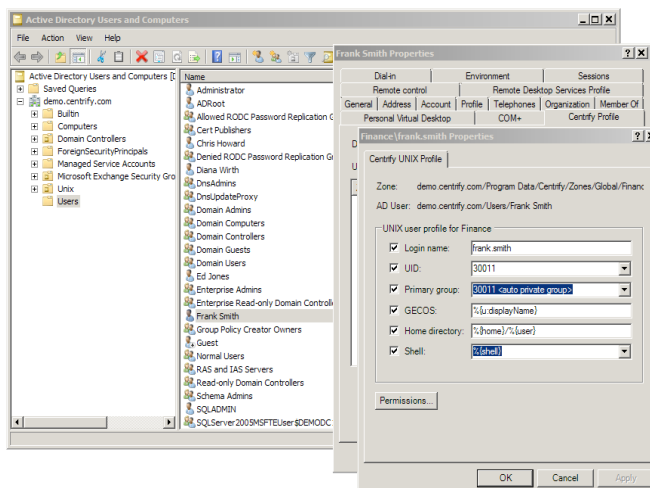
A Delinea Zone is a collection of attributes and security policies that define the identities, access rights and privileges shared by a group of users. A small organization might need only a single Zone to manage their users and desktops. A large organization may need a hierarchy of Zones to manage users who need access to thousands or tens of thousands of Windows, Linux, and UNIX systems that are used as everything from end-user workstations to web application servers.

Zones provide a flexible means of managing a set of users and computers that all need to share a common set of policies and access controls. For example, you could create a Zone for users and their computers,

regardless of where they are located geographically or what department they work for. You could create a Zone for an engineering department whose users must all share access to a set of UNIX development systems, whether located in a data centre or in the cloud. Or you could create a Zone for a branch office that has its own set of administrators tasked with managing all the Windows, Linux, and UNIX systems in their location. A user can be in multiple Zones, enabling you to create identity management, access control, privilege management and delegation solutions that are as simple or as sophisticated as you need them to be for your environment.

At minimum, a Zone contains a set of users that need to be managed as a group for efficiency or security reasons. Although some organizations will have Zones that contain only users (in particular, a Global Zone, described later), most Zones also contain:

- A set of UNIX management data that defines policies for those users' UNIX profile, such as how users' home directories are assigned (note: "UNIX profile" refers to management data for any Linux, UNIX, or Mac system)
- The set of computers or devices to which these users can be granted access.
- An inventory of the access rights that users in that Zone need, and the discrete tasks that they can perform.
- A set of computer roles that characterize the function of a subset of computers.
- A set of user roles that specify the rights (access and privileges) granted to users in that role.
- Role assignments that associate Active Directory users or groups with the user roles



This approach enables you to manage your heterogeneous server environment by tying the rights a user has on a Windows, Linux or UNIX system with a single, definitive identity centrally stored and managed in Active Directory. In so doing, you enjoy a variety of both efficiency and security benefits. Need to give a new employee rights to administer web servers scattered across your enterprise? Assign them to an Active Directory group for web developers. Need to ensure a reassigned system administrator can no longer access any system within her previous department? Remove her from the Active Directory group for that department's admins. Managing your cross-platform environment in Active Directory means you can use Delinea management tools to easily generate regulatory

compliance reports for auditors, assessors, and internal staff that illustrate specifically who has access to which systems, what they can do on those systems, along with who granted the access controls.

Enforce Separation of Duties

Organizations with hundreds or thousands of UNIX and Linux systems are plagued with managing identity on local systems or independent identity stores. With so many independent and often overlapping identity silos, consolidating identity to a single directory can be challenging and time consuming. Most other solutions require an organization to completely rationalize and homogenize all user identities before consolidation can occur.

Centralize User Profiles

Quickly consolidate complex and disparate UNIX and Linux user identities into Active Directory with Centrify's patented Zone technology — without having to first rationalize all user identities. Centrify's Zone technology enables you to manage your heterogeneous environment by tying the rights a user has on a Windows, Linux, or UNIX system with a single identity, stored and managed in Active Directory.

Large organizations may require a hierarchy of zones to manage users who need access to thousands of systems, across multiple departments. Delinea Zones are as simple or as sophisticated, as necessary.

Delegate Access

Easily establish global UNIX identities, manage exceptions on legacy systems, separate identity from access management and delegate administration of groups of systems. Create computer roles, user roles, and role assignments to control access and manage user privileges across your Windows, Linux, and UNIX systems at a granular level.

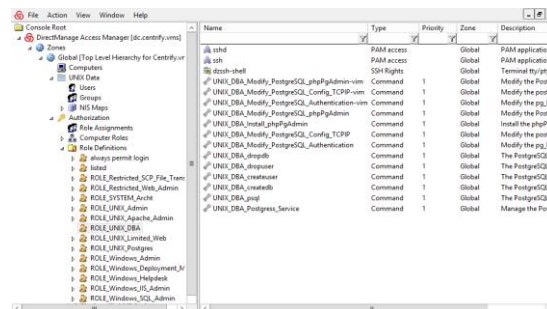
Once roles are configured, it is simple to assign new users to a role, move users from one role to another, or remove users entirely. Delinea Zones enable you to define roles and role assignments at any level within your Zone hierarchy and specify whether those properties are inherited or overridden at any individual level.

Ensure Separation of Duties

Centrify's Zone technology takes advantage of Active Directory's own delegation model to ensure separation of duties. For example, corporate IT staff can retain the privilege to create Active Directory users and computers. Administrators of Delinea Zones need only the authority to change the Delinea Zone data within Active Directory. Windows or desktop admins do not have access to UNIX data and UNIX admins do not have access to user objects.

Least privilege Access & Privilege Elevation

Users need privilege to be able to do their jobs, but root or Local Admin access is far more than they need and giving them out creates unnecessary security risks. Centrally implementing a least-privilege model across Windows, Linux and UNIX minimizes this risk and allows all users access to the exact resources they need to do their jobs. Unlike tools such as sudo, Delinea enables the control of privilege from Active Directory consistently across platforms versus requiring point solutions for Windows and UNIX.



Least Privilege Access

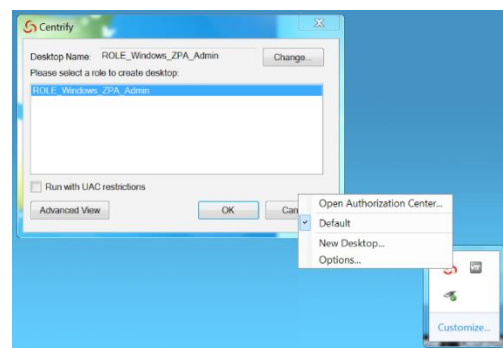
A least-privilege access policy enhances the protection of critical data, improves system and network security, and minimizes the risk associated with user error, malicious attacks, security breaches, APTs, and accidental security incidents, and is often required by industry regulations and security best-practices.

- Eliminate the risks of granting root or Local Admin access by allowing privileged users to login as themselves through Active Directory and elevate privilege through Centrify.
- Control privileges across 450 versions of Windows, Linux, and UNIX with a single solution.
- Assign users a restricted environment with access only to what they need.
- Leverage Centrify's patented Zone technology for scalable management of user or server roles and enable flexible and granular delegated administration.
- Ensure that users log in as themselves through Active Directory (or local accounts when needed), and always enforce their privileges based on a single, centralized identity.
- Monitor any or all sessions and tie activity back to a specific user with an integrated solution for authentication, authorization, and auditing, streamlining audits and proving compliance with regulatory acts and guidelines.

Privilege Elevation

Centrify eliminates the problem of too many users having too many broad, unmanaged administrative privileges. Through granular enforcement of a least-privilege access model, users get access to exactly what they need to do their jobs, but nothing more. The net result is organizations can improve security, reduce risks, and more easily meet compliance requirements.

You can also grant internal users — such as help desk reps, developers, and system administrators — or external users — such as vendors, contractors, or outsourced IT partners — temporary additional privileges for a single project, a short-term assignment or to participate in a program outside their normal job scope.



When a user needs to elevate their access privileges to run a specific application or perform a privileged operation, they can do so quickly and easily. Delinea makes it seamless to elevate privilege based on roles tightly integrated with Active Directory users and groups. And because Infrastructure Services is an integrated solution built on a common technology, privilege elevation can be used as one of the triggers to begin auditing of the user session.

Users can elevate privileges based on Delinea roles that leverage group membership in Active Directory. Users can elevate privileges per-command or open a privileged shell (with whitelisted commands) in Linux or UNIX, or one-click to a specific role or open a privileged desktop in Windows.

On-demand privilege elevation is seamless and eliminates the need to re-enter passwords, check out temporary passwords or submit help desk requests for access while maintaining least-privilege access and increasing security.

IT admins can request access to the specific systems and network devices they need to manage for just the amount of time they need — from anywhere. A simple, intuitive interface enables administrators to request a new role assignment on a specific resource, access to privileged account credentials or to request a privileged session to perform a designated task. Access is granted or denied through an automated, multi-level management approval workflow.

- Allow users to quickly elevate privilege, and optionally require users to re-enter credentials (password or smart card) or prompt for an additional factor of authentication before elevation.
- Restrict the access rights of privileged roles to specific systems, services, or applications, with the ability to enforce privileges by time allotment, job function, system, services, and applications.
- Enable just-in-time privilege via workflow-based management approvals for new role assignments to perform additional tasks, password checkouts or privileged sessions.
- Enforce privilege and privilege elevation in remote connections across the network — not just when users login to specific servers.
- Automatically trigger session recordings based on user, role, system, or privilege elevation to comply with your audit policy.
- Verify that use of privilege is associated with a trouble ticket by executing checks when privilege is elevated.

Complexity in the Many Flavors of Linux *and* AD

When you factor in different versions of Linux, Unix, and Windows AD as a result of mergers, acquisitions, or partial upgrades it gets even more complex. Open Source or products that are essentially a feature of other solutions for AD Bridging and integration tools tend to be tested against a very small number of AD versions. Support for new versions can be a long time in coming, and only if an enterprising person steps up to make a change for the community.

Centrify supports more than 450 OSES and 12+ versions of Windows AD out of the box. It is our business to deliver support of new OSES and versions of AD in a very timely manner. As an example, Mac OS X versions are released on day one, and have been for the past 7 years.

You can see the Delinea list of supported OSES and AD versions supported at:
<http://www.centrify.com/products/all-supported-platforms.asp>.

Rich Active Directory Support

Centrify's Active Directory support, developed and validated through our experience in real-world environments with thousands of servers, make the Delinea Server Suite by far the most enterprise-ready solution for integrating Linux and UNIX systems with Active Directory. Here are some of our most advanced features:

- **Intelligent Domain Controller Discovery.** The Delinea agent validates the domain controllers' health and builds a priority list of domain controllers with a tolerance of stale DNS srv records.
- **Dynamic Domain Controller Selection.** At join and login time, the highest priority domain controller is examined for health, responsiveness, and availability, ensuring a reliable and quick response.
- **Dynamic DNS Selection.** Similar to Dynamic Domain Controller Selection, at login time any DNS queries are sent to multiple DNS servers, with the quickest server response being used. This enhances login speed and reduces bottlenecks and single points of failure.
- **Tolerance of Missing DNS Configuration in resolv.conf.** In large, established *NIX environments, DNS might not exist or be configured on all servers. The Delinea agent can now be configured to work in this environment.
- **Support for Disjoint Namespaces.** In large enterprises, we have frequently found that the DNS namespace is different than the Active Directory domain (for example, centrify.com versus corp.centrify.com). When we join a system to Active Directory, we can add additional aliases so that single sign-on will just work. For example, you can use PuTTY to connect to myserv.centrify.com or myserv.corp.centrify.com and SSO will work as expected.
- **Hardened Support for Complex Trusts.** When a system is joined to Active Directory, enhanced mapping of trust relationships (forest, domain, one-way, two-way, transitive) ensures that the login experience is seamless.
- **Enhanced Network Resiliency.** Additional enhancements have been made to ensure quicker response and failover in a variety of environments, including offline access, VPN (PPTP, IPSEC, Cisco), wireless, and remote across a WAN.

Support for Complex UID Namespaces

Centrify has also found that the open-source approach also does not consider the fact that if you have multiple UIDs for a given user across multiple systems. As a result, you will be in a situation of having to rationalize UIDs. Delinea manages this with its patented Zones technology. Zones provide a flexible means of managing a set of users and computers that all need to share a common set of policies and access controls. For example:

- You can create a Zone for users and their computers, regardless of where they are located geographically or what department they are in
- You can create a Zone for an engineering department whose users must all share access to a set of UNIX development systems, whether located in a data centre or in the cloud.
- You can create a Zone for a branch office that has its own set of administrators tasked with managing all the Windows, Linux, and UNIX systems in their location.

A user can be in multiple Zones, enabling you to create identity management, access control, privilege management and delegation solutions that are as simple or as sophisticated as you need them to be for your environment.

At minimum, a Zone contains a set of users that need to be managed as a group for efficiency or security reasons. Although some organizations will have Zones that contain only users (in particular, a Global Zone, described later), most Zones also contain:

- A set of UNIX management data that defines policies for those users' UNIX profile, such as how users' home directories are assigned (note: "UNIX profile" refers to management data for any Linux, UNIX, or Mac system)
- The set of computers or devices to which these users can be granted access.
- An inventory of the access rights that users in that Zone need, and the discrete tasks that they can perform.
- A set of computer roles that characterize the function of a subset of computers.
- A set of user roles that specify the rights (access and privileges) granted to users in that role.
- Role assignments that associate Active Directory users or groups with the user roles

Restricted Shell

Centrify provides a customized Bourne shell, dzsh, to serve as a restricted shell environment that is used to limit what commands you can execute for certain roles. For most operations, working in the dzsh shell is similar to working in an unrestricted shell except that the command set is limited to the command rights added by the administrator.

Whitelisting refers to the fact that by default, no command is allowed, except for a specific list of commands, which is the so-called 'whitelist'.

Whitelisting is the basic operation of dzsh; without any command definitions in place, dzsh allows a user only to run the built-in shell commands (for a complete list of built-in shell commands on a Linux distribution, run 'man bash' and search for the section 'SHELL BUILTIN COMMANDS').

Blacklisting refers to the ability of denying access to specific commands that would otherwise be allowed. This can be used in two ways:

1. to reduce the scope of a whitelist, commonly used to disallow running a command with specific command line parameters, while running the command with other parameters is allowed.
2. to allow all commands by default, except for the commands in the blacklist.

Beyond Authentication

The reality is that customers, especially ones in well regulated industries, also need to address compliance or security regimens. Therefore, they also need capabilities such as authorization and auditing as part of an “AD Bridge” solution. Here are additional services and solutions offered by Delinea that complement the Server Suite solutions:

- **Privilege Account Management Service** – Delinea offers a secure way to manage shared account passwords, manage those passwords (rotation), manage “run with privilege”, audit, and Monitor all sessions.
- **User level auditing of UNIX user sessions** – Third parties who provide a freebie AD integration utility do not provide a solution for rich user level auditing.
- **AD optimized versions of Samba and SSH and PuTTY** – We test and maintain current versions of our solution for security vulnerabilities against other third party SSH tools regularly.
- **Smart Card support for Red Hat, Cent OS and Mac OS X and Windows.** People want multi-factor authentication as they get more security conscious.
- **Authorization and auditing tools for Windows environments** that plug into the management tools we use for AD/UNIX. Vendors such as Red Hat do not address security needs in your Windows environment.

Supportability Over Time

Your talented staff may in fact get something like Winbind to work in your environment, but the reality is how much time is set aside for them to go back and test it out if you upgrade to R2 of Windows 2012 or beyond? If you bring in SUSE or Linux Mint (i.e., a different OS vendor than Red Hat) into your shop, many of those vendors may not even support SSSD, and what you built on RHEL to get AD integration working will not easily “port” over.

Another scenario Delinea has seen often is that the person who built this homegrown and free “AD glue” leaves the organization, so the knowledge is now gone. Given all this, a typical question that arises in these scenarios is who in the organization are you going to call if there is something wrong or if a new OS or updated environment enters? Again, not to say you or your organization cannot do this, but is this where they want to spend your time?

Purchasing Delinea means you purchased a resource that will manage and maintain the product you use over time. We will maintain software that is guaranteed to work against basically any *nix OS and any AD you have — or will have — and you will have SLA's that are in place, no matter how complex your environment.

Deployment Options and Services

The fact is that most free AD join solutions out there are built by a small team of software developers with no professional services to help you deploy. Delinea is committed to ensure you are successful in deploying our solution in several ways:

- Centrify provides deployment tools optimized for AD that do a pre-install check to make sure the *nix environment can integrate with AD, can push out the software (new installs and upgrades), etc.
- Centrify also provides reports on who can access what, what systems have our AD agent, what versions, etc.
- Centrify provides other management tools including plug-ins into Active Directory Users and Computers. So, there is a whole reporting and management layer for the AD integration you do not get with SSSD or Winbind.
- Centrify has a community of thousands of admins who comment on our solution all the time and give us pointers and support each other, etc.
- Centrify has bloggers who just blog on our solution. So, we have an ecosystem around our products to make our solutions better. See <http://centrifying.blogspot.com/search/label/Business%20Problems> and <http://community.centrify.com/>.
- We have experienced professional services people who have done hundreds of successful deployments, each with years of experience with Delinea.

We have a global user group annually, and regional user groups are forming now to enhance your experience with Delinea products.

Account Lifecycle Manager

Delinea's Account Lifecycle Manager is a solution that automates and streamlines service account governance, finally allowing you to control service account sprawl. Now you can easily secure, provision and decommission service accounts to harden and ultimately shrink your attack surface with Account Lifecycle Manager.

Account Lifecycle Manager empowers you to manage and control service accounts with workflows, automated provisioning, governance, compliance, and decommissioning capabilities. Account requests follow approval workflows tailored to your organization. Now IT and security teams can control service accounts and mitigate the risk of breaches, service interruptions and human error.

Service Account – Full Lifecycle Management

Many customers struggle with service account sprawl, as well as orphaned and “unowned” service accounts. Account Lifecycle Manager (ALM) is a unique tool from Delinea that, with a workflow-driven approach, allows customers to take back full control of the creation, in-place use, and automated decommissioning of service accounts through the IT infrastructure. All of the workflows built into the tool are highly extensible and can be integrated with a large range of external platforms, including Delinea Secret Server, meaning that privileged accounts can immediately be stored in an encrypted manner and have passwords generated for them, once the creation workflow in ALM has been completed. These accounts will also be created on the appropriate directory or host, such as Active Directory, and then be made available for use only subject to the strict role-based access controls featured in Secret Server. This allows customers to minimize access to service accounts completely – the integration with Secret Server even meaning that privileged accounts can be utilized without the user even knowing the underlying password.

The solution also features ownership and decommissioning workflows, automatically meaning that G-Cloud Clients will have a superior level of governance over service accounts – easily being able to determine why a service account is in place, who owns it, what it is used for and also what services *are dependent on* the service account itself. Renewal lifecycles mean that after a certain point in time (configurable on a per account basis) the account must be actively renewed and its purpose reinstated, or it can be fully deleted from the environment and removed as a possible privileged attack vector.

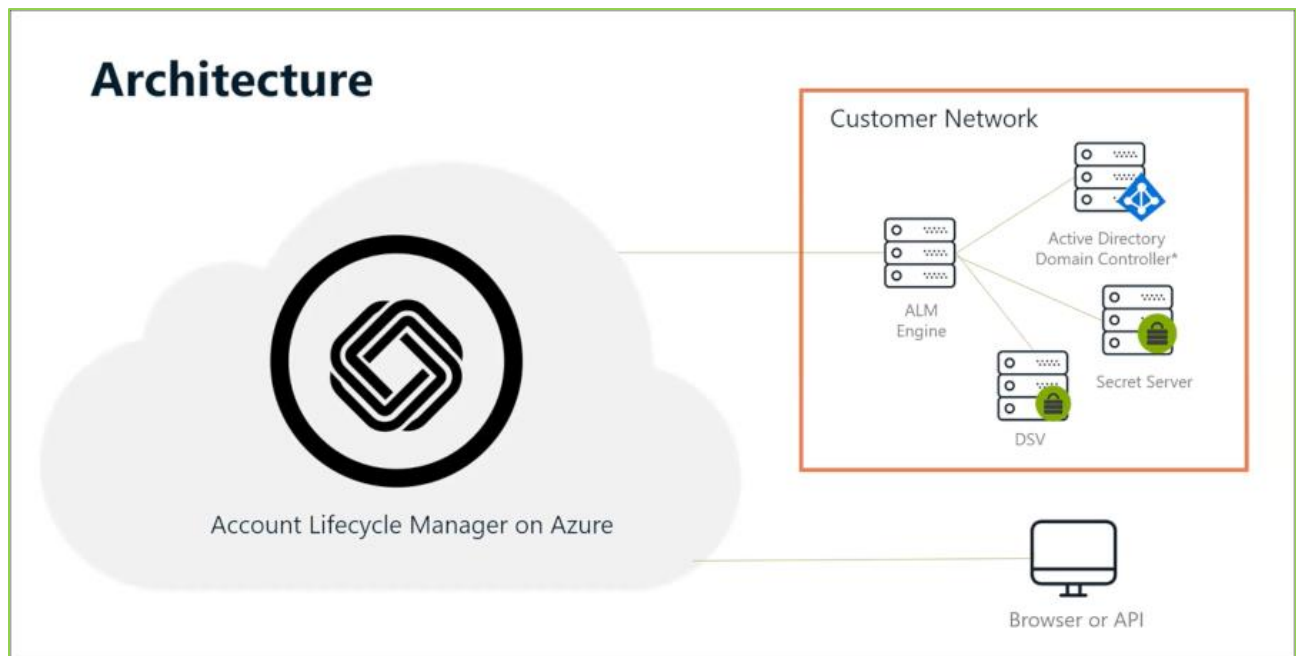
The tool has been leveraged by some of the world's biggest organizations to regain control of service accounts, thus minimizing their privileged attack surface and reinstating accountability for the creation and use of these important privileged accounts.

ALM Architecture

Account Lifecycle Manager (ALM) is a fully SaaS solution also available as On-Premise Solution

Cloud Architecture

Account Lifecycle Manager (ALM) is a fully SaaS solution that can be made available in minutes. The solution is hosted in Microsoft Azure and fully managed by Delinea, with maintenance, upgrades, infrastructure, and automated resiliency and failover all handled natively.



Also available as on-premises software to deploy on physical or cloud servers in customer environment

Functionality



Establish Workflows

Admins can define workflows for provisioning process. Required approvals can be set for each type of account request. Account requests follow approval workflows tailored to your organization.

Delegate Ownership

Role-based permissions govern user access, setup, and the request workflow. Several roles come already set up, including System Admin, Account Owner, Requesters, and Approvers. Organizations may create additional roles to support their specific business needs. Separation of duties (SOD) is allowed through an approval process created by the admin.

Provision Accounts

Manage and control service accounts with automated provisioning. Admins can create account templates that specify how an account will be created.

Enforce Governance

Create accountability and ownership over service accounts. Easily audit accounts for compliance through account searches and reporting and logging.

Decommission Accounts

Decommissioning of service accounts enabled without service disruptions. Easy notifications when accounts should be renewed or re-approved. Control service account sprawl and harden your attack surface.

DevOps Secrets Vault

The challenge

DevOps is moving toward **Continuous Integration and Continuous Delivery (CI/CD)** to build and deploy software updates faster and more efficiently. Cloud services have **accelerated the speed and scale of DevOps pipelines**, scaling up to tens of thousands of containers, servers, and applications (micro-services) being rapidly deployed across Dev, Test, and Prod environments. Every container, server, and micro-service can have privileged access, dramatically **increasing the attack surface** for intruders looking for an entry point.

Even when DevOps and DevSecOps teams are making efforts to protect and secure privileged credentials within pipelines, this means using several disparate solutions making centralized auditing, visibility, and control impossible.

The solution

Delinea DevOps Secrets Vault (DSV) provides a CLI / REST API driven PAM solution capable of meeting the high velocity workloads DevOps tools generate. This gives DevOps teams a specific tool within the Delinea platform to provide the unique requirements traditional PAM tools cannot meet.

- Advanced automation – Command-line interface (CLI) and REST API
- Serverless architecture – API built on AWS
- Infinite scalability – no need to add servers
- Speed and agility – with microservices
- High availability – 99.999% availability
- Disaster recovery – hot standby for rapid switchover
- Local caching – high-performance workload handling
- Cloud authentication - supports AWS, Azure, GCP, and Delinea One
- Dynamic secrets – AWS, Azure and GCP
- Certificate issuance – X509 leaf certificates issued from root or intermediate certificate
- Sandbox tenant available – test before deploying to production
- Compliance – SOC 2 Certification

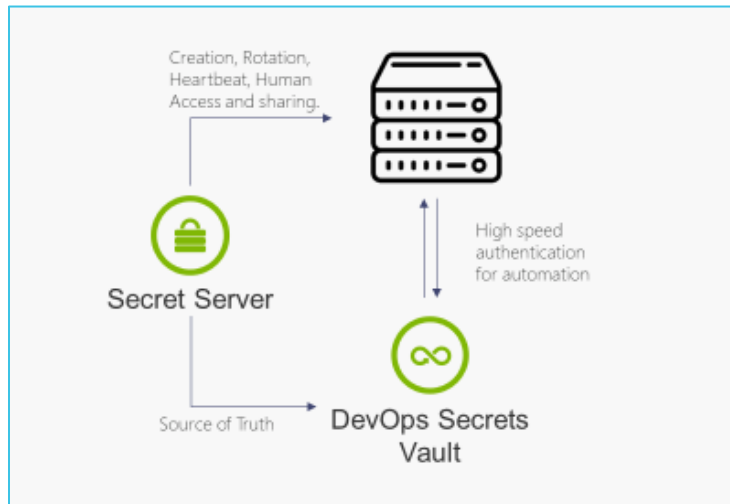
Integrations

The DSV solution is designed to be highly flexible and adaptable. The CLI and REST API can be used to integrate the solution with any platform. Delinea also provide a robust and ever-increasing range of out of the box integrations:

- Languages/ tool support
- DevOps tools: Jenkins, Kubernetes, Terraform, Ansible, Chef, Puppet
- RPA tools: UiPath Orchestrator
- Languages: Java, Go, Python, Ruby, and .NET

Integration with Secret Server

To ensure a central viewpoint of audit and control is applied across all teams, Delinea Secret Server and DevOps Secrets Vault can be fully integrated. The diagram below highlights the typical functions that the side-by-side solutions provide.



Architecture

Delinea DevOps Secrets Vault is hosted within AWS and managed by Delinea. The serverless architecture provides a highly resilient, scalable solution capable of meeting the velocity of programmatic API interaction generated by CI/CD pipelines and other DevOps tools.

As with all Delinea SaaS products, DSV is SOCII certified providing piece of mind that the solution and data within is kept secure.

Delinea Support

Delinea have an award-winning support team to help you resolve any issues and get the most out of your products. Delinea offer clients a standard support package as well as Premium and Premium+ support package with more coverage, 7x24hr, and quicker response times. We operate a comprehensive 24x7, follow the sun, support operation with support offices in the US, UK, Philippines, and Australia. More details regarding our support services can be found on our website <https://delinea.com/support> along with the full support policy covering all support options and conditions.

All support calls are logged in our ticketing system and can be tracked fully by both the client and Delinea. Our Support and maintenance licences include email and telephone technical support, upgrades and patches to our software, and access to our support portal with admin guides, knowledge base articles, how to video, and other documents and discussion forums.

More information about our support services and processes can be found in our Support guide <https://delinea.com/support>.

Support Portal

Delinea have support portal, <https://thycotic.force.com/support/s/>. There is limited access to the portal for all users however all clients under support contracts have full access to the portal using their assigned user login. The support portal includes all admin guides, knowledge base articles, how to videos, and other documents and discussion forums. The support portal also includes information on your products, licence keys and support dates.

Support SLA Summary

Below is a summary table of the Secret Server SLA by product and Support type.

	Standard Support	Premium Support	Premium+ Support
Business Hours Monday through Friday, except major holidays	Americas 8am – 8pm ET EMEA 8 am – 8 pm GMT APAC 8 am – 8 pm PHT Middle East 8 am – 8 pm Sunday -Thurs (UAE)	24x7x365	24x7x365
Severity 1 (Critical/ Severe)	2 business hours	1 hour 24/7	1-hour response 24/7
Severity 2 (Major)	6 business hours	4-hours response 24/7	4-hours response 24/7
Severity 3 (Partial)	8 business hours	6 business hours	4 business hours
Severity 4 (Minor/ General)	24 business hours	12 business hours	24 business hours
Severity 5 (Feature request)	24 business hours	24 business hours	24 business hours
Correspondence / Response	Phone, Case, Email	Phone, Case, Email	Phone, Case, Email
Online Tools	Knowledge Base, documents, downloads, release notes	Knowledge Base, documents, downloads, release notes	Knowledge Base, documents, downloads, release notes
Product Releases and Notifications	Product UI notification or webpage downloadable	Yes	Product UI notification or webpage downloadable
Live Phone Support	Yes	Yes	Yes
Cloud Status Page	Yes https://status.thycotic.com	Yes https://status.thycotic.com	Yes https://status.thycotic.com
Maintenance & upgrade Notification	Yes	Yes	Yes

Delinea Training

Delinea solutions are easy to deploy and intuitive to use however Delinea have a professional services and training teams that can provide G-Cloud Clients training based on G-Cloud Clients's requirements. Further details of the training package can be found in Appendix 3 - [delinea-datasheet-training-professional-services.pdf](#) or <https://delinea.com/training>.

While Delinea solutions are easy to deploy and intuitive to use, Delinea offer a range of training options.

- E-Learning – Predefined courses available on-line for people to complete in their own time
- Certification Administrator Training – Advanced online training to become a Delinea Certified engineer
- Admin training – 3-day Instructor led training delivered on site, Covid permitting, or remotely, covering standard administration and use cases.
- Business user training – training delivered remotely covering standard cases.
- Instructor Led Client Specific training– 3-day Tailored to each clients need in the location of your choice or delivered virtually via remote video conferencing.
- Additional Professional services training – Professional services days can also be used to cover specific training needs by agreement.

Delinea Training Methodology & Framework

Delinea's methodology for training and enablement follows a simplistic model: Educate -> Reinforce -> Assess. Our recommended training process is defined as a combination of reading, hearing, seeing, and doing to offer learners both active and passive learning options to accommodate personal preferences. Delinea's recommends both instructor-led training and E-learning. Both provide unique value and together represent the most comprehensive learning package offered by Delinea. Instructor-led training gives learners the ability to customize models and hands-on labs to their environment, ask questions about use cases or best practices and test configurations in a safe, lab environment. Compared to E-learning which offers much deeper learning on more topics, with quizzes for validation of knowledge and continuously updated to enable education on Delinea's most current product capabilities and solutions.

Delinea's Instructor-led training

Delinea's Instructor-Led Training is three days of classroom-style instruction with informative slides, hands-on labs, and Q&A sessions with a Delinea expert. Delinea's Instructor-Led Training is custom and adapted to your organization's use cases, current knowledge, and deployment type. Hands-on labs provide students the ability to easily practice, test, and discuss alternative configuration options in a safe, non-production environment. Students are also given the option to rent lab environments for additional on-going sandbox learning and testing.

Delivery

The training will be delivered on site or remote, instructor-led by a certified Delinea Professional Services or Training professional (this may include Delinea Certified Partners or Delinea employees). The trainer will use both PowerPoint slides and hands-on labs for delivering training.

The labs are critical to ensure that learners are knowledgeable of configuration options, best practices and use cases. Labs provide an opportunity to:

- Build hands-on experience with Secret Server in a risk-free training environment.
- Build confidence in case of disaster recovery and to help with planning for future use cases.

Sample Schedule

The schedule below will vary depending on the skill level of the attendees and use cases that the Customer would prefer to focus on:

Day 1

Content	Delivery
Introduction to Delinea Secret Server, main use cases, and labs setup	Lecture, slides and hands-on lab
User Interface Secrets and Templates Folders and Policies	Lecture, slides and hands-on lab
Roles, Groups and Users	Lecture, slides and hands-on lab

Day 2

Content	Delivery
Workflow Launchers Discovery Remote Password Changing	Lecture, slides and hands-on lab
Service Account Management Auditing & Reporting Alerting & SIEM	Lecture, slides and hands-on lab
Distributed Engine SSH Key Management & Whitelisting	Lecture, slides and hands-on lab
Security Hardening	Lecture, slides and hands-on lab

Day 3

Content	Delivery
Session Recording & Monitoring Integrations	Lecture, slides and hands-on lab
SSH/Process Custom Launcher SSH Password Changers Extensible Discovery	Lecture, slides and hands-on lab
Backups High Availability Upgrades	Lecture, slides and hands-on lab
Vault Troubleshooting Cross-Functional dependencies Wrap up and Questions	Lecture, slides and hands-on lab

The offering has a fixed price which is for a fixed set of hours. Since customer environments vary significantly, we do not expect to complete the entire list of items listed above during this engagement. Instead, Delinea will work with the customer during the first phase of the engagement to establish a mutually agreed upon subset of the above items that fits within the allotted hours.

Delinea's E-learning

Delinea's Training & Certification programs also include an E-learning offering. With over 100 E-Learning courses, Delinea's digital learning program emphasizes self-paced learning for students juggling work, personal, project, cyber-security, and training priorities. Each Delinea course includes a quiz for validation of knowledge and, if successfully passed, a course completion certificate. Topics range per solution but sample topics include:

- Installation, Upgrades, & Basic Configurations
- Best Practices & Security Hardening
- Auditing, Reporting, & Monitoring
- Discovery & Workflow
- APIs, Scripting, & Integrations

Project Overview

Delinea solutions are easy to deploy and intuitive to use however Delinea have a professional services team that can provide G-Cloud Clients expertise and assistance to ensure the solution is designed, implemented, configured, and utilised according to Delinea best practices and to train your team to help you drive rapid adoption of the solution and maximize the return on your investment.

Delinea offer a range of Professional Services packages that are designed to help G-Cloud Clients implement the solution and gain proficiency and become self-sufficient quickly.

For enterprise clients or those that have more complex requirements, Delinea offers custom professional service offerings. Our consultative approach produces an engagement that is a perfect fit for our client's specific needs and has resulted in successful implementations at a range of Fortune 500 organizations including enterprise deployments on some of the world's largest networks.

Delivery of Delinea professional services can be provided remotely or onsite with many customers choosing an initial onsite engagement followed up with remote activity and intermitted on site visits.

Once deployment is complete the support portal and team are there to help you with your Delinea solutions. Please also see Support Policy for more details at <https://delinea.com/support>

Professional Services Team

Delinea Professional services team consists of the following different units:

- Technical Consultants
- Solutions Architects
- Project Managers
- Scripting and customization experts
- Documentation Experts
- Advisory Services
- Penetration Testing (Red Team) Services

Globally, Delinea has over one hundred fully certified, experienced professional services consultants. This ensures our ability to provide local presence in any country. All project phases are managed by an assigned Project Manager within Delinea who will be responsible for ensuring that throughout the life of the project, architects and consultants are deployed as required to ensure key deliverables are met and the each phase is completed successfully.

Implementation Approach

This section outlines professional services package option for G-Cloud Clients covering the following items:

- ✓ Installation of Secret Server and its components, and Delinea Products with direct Delinea assistance
- ✓ Learn how to configure a PAM solution from the ground up, with all teams involved.
- ✓ Configure a multi-tiered network infrastructure.
- ✓ Ensure all features of our products are utilized to maximize your organization's security posture.
- ✓ Implement Privileged Account Management best practices.
- ✓ Provide Project management support
- ✓ Provide workshops to support the definition of a customized architecture

The project delivery is divided in 4 distinct phases:

1. Project Initiation
2. Technical Pre-Implementation workshops and architecture review
3. Implementation phase – either Pilot or production Installation and configuration
4. Training and handover

Please note that the actual timescales will be reviewed after the pre-implementation and architecture workshops have taken place and availability of the relevant teams will be confirmed.

Delinea is happy to review together with clients the list and priority of the specific applications requirements during the architecture and pre-implementation workshops.

Project Governance

Whether the project is large or small, Delinea's implementation of the solutions is reliable with a consistent project methodology and workflow based on PMI and Prince2 standards. This process can be used to drive adoption as well as ensure that the solution is deployed satisfactorily from an architecture and security standpoint.

Delinea use project management tools such as Mavenlink and Smartsheets to manage the project as well as other documents and tools to track issues and manage risks.

Project Team

During the implementation, the Delinea team will be made up of a team of professionals that will fulfil the roles and responsibilities required by the project as detailed below. The project teams will provide Delinea consultant(s) with any supporting information, data, and documentation necessary to ensure the development of appropriate deliverables. Below are the typical project teams for Delinea projects.

Delinea Project Team

Role	Responsibility
Project Sponsor	✓ Delegated authority / oversight of whole project ✓ Escalation point for all key issues that have not been resolved by Project Manager
Project Manager	✓ Primary line of communication for the project between Delinea and G-Cloud Clients ✓ Ensure Delinea resources are available, and tasks and milestones are completed according to the agreed schedule ✓ Direct activities of the Project Team and other resources appointed to the project ✓ Resolve disputes and issues that arise in the course of the implementation ✓ Escalation point if required during the project
Senior Consultant /Architect	✓ Provide project Support for scoping discussions and formulate design for the solution to meet G-Cloud Clients's requirements and environments.
Consultant/Engineer	✓ Responsible for delivery of the project including configuration, scoping and completion of Requirements Document ✓ Responsible for articulating requirements to G-Cloud Clients as to what G-Cloud Clients needs to do to set up the environment in preparation for implementation

G-Cloud Clients Project Team

Below is the typical project team and roles required from the G-Cloud Clients for Delinea projects. The roles and responsibilities may be assigned one or more persons as required by G-Cloud Clients. The project assumption is that G-Cloud Clients will ensure timely access to the appropriate stakeholders and staff for consultation.

Role	Responsibility
Project Sponsor	✓ Delegated authority / oversight of whole project ✓ Final acceptance sign-off on project
Project Manager	✓ Oversee all aspects of the project ✓ Approve or reject change requests and therefore budget for project ✓ Communicate progress of project deliverables, budget, and timeline in relation to scope document and project plan ✓ Ensure appropriate resources are available and tasks and milestones are completed according to the agreed schedule ✓ Direct activities of the Project Team and other resources appointed to the project
Project Steering Group	✓ As identified by G-Cloud Clients ✓ Communication and ownership of the software to increase awareness; build desire and enthusiasm and obtain buy in from stakeholders ✓ Aim for one per division
Technical Lead	✓ Oversees any technical assistance required from the G-Cloud Clients side, including integrations, data migrations etc.
System Administrator	✓ Full system administration including security ✓ This role will continue beyond the project for ongoing support to key stakeholders internally
Key Business Users	✓ Resource and task management ✓ Communicate to project team members ✓ Test the system for their component

Implementation Approach & Key Deliverables

Below are the typical phases for Delinea professional service projects.

Phases:	Purpose	Approach
Phase 1: Project Initiation	To discuss the implementation process with the G-Cloud Clients that ensures there is a clear understanding of what is to follow. Preparation for implementation is undertaken.	✓ Gather and review existing documentation and processes ✓ Project set up ✓ Kick off meeting
Phase 2: Scoping	To establish an implementation plan that outlines the project team, project scope, objectives and system requirements that is documented and agreed upon by both parties. Further, during this phase all relevant information to G-Cloud Clients's current business process is collected and reviewed.	✓ Scoping session to determine G-Cloud Clients system requirements ✓ Development of Project Requirements Document (PRD) ✓ Review and approve PRD with G-Cloud Clients
Phase 3: Configuration	To establish and configure the environment, applying relevant software parameters, and configurations. Systems integration is also undertaken.	✓ Ensure G-Cloud Clients environment is ready for the deployment of the software ✓ Establish if the application will be hosted on the Delinea cloud or on client Premise ✓ Delinea to complete configuration and check points to confirm approval by G-Cloud Clients ✓ Delinea will complete Integration where applicable ✓ Configuration sign off lies with the G-Cloud Clients
Phase 4: Training and UAT	Facilitating user training across the different users Ensure that the application is ready to "Go live". Including testing the environment to ensure it meets G-Cloud Clients's expectations and it is as per the Requirements document specification. Resolving any outstanding issues. Administrator training is also undertaken in preparation for User Acceptance Testing (UAT) by G-Cloud Clients.	✓ Admin training with core project team ✓ UAT period with Admin group to confirm configurations, integration in line with the Requirements Document ✓ G-Cloud Clients to undertake testing within Test environment ✓ Clients are required to formally sign off on completion of each user acceptance testing. In case of no response from the Customer within the agreed timeframes, Delinea will take it as a sign off and official completion of the UAT sign off period.
Phase 5: Project Closure	The application is ready to 'go live'. G-Cloud Clients signs off go live documentation. PS team completes the PS to account manager handover document. PS team sends out the Client survey. Final project status report is completed issues register, risk register and Lessons learnt register are updated.	✓ The solution is verified to ensure it behaves as predicted and G-Cloud Clients implementation team transitions support to its operations, or 'business as usual', teams. ✓ G-Cloud Clients to sign off Project closure ✓ G-Cloud Clients to complete Survey
Phase 6: Development & Operational Handover	Final Deployment occurs and G-Cloud Clients is transitioned to the Account Manager.	✓ Following Go Live sign off, Delinea will introduce G-Cloud Clients to their Account Manager
Phase 7: Post implementation	Optional Post implementation reviews and health checks can be scheduled if required.	

Project Communication Plan

The table below outlines a typical communication schedule to meet the project milestones.

Communication	What	Frequency	Who	Output
Project Progress	- Regular progress meetings - Project Steering Group Meeting (risks, issues, escalations, and project direction)	- Weekly (or as agreed) - Monthly (or as agreed)	- Delinea and G-Cloud Clients PMs and POs - Delinea and G-Cloud Clients Project Sponsors / Senior Management (and PMs and POs)	Delinea Progress Report
Issues / Risks	Key risks or issues to be logged within Delinea project and discussed and documented as part of internal and G-Cloud Clients progress meetings	As required	Delinea Project Manager	Documented in Delinea Progress Report
Escalation	Escalation of any issues, scope variation etc.	As required	Delinea and G-Cloud Clients Project Manager or Sponsor	
Key Project Sign offs	Sign offs include: - Requirements Doc - Configuration - Integrations - Training/UAT - Go-live	As documented in the project plan	G-Cloud Clients Project Manager	Sign sign-off documentation

About Delinea

Delinea is a leading provider of privileged access management (PAM) solutions for the modern, hybrid enterprise. We make privileged access more accessible by eliminating complexity and defining the boundaries of access to reduce risk, ensure compliance, and simplify security. Delinea empowers thousands of customers worldwide, including over half the Fortune 100. Our customers include the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. delinea.com