



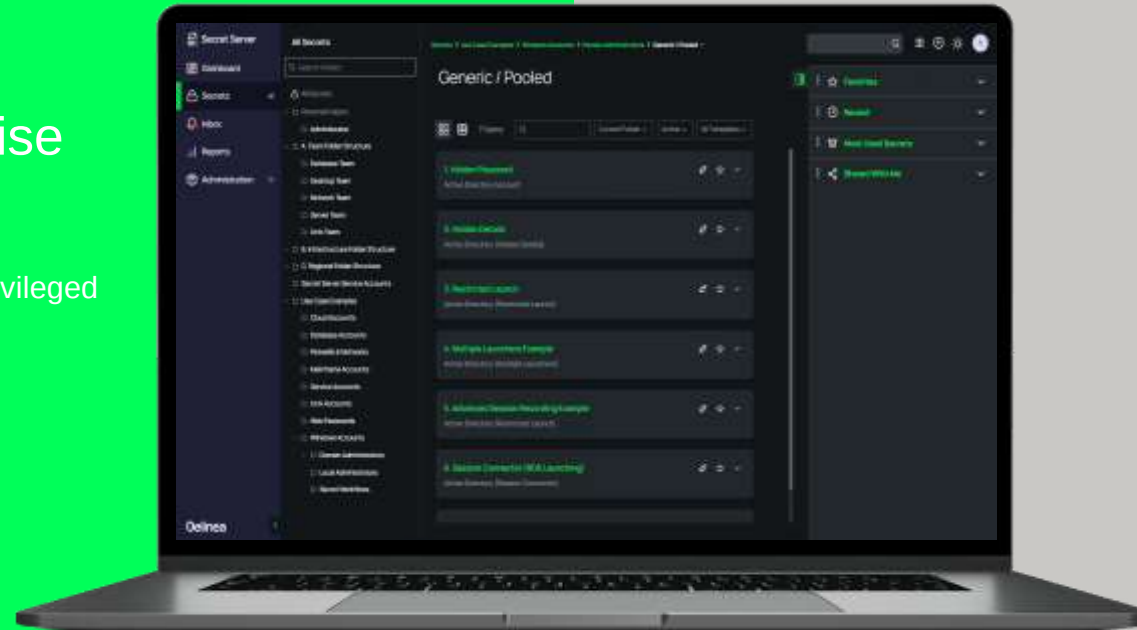
Secret Server: Privileged Access Management



Secret Server

Privileged Access Management at Enterprise Scale

Discover, manage, protect, and audit privileged account access across your organization



Establish vault



Discover unknown Accounts



Delegate access

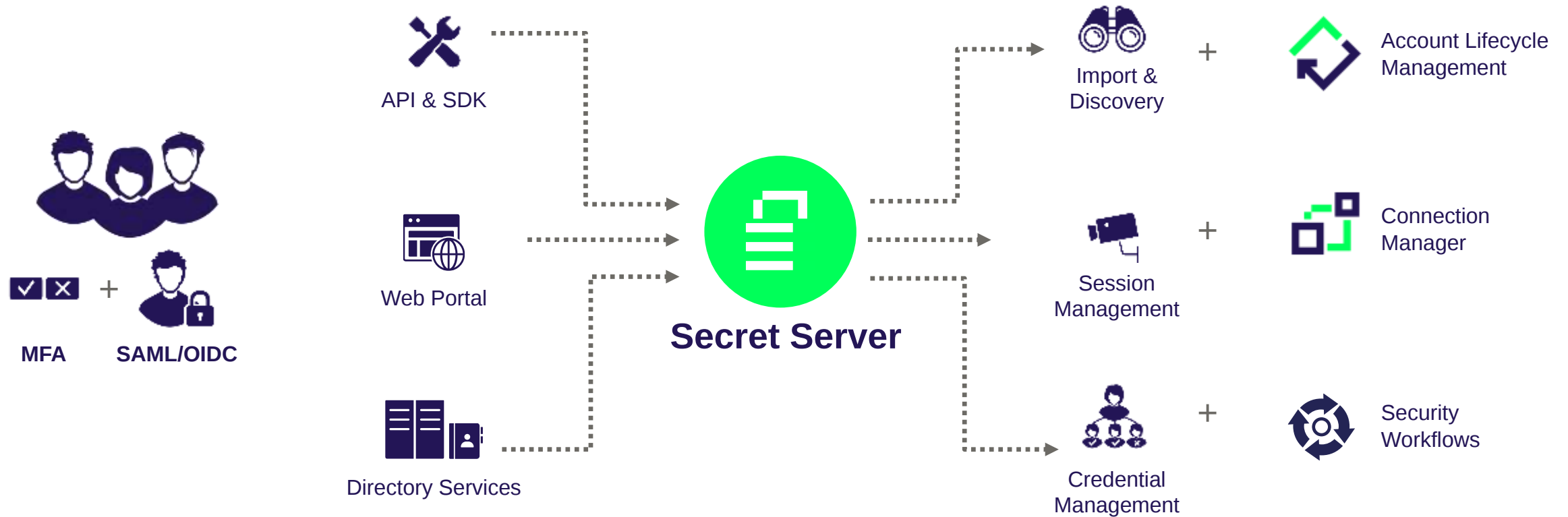


Manage secrets



Control sessions

Secret Server Overview



Account Lifecycle Management (Create, Import & Discover credentials)

- Manual creation
- Quick Initial and Ongoing Importation of Network Credentials
 - Protection Against Backdoor Accounts
 - When Secret Server is configured to discover new accounts, it provides added protection by regularly running discovery on your network to identify those accounts. Secret Server adds the new accounts to its records and resets the accounts password to values that meet your security policy.
- Discovery Types
 - Active Directory Discovery
 - Scans for local accounts, domain accounts, scheduled tasks, Windows services, and IIS application pools. You can discover additional accounts and dependencies by creating PowerShell scanners.
 - ESX/ESXi Discovery
 - AWS Discovery
 - Google Cloud Platform Discovery
 - Unix Discovery

Account Lifecycle Management (Secret Management)

- Deactivating and Reactivating Secrets
- Remote Password Changing
 - Automatic Remote Password Changing
 - Schedule Password Expiration
 - Heartbeat
 - Check in / check out
- Creating Secret Policies
- Secret-templates [Built in secret templates](#)

- Folders

Folders in Secret Server allow you to organize your secrets into logical groups and control access through permissions assigned to the folders.

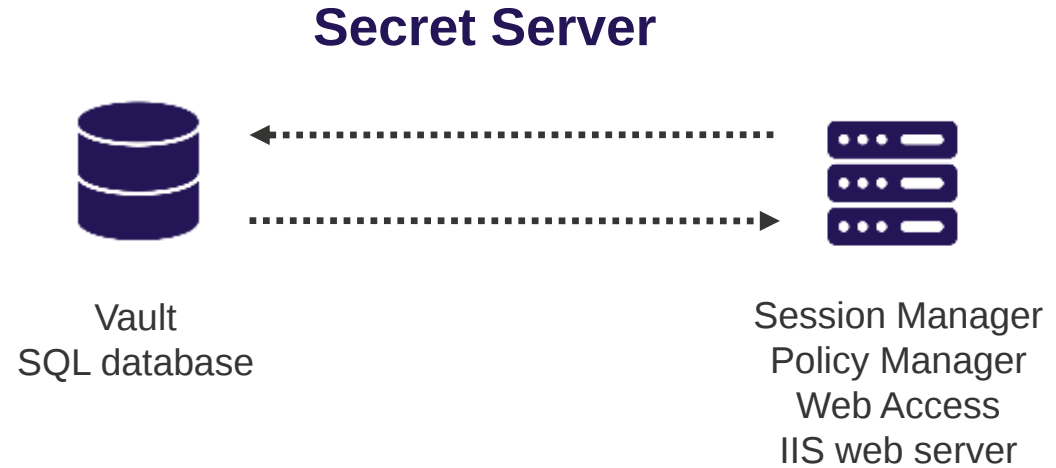
- Secret Launchers and Protocol Handlers
 - RDP
 - SSH
 - Custom (eg. WEB)

- Access Requests

The [access](#) request feature allows a secret to require approval prior to accessing the secret.

Architecture

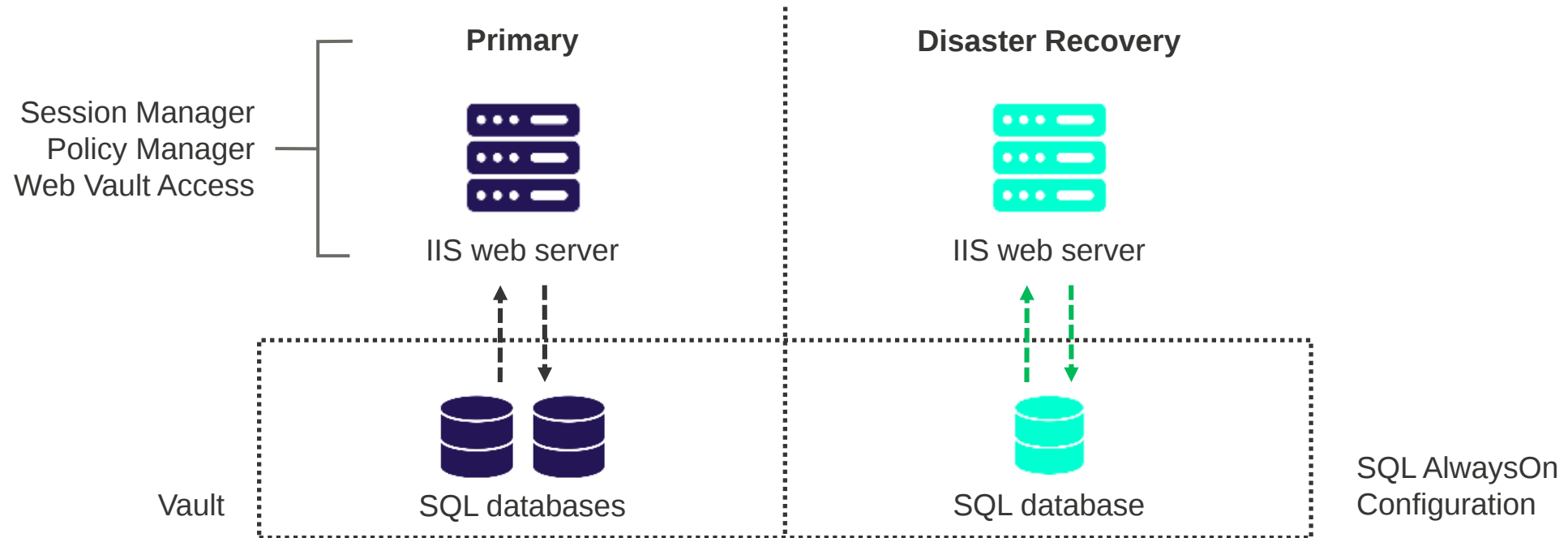
- Single IIS web node
- SQL Server database
- SQL on web node or dedicated server



- **“Off the shelf” common components**
- **Easily scales down to two servers**
- **Minimal complexity**

Secret Server – Installed

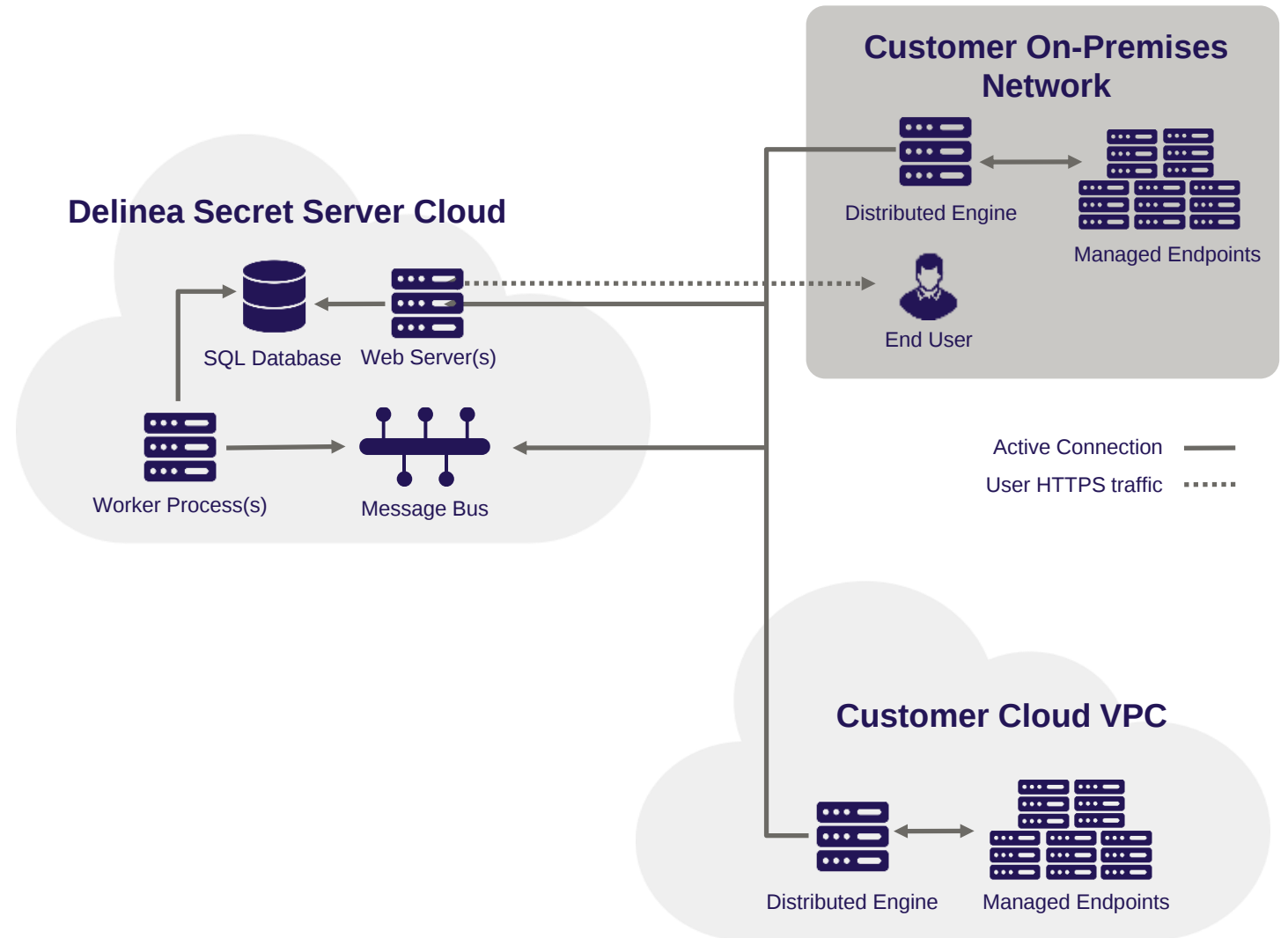
HA/DR Deployment Architecture

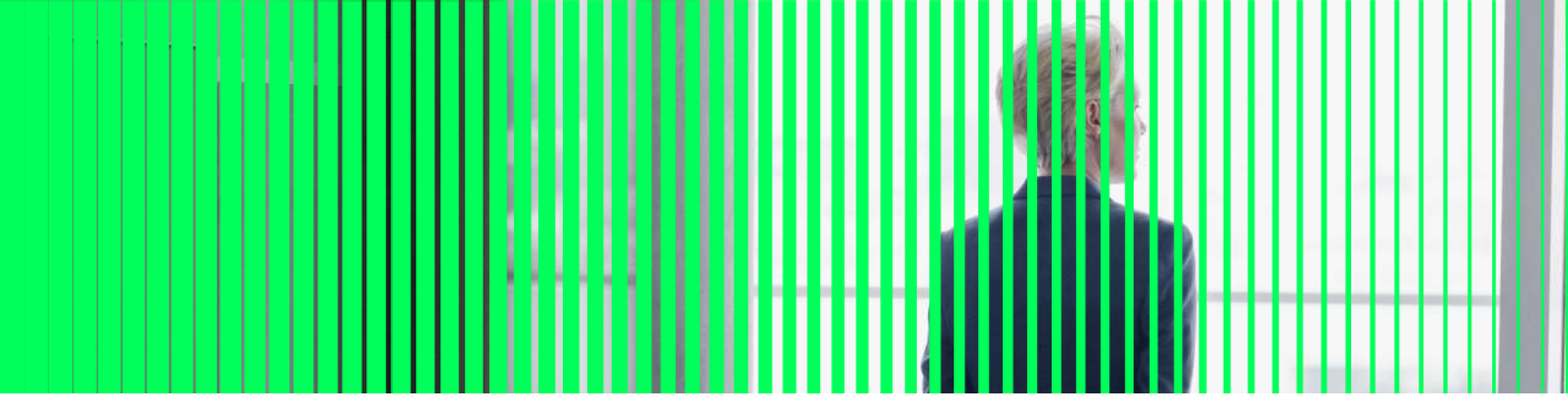


- “Off the shelf” common components
- Minimal complexity

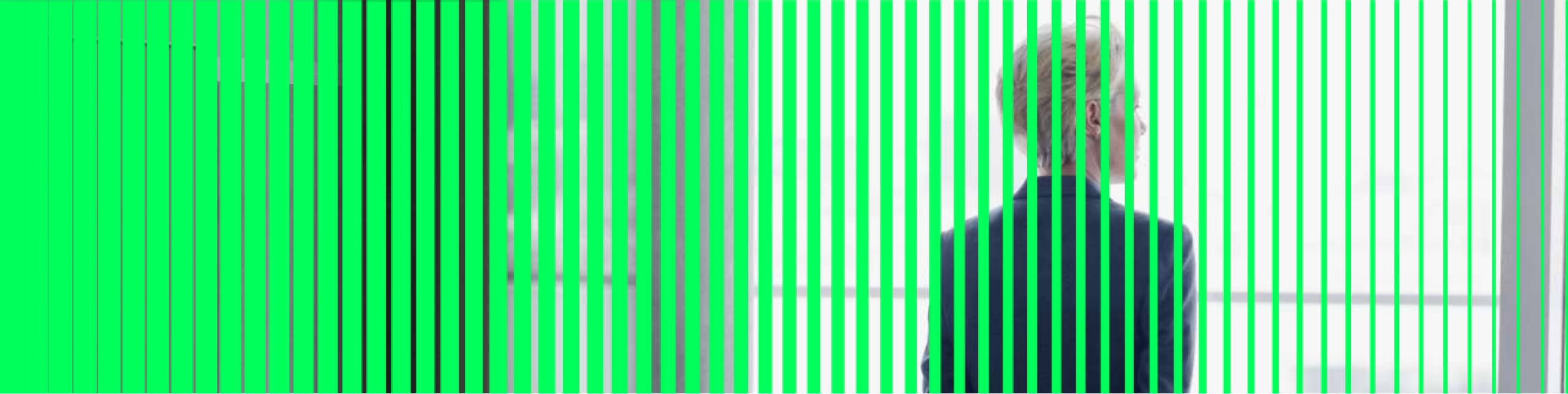
Secret Server

- DE facilitates Directory Services integration, password changing, discovery, RDP/SSH proxying and more
- Only outbound connections to SS Cloud (port 443)
- Multiples can be used for HA
- Not required for accessing Secret data
- DE upgrade automatically
- DE is only on-premise component





Centralized Auditing



Every action within Secret Server is audited!

- ✓ User Access
- ✓ Administrative actions
- ✓ Permissions
- ✓ Configurations
- ✓ Active Security
- ✓ Compliance
- ✓ Activity

- 60+ Reports out of the Box
- Customizable with SQL queries
- Receive automatically on a schedule

Ex. User Audit Report: From report, directly trigger password rotation for “expired secrets”

User Audit

Use Case: User leaves the organization

The audit search displays results for all the secrets the selected user has viewed or edited during the selected time period. The administrator has the option of expiring all the viewed secrets, to notify users to change sensitive information, or to force password changing.

Secret Server

Dashboard

Secrets

Inbox

Reports

Administration

Delinea

User Audit Reports

GeneralSecurity HardeningUser Audit

This report shows all Secrets accessed by a particular user during the time period specified.
Note: Only Secrets for which *you* have access are displayed.

User:

DHughes

 From:

1/1/2022

Show Inactive Users

Exclude Rotated Secrets

Exclude Inactive Secrets

to:

11/7/2022

< All Folders >

☒ Include Subfolders

Search History

Expire Now

Save To File < 1 to 24 of 24 >

SECRET NAME	SECRET TEMPLATE	FOLDER NAME	IP ADDRESS	LAST DATE	STATUS
1. Checkout Example	Active Directory Account	Secret Workflows		10/14/2022 01:25 AM	Active
1. Checkout Example	Active Directory Account	Secret Workflows	172.31.32.118	10/14/2022 01:25 AM	Active
1. Hidden Password	Active Directory Account	Generic / Pooled	172.31.32.114	8/5/2022 06:29 AM	Active
1. Hidden Password	Active Directory Account	Generic / Pooled	172.31.32.118	10/14/2022 02:25 AM	Active
1. Hidden Password	Active Directory Account	Generic / Pooled	fe80::5802-654b-afa-9919%2	9/22/2022 11:51 AM	Active

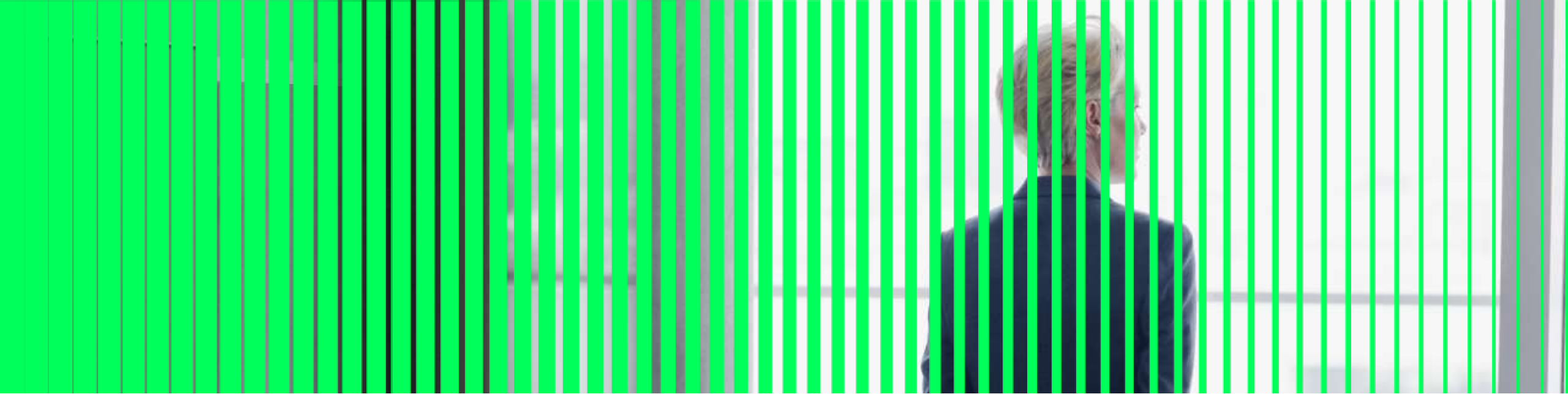
Auditing

Secret Audit Log

The audit log for a secret can be accessed by clicking the View Audit button on the Secret View page or navigating from the User Audit report. The log shows the date, the username, the action, and any other details about the event. Secret auditing provides a detailed view of each change or view on a secret.

The screenshot displays the Delinea Secret Server interface. On the left is a navigation sidebar with options: Secret Server, Dashboard, Secrets (selected), Inbox, Reports, and Administration. The main content area is titled 'All Secrets' and shows a search bar and a tree view of folders. The selected secret, '1. Hidden Password', is displayed in a detailed view. This view includes tabs for General, Security, Audit (selected), Remote Password Changing, Dependencies, Sharing, Settings, and Metadata. The Audit tab shows a list of 187 items, with a toggle for 'Display Password Change Log' set to 'On'. Below this is a table with columns: DATE, FULL NAME, USERNAME, ACTION, and NOTES.

DATE	FULL NAME	USERNAME	ACTION	NOTES
11/7/2022 08:50 AM	thylab.local\Administrator	thylab.local\Administrator	View	
10/27/2022 05:04 ...	thylab.local\Administrator	thylab.local\Administrator	View	
10/27/2022 05:01 ...	ss_admin	ss_admin	Launch	Remote Desktop - DC1
10/27/2022 05:01 ...	ss_admin	ss_admin	Password Displayed	Fields: (Password)
10/27/2022 05:01 ...	ss_admin	ss_admin	View	
10/26/2022 07:50 ...	api_RAS	api_RAS	Password Displayed	Fields: (Password)
10/26/2022 07:50 ...	api_RAS	api_RAS	View	
10/18/2022 12:16 ...	api_RAS	api_RAS	Password Displayed	Fields: (Password)
10/18/2022 12:16 ...	api_RAS	api_RAS	View	
10/14/2022 01:25 ...	thylab.local\DHughes	thylab.local\DHughes	Launch	Remote Desktop - DC1
10/14/2022 01:24 ...	thylab.local\DHughes	thylab.local\DHughes	View	
10/14/2022 12:25 ...	thylab.local\DHughes	thylab.local\DHughes	View	
10/13/2022 02:03 ...	api_RAS	api_RAS	Password Displayed	Fields: (Password)
10/13/2022 02:03 ...	api_RAS	api_RAS	View	



Session Recording / Monitoring

Session Monitoring

Live Monitoring

1. Watch an active session of a user live
2. Take action as an Auditor:
 - a. Terminate immediately
 - b. Limit Session to 5 min
 - c. Send message only

The screenshot displays the 'Secret Server' interface for 'Session Monitoring'. On the left is a navigation sidebar with links to Dashboard, Secrets, Inbox, Reports, and Administration. The main panel shows a table of active sessions. One session is listed with the following details:

START DATE	SECRET NAME	USER	TYPE	MACHINE
11/7/2022 09:16 AM	5_Advanced Session Recording Ex...	Thylab\DHughes	Remote Desktop	DC1

Below the table, there are controls for 'Watch Live' and 'Terminate'. A 'Back' button is also present. A 'Terminate' dialog box is open, featuring a 'Response Comment' text area and an 'Action' dropdown menu. The dropdown menu is expanded, showing three options: 'Terminate immediately', 'Limit Session to 5 minutes', and 'Send message only' (which is highlighted in blue). The dialog also includes 'OK' and 'Cancel' buttons. The 'Delinea' logo is visible in the bottom left corner.

Session Recording

Recorded Video with metadata

- Session Summary / Details
- Video with heatmap
- Session Activity

Secret Server

Dashboard

Secrets

Inbox

Reports

Administration

Oelinea

Watch Session Recording

SESSION SUMMARY

Session Secret: < None >

Machine: ssptm

Session User: thylabadministrator

Launcher Used: < None >

Session Start: 10/28/2022 06:18 AM

Session End: 10/28/2022 12:16 PM

SEARCH SESSION ACTIVITY

Activity Type: All

Keyword:

ELAPSED	TYPE	ACTIVITY	JUMP TO
00:00:00		explorer	
00:00:00		svchost	
00:00:00		csrss	
00:00:00		taskhostw	
00:00:00		vm3dservice	
00:00:00		vmtoolsd	
00:00:00		dwm	
00:00:00		explorer	
00:00:00		taskhostw	
00:00:00		RuntimeBroker	
00:00:00		Thycotic.SessionRecorder	
00:00:00		sihost	
00:00:00		winlogon	
00:00:00		SearchUI	
00:00:00		ShellExperienceHost	
00:00:00		chrome	

APPLICATION MADE ACTIVE ACTIVITY DETAILS

C:\Windows\explorer.exe

explorer.exe

administrator

THYLAB

0-00:00 / 5:58:37

Screen

Keystrokes

Processes