Executive Summary

The Delinea Secret Server Platform is a robust Privileged Access Management (PAM) solution designed to secure, manage, and govern privileged accounts across hybrid environments. For Security Mutual Life Insurance Company of New York (SMLINY), a financial services provider handling sensitive customer data, policy information, and regulatory compliance requirements (e.g., NYDFS cybersecurity regulations), this platform is essential for mitigating insider threats, enforcing least privilege, and streamlining audits. By centralizing privileged credential management, Secret Server helps SMLINY reduce breach risks, ensure compliance with standards like SOX and HIPAA, and optimize operational efficiency in its on-premises Active Directory (AD) and local workstation ecosystems.

Below, we discuss three core use cases at a high summary level, tailored to SMLINY's needs in managing administrative access for IT operations, policy administration systems, and claims processing servers.

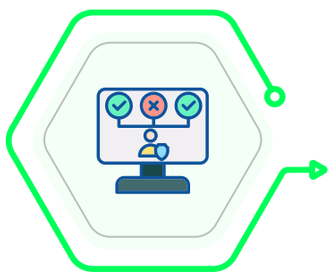
Main Use Cases

Just-In-Time (JIT) Access

JIT Access empowers SMLINY's IT administrators and support staff to temporarily elevate standard user accounts to privileged levels (e.g., local admin on servers or workstations) for short, predefined durations—typically minutes to hours. This eliminates standing privileges, reducing the attack surface from dormant admin accounts that could be exploited in phishing or ransomware scenarios common in the insurance sector. For SMLINY, JIT integrates seamlessly with AD for on-demand elevation during tasks like software deployments or incident response, with automated de-elevation and session monitoring to maintain audit trails. Benefits include faster incident resolution without compromising security, aligning with zero-trust principles to protect customer data integrity.

Delinea:

Delinea Secret Server Platform - Main Use Cases for Security Mutual Life Insurance Company of New York



Privileged Account Review

This use case provides SMLINY with comprehensive visibility and governance over privileged accounts by auditing and enforcing entitlements across on-premises AD domains and local machines. It identifies "who" has admin rights (e.g., via role-based access), "what" permissions are granted (e.g., full control vs. read-only), and "where" they apply (e.g., specific servers hosting claims databases). Over time, enforcement policies can revoke unnecessary privileges, preventing privilege creep in a growing organization like SMLINY. Key for compliance reporting, it supports quarterly reviews to flag over-privileged accounts, ensuring adherence to regulatory mandates and minimizing risks from insider errors or external compromises.

User Account Review

Focused on proactive hygiene, this feature enables SMLINY to generate reports and set alerts for dormant or underutilized accounts—both privileged (e.g., legacy service accounts for policy legacy systems) and non-privileged—triggering a "pruning protocol" to disable or decommission them. By analyzing login frequency and activity patterns, it uncovers "zombie" accounts that pose hidden risks, such as those unused for 90+ days, which are prime targets for lateral movement in breaches. For SMLINY, this supports automated alerts via integration with SIEM tools, facilitating routine cleanups that enhance overall identity posture, reduce license costs, and bolster defenses against credential stuffing attacks prevalent in financial services.

Success Criteria Checklist

To validate successful implementation and ongoing operation of the Delinea Secret Server Platform at SMLINY, the following checklist outlines key milestones. Each item should be verified during deployment phases, with evidence documented (e.g., screenshots, logs) for audit purposes. Use this as a phased guide: configuration, testing, and reporting.

Success Criteria	Description	Status (e.g., Not Started/ In Progress/Completed)	Owner	Notes/ Evidence
Vault Main Service Account and Configure	Establish and configure the primary service account for the Secret Server vault, ensuring secure authentication and integration with AD.			
Vault Discovery Account and Configure	Set up a dedicated discovery account with minimal privileges to scan for unmanaged credentials across the network.			
Run Discovery Process and Review Network View	Execute the initial discovery scan and validate the generated network topology view for accuracy in identifying assets and accounts.			
Vault Test Account and Rotate Password	Create a test privileged account in the vault, perform an automated password rotation, and confirm successful update.			
Place Test Account on Test Server and Import	Assign the test account to a non-production server and import it into Secret Server for management.			

Delinea:

Delinea Secret Server Platform - Main Use Cases for Security Mutual Life Insurance Company of New York

Delinea

Enable Check-In Check-Out for Vault Test Account	Activate session-based check-in/check-out workflows for the test account to enforce controlled access and logging.			
Setup SSPCred for Secret Server	Configure SSPCred (Secret Server Privileged Credential) for secure credential injection and just-in-time elevation testing.			
Run Secret and User Activity Reports	Generate and review reports on secret access patterns and user behaviors to baseline normal activity.			
Run User Audit Report	Execute an audit report on user entitlements, verifying coverage of privileged accounts and flagging anomalies.			
Review Reports within Identity Posture and Inventory	Analyze aggregated reports in the Identity Posture dashboard and Inventory module to assess overall PAM health and compliance gaps.			