NORTHERN TRUST

Northern Trust Achieves 137% Improvement in Password Rotation Compliance and 300% Improvement in Application Security with CyberArk

Global bank transforms endpoint, human and non-human identity security across 50K endpoints, 400 applications, and 70,000 accounts with zero user disruption

---

↑ **Back to Top**   Jump to ⌄

Summary

Together with CyberArk Identity Security Platform and SDG Corporation (formerly Synergetika), Northern Trust secures tens of thousands of endpoints and accounts, and hundreds of applications, leading to an improvement of 137% in password rotation compliance, a growth of 250% in managed privileged accounts, and a 300% increase in application security coverage, all while maintaining a seamless user experience and meeting stringent regulatory requirements for the financial sector. Northern Trust's success earned them the **CyberArk 2025 Identity Security Impact Award** for **Cyber Risk Reduction**.

Company profile

Northern Trust: Built on a 135-year legacy, this Chicago-based global financial institution manages more than $1.6 trillion in client assets and provides asset servicing, wealth management, and investment services to institutions, individuals, and pensions.

SDG Corporation is a privileged access management systems integrator that has provides expertise and repeatable frameworks for large-scale deployments, specializing in license acquisition, procurement, design, implementation, and managed services.

Products and services

CyberArk Endpoint Privilege Manager (EPM) →

CyberArk Privileged Access Manager (PAM) Self-Hosted →

CyberArk Secrets Manager, Self-Hosted →

CyberArk Certificate Manager, Self-Hosted →

CyberArk Code Sign Manager →

Solutions

Secure IT Admins →

Challenges

What does it take to overhaul local admin access and password control to 50,000 endpoints without disrupting a single user? That's the critical challenge Northern Trust faced. The company also faced scalability and compliance challenges related to privileged access management and risks related to long-lived SSL certificates, which increased exposure to potential compromise and outdated encryption practices.

As one of the world's largest and most respected financial institutions, security and compliance are at the core of its operations. However, its existing endpoint privilege management tool presented more problems than protection.

Although technically deployed, it had significant limitations. "The list of challenges before and after we implemented our legacy tool were almost identical," said Manish Dixit, director of cybersecurity engineering at Northern Trust. "It was like not having a solution at all." With over 23,000 employees across the globe, they needed better control over user access, more stringent policies, and a clearer line of sight into security gaps.

At the time, only 40% of endpoints met basic password rotation requirements. Without centralized control, employees managed their own local admin passwords. This practice led to weak credentials, shared accounts, and frequent lockouts when users forgot or mistyped passwords.

With licensing renewal on the horizon—and a complex IT environment that included non-persistent VDIs, global remote users, and layered regulatory demands—Northern Trust needed a smarter, faster way forward for banking resilience.

Internal alignment would be essential. "Even the best technology won't succeed if the people using it don't buy in," Manish said. "You need user buy-in, leadership support, clear communication, and coordination across teams. Otherwise, even the best tools fail."

They had to get the rollout right the first time.

Solutions

Joining forces with implementation partner SDG Corporation, Northern Trust chose the CyberArk Identity Security Platform consisting of: CyberArk Endpoint Privilege Manager (EPM), CyberArk Privileged Access Manager (PAM) Self-Hosted, CyberArk Secrets Manager Self-Hosted, CyberArk Code Sign Manager, and CyberArk Certificate Manager, Self-Hosted.

As their largest deployment, what was the plan for implementation without disrupting business workflows? Execute a structured, three-phase rollout designed to reduce disruption, maintain security, and improve compliance across the financial services business.

- **Phase one**: The team deployed CyberArk EPM and PAM Self-Hosted in coexistence mode alongside the legacy system to prevent operational impact. They began with the loosely connected devices (LCD) feature, focusing on quick wins and validation. By assigning a specific number of endpoints each day and monitoring them closely, SDG Corporation was able to control the impact and help deliver a seamless experience. "We were able to manage local admin **rights** using CyberArk EPM and rotate **credentials** on a periodic basis to keep them compliant," Manish. "With automated password rotation, we significantly lowered the support burden for IT. We achieved better compliance and fewer tickets."
- **Phase two**: A meticulous policy mapping process ensured that all functionality was preserved, while unnecessary complexity was removed. The legacy agent was disabled in place rather than uninstalled, reducing technical risk during the transition. Despite the scale of the change, the financial services organization experienced **no disruption to end users**. "We went through a thorough round of testing to ensure a seamless cutover, and that's exactly what we achieved," said Nikhil Rao, director of endpoint privilege management and privileged access management at SDG Corporation. "We had regression test cases, policy dry runs, and stakeholder reviews—all of which let us deploy with confidence."
- **Phase three**: Northern Trust expanded the capabilities of CyberArk EPM even further. They introduced just-in-time (JIT) admin access through ServiceNow, supported by a custom two-level approval workflow. Application control was tightened through targeted allow-listing and blocking, while new integrations with Azure Sentinel enabled detection of threats that had previously gone unnoticed.

According to Vaibhav Nigam, managing director at SDG Corporation, "CyberArk EPM was able to detect attack types that the existing SIEM couldn't. The simulated attacks triggered alerts in EPM—but not in the existing SIEM.

Industry

also cleaned up account data, resolved Central Policy Manager (CPM) issues, and developed a real-time PowerBI dashboard for compliance reporting.

When it came to tackling machine (non-human) identities – the company onboarded nearly 400 applications with CyberArk Secrets Manager Self-Hosted, dramatically improving the security of machine identities. Additionally, they integrated CyberArk Certificate Manager, Self-Hosted to manage their digital certificates more securely, implementing a policy that requires all SSL certificates to be renewed every six months. They also use CyberArk Code Sign Manager to securely sign both Microsoft code and Java applications.

Results

Northern Trust was able to onboard all 50,000 endpoints in just 16 days—with zero incidents. Perhaps most notably, password rotation compliance jumped from 40% to over 95%, significantly reducing one of the banking organization's most pressing risks.

"CyberArk EPM has the capability to do whitelist, blacklist, JIT access, and more—our risk team loves us for that," said Manish. "The control granularity and automation saved our support teams hours." Privilege elevation entitlements were reduced by more than 30%, and critical compliance gaps were closed by extending coverage to parent images of non-persistent VDIs. The rollout not only improved security and compliance—it streamlined operations without compromising the user experience. Integration with SIEM and ITSM systems further strengthened governance and reduced support overhead.

"We built custom dashboards using EPM logs, application usage, and AD data," said Nikhil. "That helped us enforce real controls—not just deploy software."

"As we began rolling out CyberArk EPM we realized we could do much more—password rotation, application allow/block lists, ServiceNow just-in-time integration, and threat analytics. We kept expanding the scope. We started with one solution—elevation of access—and ended up implementing five."

– Manish Dixit, Director of Information Security Engineering, Northern Trust

The improved PAM program was successfully onboarded and now manages approximately 70,000 accounts—a growth of around 250%. Compliance posture improved significantly through real-time reporting, streamlined data, and more reliable credential management. The modernized, scalable architecture in Azure positions the company for continued growth and future security enhancements.

The team's efforts to secure non-human and machine identities led to a 300% increase in application security coverage and a significantly strengthened security posture. By enforcing shorter certificate lifetimes, the company reduced its risk exposure from compromised or outdated certificates and positioned itself for more agile and automated certificate management.

By modernizing its approach to endpoint privilege management, privileged access management, and machine identity security, Northern Trust didn't just meet its security and compliance goals—it raised the bar. The financial institution's success proves that with the right technology, partners and execution, large-scale transformation can be fast, secure, and user-friendly, and ultimately earned them the CyberArk 2025 Identity Security Impact Award for Cyber Risk Reduction.

Key benefits

- **Efficiency**: Eliminated overhead caused by legacy EPM licensing and complexity and secured 50,000 endpoints in 16 days.
- **User experience**: The coexistence model allowed full migration with zero outages or downtime.
- **Financial sector compliance and governance**: Privilege elevation entitlements reduced by 30% and

Related customer stories

Persistent

CyberArk Helps Global IT Service Business Build Cybersecurity Assurance

Read Case Study →

First Horizon Bank Makes Cybersecurity Efficient, Cost Effective and Business Operations More Secure

Read Case Study →

Leading Indian Bank protects one million business and individual customers with CyberArk

Read Case Study →

Talk to an expert

Understand the key components of an Identity Security strategy

Get a first-hand look at CyberArk solutions

Identify next steps in your Identity Security journey

Contact Sales

Support

Contact Support

Training & Certification

CyberArk Community ⤢

Technical Support

EPM SaaS Register / Login

Product Security

Resources

Resource Center

Events

Blogs

CIO Connection

CyberArk Blueprint

Scan Your Network

Marketplace ⤢

Partners

Partner Network

Partner Community ⤢

Partner Finder

Become a Partner

Alliance Partner

Company

Investor Relations ⤢

Leadership

Newsroom

Office Locations

Environmental, Social and Governance ⤢

Terms and Conditions

Privacy Policy

Your Privacy Choices

Cookie Preferences