

Case Study

CYBERARK®
THE IDENTITY SECURITY COMPANY™NORTHERN
TRUST

Northern Trust Teams with SDG and CyberArk to Secure 50,000 Endpoints Without Disrupting a Single User

Global bank achieves 137% improvement in password rotation compliance and 300% boost in application security, securing 50K endpoints, 400 applications, and 70,000 identities—all with zero user disruption.

SUMMARY

Northern Trust, a Chicago-based global financial institution managing more than \$1.6 trillion in client assets, faced a massive challenge: overhauling local admin access and password control across 50,000 endpoints without disrupting a single user. To solve it, the company partnered with CyberArk and SDG Corporation, combining the CyberArk Identity Security Platform with SDG's proven PAM integration and deployment expertise. Together, they delivered a seamless rollout that modernized privileged access, strengthened compliance, and scaled protection across tens of thousands of accounts and hundreds of applications.

The results were dramatic: **137% improvement in password rotation compliance, a 250% increase in managed privileged accounts, and a 300% expansion in application security coverage** – all achieved while maintaining a frictionless user experience and meeting stringent financial regulations. This transformation earned Northern Trust the CyberArk 2025 Identity Security Impact Award for Cyber Risk Reduction.

THE CHALLENGE

As one of the world's largest financial institutions, security and compliance are non-negotiable. So when Northern Trust recognized the need to modernize their privilege access strategy and tools, they quickly realized a critical challenge: **How do you overhaul local admin access and password control across 50,000 endpoints without disrupting a single user?**

Northern Trust faced mounting pressure to get the rollout right, with both technical and organizational challenges raising the stakes, including:

- Ⓞ Long-lived SSL certificates that increased security exposure
- Ⓞ Remote workers and non-persistent VDIs that added complexity
- Ⓞ Strict regulatory requirements driving compliance demands
- Ⓞ Looming renewal deadlines creating urgency
- Ⓞ The need for user adoption, leadership support, and clear communication to ensure success

THE SOLUTION

Northern Trust partnered with SDG's team of PAM advisory and transformation experts to deploy the CyberArk Identity Security Platform, including Endpoint Privilege Manager (EPM), Privileged Access Manager (PAM), Secrets Manager, Code Sign Manager, and Certificate Manager – all in a self-hosted model.

To minimize disruption, the rollout followed a three-phase plan:

- Ⓞ **Phase 1:** EPM and PAM were deployed in coexistence mode with the legacy system. Quick wins came through local admin rights management and automated password rotation, cutting support tickets and improving compliance.
- Ⓞ **Phase 2:** Policies were streamlined, complexity reduced, and the legacy agent disabled in place. Extensive testing and stakeholder reviews ensured a smooth cutover with zero user disruption.
- Ⓞ **Phase 3:** EPM capabilities were expanded with just-in-time access through ServiceNow, a two-level approval workflow, advanced application allow-listing, and Azure Sentinel integration for stronger threat detection.

Beyond endpoint and privileged access management, Northern Trust:

- Ⓔ Expanded its human identity security program, migrating to two self-hosted Azure instances to separate human IDs from machine identity secrets.
- Ⓔ Onboarded nearly 400 applications with CyberArk Secrets Manager to protect machine identities.
- Ⓔ Secured digital certificates with CyberArk Certificate Manager, enforcing six-month renewal policies.
- Ⓔ Adopted CyberArk Code Sign Manager to safely sign Microsoft and Java applications.

THE RESULT

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.

In addition, Northern Trust achieved:

- Ⓔ **Stronger access control:** Whitelisting, blacklisting, and just-in-time (JIT) access provided precise, automated privilege management.
- Ⓔ **Reduced support workload:** Granular controls and automation saved IT support teams significant time and effort.
- Ⓔ **Improved compliance:** Privilege elevation entitlements were cut by **30%+**, and coverage was extended to parent images of non-persistent VDIs, closing key compliance gaps.
- Ⓔ **Better user experience:** Security and compliance improvements were achieved without disrupting day-to-day operations.
- Ⓔ **Enhanced governance:** Seamless integration with SIEM and ITSM systems tightened oversight while lowering support overhead.
- Ⓔ **Actionable visibility:** Custom dashboards built from EPM logs, application usage, and AD data enabled enforcement of real controls—not just software deployment.

Northern Trust's modernized PAM program now secures nearly **70,000 accounts**—a 250% increase—while strengthening compliance with real-time reporting, streamlined data, and more reliable credential management.

By moving to a scalable Azure architecture, Northern Trust improved its current security posture and positioned itself for future growth. Extending protection to non-human and machine identities drove a **300% increase in application security coverage**, and enforcing shorter certificate lifetimes reduced risk from outdated encryption while enabling more agile, automated certificate management. Together, these efforts delivered a measurable boost in resilience, compliance, and operational efficiency without disrupting the business.

“As we began rolling out CyberArk EPM,” Manish said, “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

KEY BENEFITS

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.

- Ⓔ **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 password rotation improved from 40% to over 95%. Audit-ready controls and detection integrated with ServiceNow and Azure Sentinel.

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. To learn more visit www.sdgc.com.

ABOUT CYBERARK

CyberArk (NASDAQ: CYBR) is the global leader in identity security, trusted by organizations around the world to secure human and machine identities in the modern enterprise. CyberArk's AI-powered Identity Security Platform applies intelligent privilege controls to every identity with continuous threat prevention, detection and response across the identity lifecycle. With CyberArk, organizations can reduce operational and security risks by enabling zero trust and least privilege with complete visibility, empowering all users and identities, including workforce, IT, developers and machines, to securely access any resource, located anywhere, from everywhere. Learn more at cyberark.com.

ABOUT NORTHERN TRUST

Built on a 135-year legacy, Northern Trust is a Chicago-based global financial institution managing more than \$1.6 trillion in client assets; providing asset servicing, wealth management, and investment services to institutions, individuals, and pensions.

Contact Us: solutions@sdgc.com



■ 75 North Water Street
Norwalk, CT 06854
■ 203.866.8886
■ sdgc.com