Silverfort

CASE STUDY

How a leading US healthcare organization secured privileged access to ensure HIPAA compliance

BASED

Northeast US

INDUSTRY

Healthcare

PROTECTED ACCOUNTS

40+ users
100+ service accounts

ENVIRONMENT

AD domains: 2 (root + child)
Infrastructure: NSX, Nutanix Flow, Microsoft Entra, Hybrid AD
Privileged admin tools: PowerShell, SSH, RDP, DRAP, IIS

THE CHALLENGE:

To meet stringent HIPAA requirements and combat the rising threat of credential-based attacks, the healthcare organization set out to significantly strengthen its identity security posture. The initiative centered on securing the most critical access points, including domain admin accounts, sensitive service accounts, and high-risk protocols such as PowerShell, SSH, RDP, and Dell DRAC. At the same time, they sought to eliminate reliance on legacy tools, streamline operations, and gain unified visibility into authentication activity across their hybrid Active Directory (AD) environment all while minimizing user friction.

CUSTOMER OVERVIEW

About

The Northeastern US-based healthcare organization supports patient services across senior care and pharmacy operations. With a highly customized IT environment and an in-house development team, the organization manages critical infrastructure and sensitive data, all of which is governed under HIPAA compliance.

Environment

The organization operates a hybrid environment with a root and child on-prem AD domain, integrated with Microsoft cloud services. They use a custom IAM system that automatically maps users to job roles. Key technologies include PowerShell, Internet Information Services (IIS), RDP, VMware ESXi, and NSX micro segmentation with ongoing migration to Nutanix Flow. The team also oversees more than 100 service accounts and an elevated number of domain admins supporting homegrown applications and legacy resources.

Why now: Addressing regulatory mandates and identity security blind spots

The organization's main goal was to close identity security blind spots and ensure HIPAA compliance with strong access controls for highly privileged users and service accounts. In parallel, they aimed to reduce the operational burden of managing endpoint agents, gain full visibility into authentication flows, and secure critical systems that don't support agent-based deployments, including Dell Remote Access Controllers (DRACs), Intelligent Platform Management Interfaces (IPMIs), and SSH endpoints.

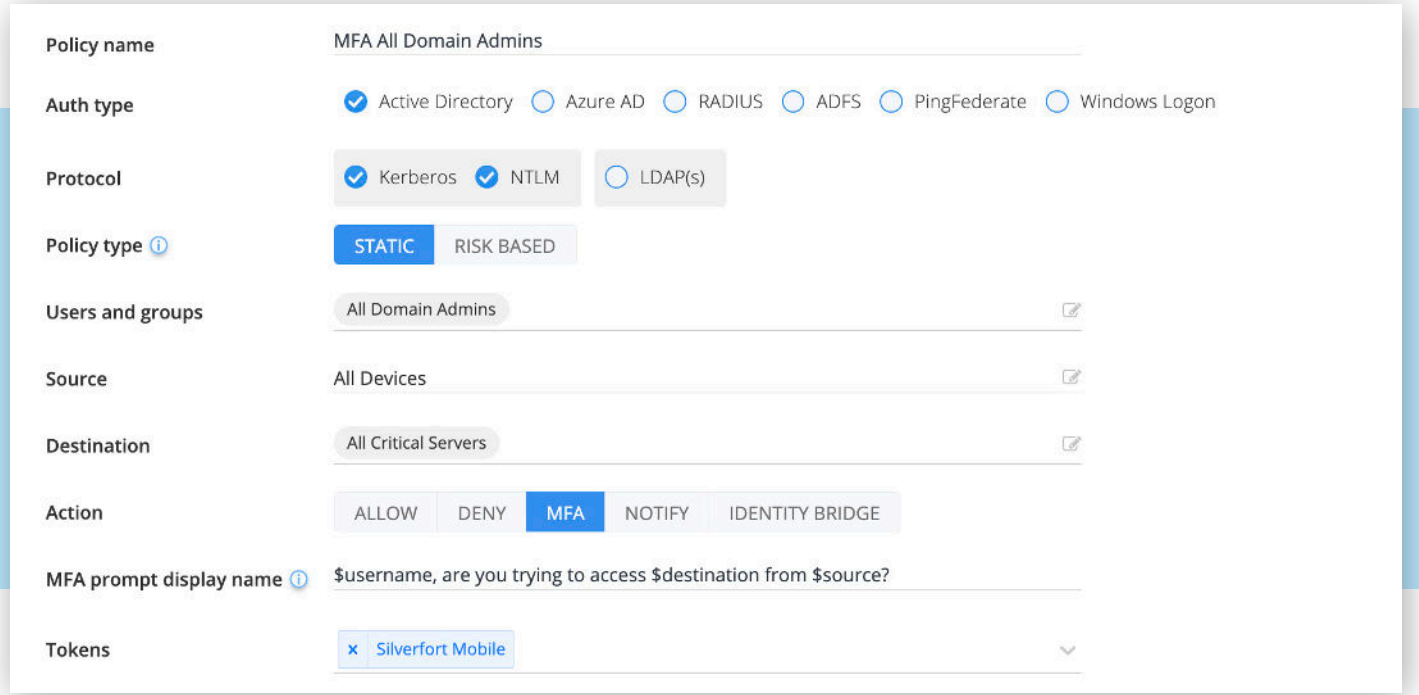
Challenge 1: Meeting HIPAA access control requirements

Compliance mandates and privileged access risk

To meet tight HIPAA requirements and reduce identity security risk, the healthcare organization needed to enforce multi-factor authentication (MFA) protection for domain admins and other privileged users across all sensitive access points, including PowerShell, RDP, SSH, IIS, and DRAC. Legacy infrastructure and operational constraints posed significant challenges in deploying agent-based solutions, particularly on systems that couldn't support endpoint software. Past disruptions caused by persistent, hard-to-remove agents further reinforced the need for an agentless approach.

Complying with HIPAA requirements

With Silverfort, the business enforced MFA across all critical privileged access points, including PowerShell, SSH, RDP, IIS, and DRACs, without relying on agents and reconfiguring endpoints. The IT team established policies that enabled short-term access exceptions for critical resources, minimizing administrative friction. As a result, they strengthened protection for privileged accounts used in day-to-day operations, met HIPAA compliance requirements, and reduced the risk of lateral movement across sensitive systems.



The company's MFA policy requires all access requests by domain admin accounts to be verified with MFA. During Kerberos or NTLM authentications, they see which critical server the admin is trying to access and the ID address of users

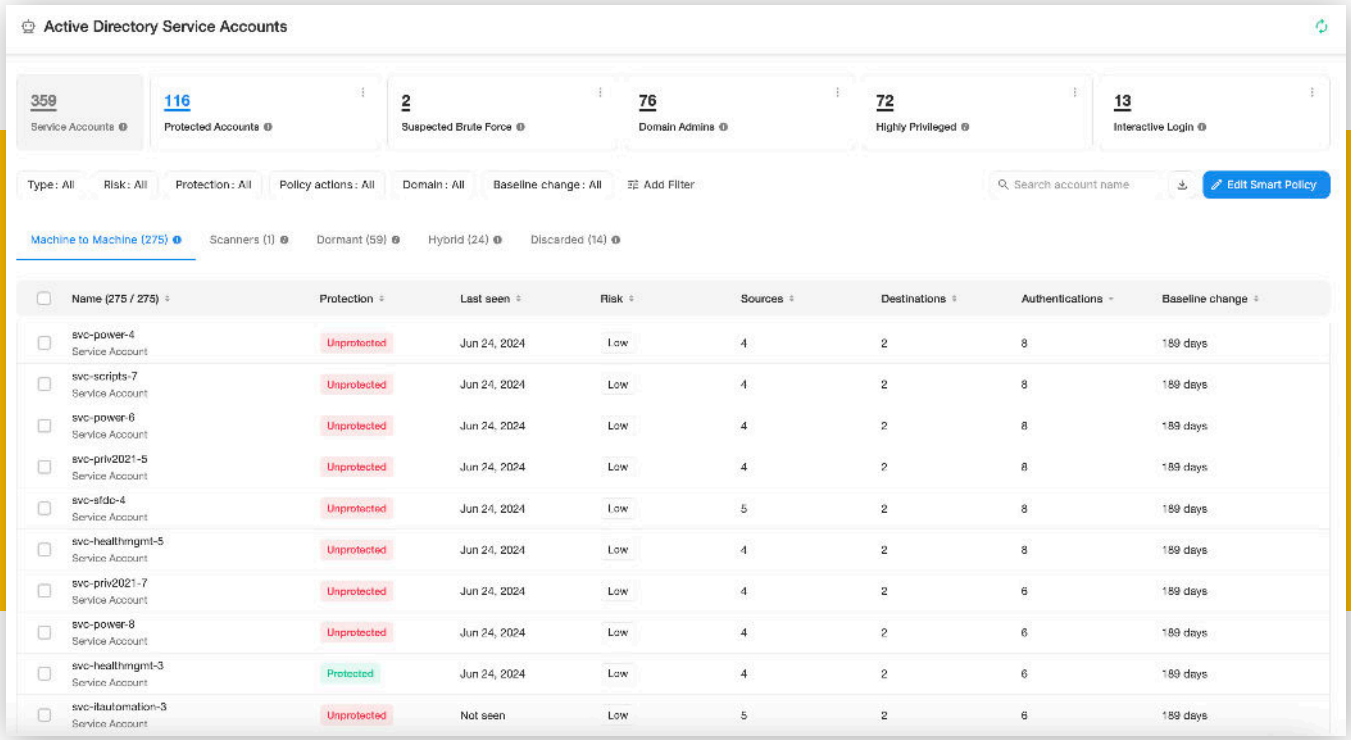
Challenge 2: Visibility into service accounts

Limited visibility into service accounts

The organization relies heavily on service accounts to support homegrown applications, automation scripts and system integrations, many of which had excessive privileges. The legacy tools offered limited visibility into how these accounts behaved across the hybrid environment, what systems they accessed and whether any were overprivileged or stale. These blind spots made it difficult to enforce consistent access controls and increased the risk of lateral movement.

End-to-end visibility and security for service accounts

The healthcare organization gained full visibility into all authentication activity across both users and non-human identities (NHIs). With Silverfort, the healthcare organization discovered over 100 active service accounts and analyzed their access behaviors. This allowed them to identify excessive privileges or unnecessary permissions, and isolate high-risk accounts using a virtual fencing approach. By segmenting service accounts based on their purpose and enforcing granular access policies, the organization gained tighter control over NHIs that reduced the attack surface and improved operational oversight.



The company's active directory service accounts dashboard in Silverfort displays all detected service accounts, including name, source, destination, number of authentications, risk score, baseline change and other account info.

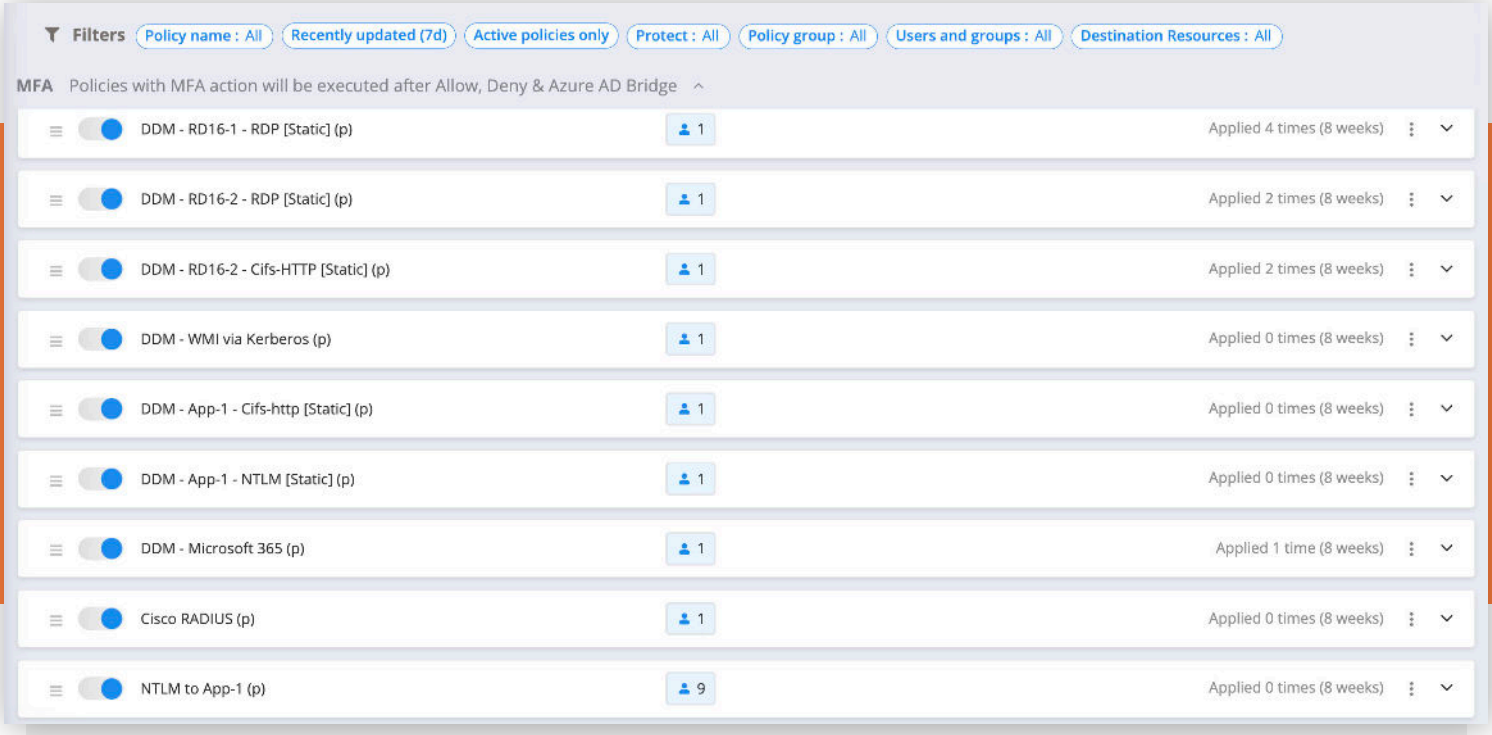
Challenge 3: Managing strong security controls without operational overhead

Need for flexible controls without creating admin friction

The organization needed to implement strong authentication controls without introducing unnecessary friction for administrators or creating workflow disruption. Their privileged users need to access servers dozens of times per day through command-line interfaces, automation tools, or legacy applications, making strict MFA prompts impractical. The IT team also wanted to create exceptions or adjust policies temporarily during maintenance or when onboarding new tools. Without this level of control, they risked generating resistance to user adoption.

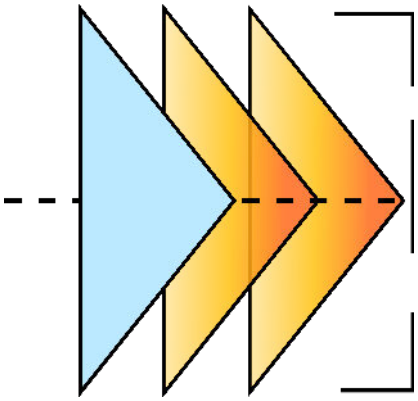
Customizing access policies to fit operational needs

With Silverfort, the healthcare organization implemented flexible, context-aware access policies that helped to balance security with usability. MFA prompts were tailored based on user role, access frequency, and resource sensitivity. Using Silverfort, their IT team configured granular access policies rules, reducing overhead during maintenance or urgent tasks. These capabilities allowed the organization to maintain strong authentication standards while supporting operational efficiency for privileged users, reducing helpdesk burden, and ensuring smoother adoption across teams.



The company's list of access based policies that set granular access rules with MFA prompts based on user roles, access frequency, and resource sensitivity.

Moving forward



What began as a HIPAA compliance-driven initiative to secure privileged access quickly evolved into a broader effort to strengthen identity security across the organization's hybrid environment. By implementing strong access controls for privileged users and service accounts, the healthcare provider significantly reduced its exposure to identity-based threats spanning legacy infrastructure, on-prem systems, and hybrid environments.

With consistent MFA enforcement, full visibility into authentication activity, and granular policy flexibility, the organization is now better equipped to manage privilege access at scale. Looking ahead, the organization plans to further mature its identity strategy by applying Just-in-Time (JIT) access policies and expanding protections across its growing cloud infrastructure, ensuring long-term alignment with compliance, security and operational priorities.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Learn more