Silverfort

CASE STUDY

Securing privileged access in legacy hybrid environments: How the University of the Pacific gained unified visibility and control

BASED	INDUSTRY	USERS	ENVIRONMENT
California, US	Education	10,000+	On-prem Active Directory (AD) Okta, Entra ID

UNIVERSITY OF THE PACIFIC

University of the Pacific is a private university in California with campuses in Stockton, Sacramento, and San Francisco. Founded in 1851, it holds the distinction of being California's first chartered university and today serves a diverse academic community of students, faculty, and administrative staff. With a strong focus on interdisciplinary learning, professional programs, and community engagement, the university supports a complex and growing IT environment that combines multiple domains and user types.

THE CHALLENGE:

Needed better visibility and the ability to apply security controls in legacy AD environment

- Apply MFA for privileged accounts across four on-prem AD domains
- Improve discovery and visibility into on-prem service accounts, including outdated and misconfigured non-human identities
- Monitor and reduce reliance on legacy authentication protocols

THE SOLUTION:

End-to-end visibility, control and real-time protection for privileged users and AD service accounts

- Identified and audited over 1,200 service accounts across four AD domains, eliminating unnecessary access and reducing the attack surface
- Enforced MFA protection for high-risk privileged users to secure sensitive administrative operations, reducing risk of credential-based breaches
- Detected and retired legacy protocols across critical systems, reducing technical debt tied to outdated infrastructure

The challenge: Legacy identity infrastructure was in urgent need of improved access control

Like many long-established institutions, University of the Pacific operated within a legacy Active Directory (AD) environment that had grown increasingly complex over time. Years of technical debt, limited visibility, and overlapping permissions created a security blind spot in their identity infrastructure.

> "We have a legacy Active Directory environment and even for experts, it's confusing. The complexity had grown over the years, and it became clear – we needed to take control."
>
> Shawn Kerns, Information Security Engineer at University of the Pacific

The university's hybrid environment spanned four separate domains and included thousands of users, as well as hundreds of applications and AD service accounts, many of which seemed to be either inactive, misconfigured or completely undocumented.

The security team had limited visibility into how both privileged users and service accounts were behaving: which resources they were authenticating to and from, or whether they were even still in use. Outdated authentication protocols, were still widespread across the environment, introducing exposure risks that were difficult to detect and secure.

"Our own privileged accounts had gradually accumulated access over time, and I was looking at my own account and the level of access it had. There was no centralized control, no visibility, and no easy way to enforce MFA or an access policy across the board," added Kerns.

Finding the right identity security platform

The University of the Pacific team recognized the need for an identity security platform – one that could not only strengthen security controls but also help them rethink how to manage access across a legacy infrastructure. As an existing CrowdStrike customer, the team considered expanding into its Identity Protection capabilities to cover AD risks and privileged access gaps.

When it came to selecting an identity security partner, University of the Pacific found that Silverfort stood out not just for technical capabilities, but for the speed and simplicity of rollout.

> "We considered CrowdStrike's Identity platform, but Silverfort stood out for the granular control of both human and non-human identities. Silverfort was easier for our teams to understand from a configuration standpoint and no need for an agent running on each endpoint made the deployment easy."
>
> Shawn Kerns, Information Security Engineer
> at University of the Pacific

"One of my indicators of success is how quickly a demo or POC gets off the ground. Once we began mapping our environment to the Silverfort platform, we had it up and running in just two hours. By the next day, we were already seeing value: experimenting with policies, generating reports, and uncovering unknown issues almost immediately. That kind of instant feedback gave us real confidence that Silverfort was the right fit," declared Shawn Kerns.

The solution: Immediate value through visibility, control, and smart enforcement

Following a fast and insightful POC, University of the Pacific moved ahead with Silverfort to extend security across its hybrid identity environment. The security team began by focusing on real-time insights into how accounts – especially highly privileged users and service accounts – were interacting with their domain controllers.

> "It was easy to use Silverfort; anytime you put an application or agent on a domain controller, there's always fear. But once we were live, we saw no disruptions. And almost immediately, we could validate that everything was working as expected."
>
> Shawn Kerns, Information Security Engineer
> at University of the Pacific

The University of the Pacific focused on monitoring service account behavior using Silverfort's report-only mode. Within days, the team surfaced over 1,200 service accounts. With this clarity, they began building conditional access policies using Silverfort's Smart Policy capability, gradually restricting risky behavior while maintaining operational continuity.

"We had three accounts generating hundreds of thousands of events a day. I had a sense of what was going on, but Silverfort gave me the data to back it up and helped me show the technology teams what needed to be fixed," said Kerns.

With policy enforcement underway for service accounts, the team then shifted focus to protocol hardening and privileged access enforcement. They worked on long-standing gaps with legacy protocols by setting rule-based policies to detect usage, monitor system-level activity, and sending alerts on outdated authentication attempts without disrupting services.

> "One of the first things we did was create a policy to track legacy authentications, and we quickly had complete visibility into what was still using it. That gave us the data and visibility we needed to start addressing the problems without breaking our production environment. "
>
> Shawn Kerns, Information Security Engineer at
> University of the Pacific

Enforcing MFA security controls for high-risk privileged activity

Simultaneously, they began rolling out adaptive MFA protection policies for privileged users, ensuring high-risk operations like domain elevation or PowerShell access were gated by step-up authentication.

"We have tried to solve MFA at the desktop level for years, and now we have that capability. I can sleep easier at night knowing that if someone's knocking, I'll get the Silverfort prompt," said Kerns.

> "This was a problem we had struggled with for years, and now, within months we've gained clarity and control. And this is just the beginning, we're already thinking ahead to continue our journey toward a Zero Trust framework, secure cloud-based non-human identities, and more. "
>
> Shawn Kerns, Information Security Engineer at
> University of the Pacific

By deploying Silverfort's Identity Security Platform, University of the Pacific gained end-to-end visibility into its most critical identity layers – including highly privileged users, service accounts, and legacy authentication protocols. The security team now has the tools to continuously monitor identity behavior, apply risk-based security controls, and proactively reduce exposures across their hybrid environment.

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