Silverfort

CASE STUDY

Shannon Medical Center's proactive identity security approach leads to strict access control for all users while strengthening their AD hygiene

BASED
San Angelo, TX, US

INDUSTRY
Healthcare

USERS
8,000

ENVIRONMENT
On-prem Active Directory, SQL servers
Medical legacy applications
Privileged admin accounts

SHANNON

For more than 75 years, Shannon Medical Center has served the healthcare needs of the community in the San Angelo area. Their facility is licensed for 400 beds and provides a variety of clinical services to meet each patient's needs. They are the designated Lead Level 3 Trauma Center for the region, have a nationally recognized Intensive Care Unit, provide critical care to newborns as young as 28 weeks, perform state-of-the-art diagnostics in their radiology department, and provide complete testing and surgical capabilities for cardiology patients among many more services.

THE CHALLENGE:

Implement access controls on all users

- Minimal security controls to protect user access requests, especially for admins
- Limited visibility and insights into their AD environment
- No visibility into service accounts

THE SOLUTION:

Real-time protection and visibility into all access-related activity

- Implemented MFA protection for all users and resources
- Strengthened AD hygiene by having complete visibility into user types and their activity
- Gained full visibility and protection of all service accounts

The challenge: Implement MFA protection across their user base and improve AD hygiene

As a prominent healthcare provider, Shannon Medical Center needed to increase its overall security posture. This meant applying MFA protection to its entire user base and gaining better visibility into its admin users' activity as well as its overall IT infrastructure.

"We wanted to be more secure because we run a hospital and protecting our patients' sensitive data is a top priority. We initially didn't have MFA protection applied to any of our users or resources across our environments, and we specifically needed it on all access requests to our electronic medical records (EMR) application. We also needed external MFA for remote users and for our admin credentials to prevent malicious actors from making powerful lateral movements via PowerShell if they were compromised. This led us to think about how we could add MFA protection to our admin credentials and domain admins," says Ashley Nesbitt, System Security Administrator at Shannon Medical Center.

To strengthen their overall identity security posture management, Shannon Medical Center first needed to gain better visibility and management of their Active Directory.

> "We faced significant challenges in maintaining Active Directory (AD) hygiene. We lacked visibility into our user base and the different types of users that we had in our AD environment."
>
> – Ashley Nesbitt,
> System Security Administrator at
> Shannon Medical Center

Our efforts to secure our environment were further complicated by this blind spot, which made it difficult for us to understand how we could improve our overall security posture. Conducting AD audits was an extremely challenging task, further complicating our efforts," Nesbitt added.

Limited visibility into user and service accounts

Additionally, Shannon Medical Center quickly realized they needed visibility into the activity of user and service accounts in their environments.

> "As part of our efforts to increase our security posture, we faced challenges around protecting our service accounts. We have approximately 1000 service accounts, and we needed improved visibility into their activities."
>
> — Ashley Nesbitt,
> System Security Administrator at Shannon Medical Center

"We had an issue where people's accounts were being locked randomly. Due to the inability to pinpoint the problem, troubleshooting was very difficult. After becoming a Silverfort customer, they helped us realize it was our RADIUS server," said Nesbitt

"This helped us determine/troubleshoot the issue of these random locked-out accounts. The limited visibility into these user and service accounts made it extremely difficult to identify and troubleshoot irregular activity," added Nesbitt.

Due to the variety of security challenges and their increased awareness of identity threats, Shannon Medical Center began searching for an identity security solution that would meet all their security needs as well as the needs of their healthcare environment.

"We were looking to proactively – rather than reactively – secure our admin credentials and this led us to Silverfort. We ran a demo and a technical POC with Silverfort and they clearly displayed that what they were offering actually works. This helped us make the decision to go with Silverfort. Unlike other security solutions, Silverfort does exactly what it says it does, which is the most important factor for us when deciding to partner with a security solution," says Nesbitt.

The solution: Quick deployment led to company-wide MFA protection and greater AD hygiene

After signing on with Silverfort, Shannon Medical Center quickly deployed the solution and immediately saw an increase in its security posture.

"We implemented ten access policies that quickly extended MFA protection across our environments. Our Silverfort policies helped us secure our admin credentials while adding MFA protection to access requests to our domain controllers. As an additional security measure, we implemented Silverfort's MFA protection for all access requests to VMware vCenter Server. Thanks to Silverfort, we now have complete visibility into all our accounts' behavior and all access requests to our core business applications," Nesbitt said.

Shortly afterward, Shannon Medical Center gained additional value from Silverfort around AD hygiene.

> "After deploying Silverfort, we started to see a return on our investment, especially around our AD hygiene needs. We now have complete visibility and proactive insights into our users' activities, the types of users in our AD environments, and which users were using NTLMv1."
>
> — Ashley Nesbitt,
> System Security Administrator at Shannon Medical Center

This helped us manage our AD environment more efficiently while improving our company security posture," Nesbitt added.

They also improved their AD hygiene by decreasing the number of unwanted authentications in their environment. “As a result of Print Nightmare, our environment was experiencing over 24,000,000 daily authentications, which was extremely unusual,” said Nesbitt

> "In addition to identifying the issue and helping us eliminate a remnant log that Print Nightmare caused, Silverfort also lowered the daily authentication amount to 2,000,000. If it were not for Silverfort, we would not have known what was occurring in our environment."
>
> — Ashley Nesbitt,
> System Security Administrator at Shannon Medical Center

Complete service account protection

In their initial review of the product, Shannon Medical Center was shown how Silverfort could help with service account security. They soon realized that Silverfort’s service account capabilities were extremely useful for their security needs.

> "Once we realized that Silverfort could help us protect our service accounts with virtual fencing, we knew this was a feature we needed."
>
> — Ashley Nesbitt,
> System Security Administrator at Shannon Medical Center

Since implementing Silverfort’s service account capabilities, Shannon Medical Center has full confidence in knowing that its service accounts are being continuously monitored and protected.

“We are protecting approximately 1000 service accounts using Silverfort, enabling us to determine the source, destination, and last time a service account was used for each account. If, for instance, we notice in our Silverfort console that there is a service account that has not been used for more than three months, we know it is time to remove the account from our environment. We have found Silverfort’s service account capability to be extremely valuable for our overall security posture strategy,” said Nesbitt.

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