Silverfort

CASE STUDY

Reducing risk from high to low: How Encora brought every AD identity under control with Silverfort

BASED

Bangalore, India

INDUSTRY

Digital engineering and technology services

USERS

10,000+

ENVIRONMENT

Active Directory
Entra ID, Microsoft Authenticator
SIEM

encora

Encora is a global digital engineering company that helps organizations design, build, and scale technology products and services. Operating across multiple geographies worldwide, Encora works with clients across industries to accelerate innovation—from cloud and data modernization to AI-driven product development.

THE CHALLENGE:

Enforcing Identity Security controls across a distributed hybrid environment with no centralized visibility into critical Active Directory (AD) accounts.

- Lack of visibility into service accounts and privileged accounts managed independently across global business units
- Inability to enforce MFA across privileged accounts and restrict service account activity to approved sources and destinations
- Unknown service account ownership and uncontrolled authentication paths created unquantified risk across the entire AD environment

THE SOLUTION:

Gained full visibility into all AD-based identities, enforced MFA protection across privileged access, and applied identity-based controls across a distributed hybrid environment.

- Discovered and classified 100+ previously unmanaged service accounts across decentralized business units
- Enforced MFA protection across 250 previously unprotected privileged accounts
- Replaced uncontrolled authentication paths with granular access-based control policies, achieving audit-ready controls aligned with ISO 27001, SOC II, and cyber insurance requirements

The challenge: Decentralized account management left critical identities unmonitored and access paths uncontrolled

Encora delivers its global technology services across multiple geographies through a deliberately decentralized model, delegating account management and system administration to local business units. For day-to-day business operations, this works well, but for Identity Security, it created a critical blind spot: with no central visibility, a growing number of accounts sat outside any security controls.

> "We were trying to identify accounts that are not mapped as user accounts—service accounts, accounts we cannot put MFA on, admin accounts. There was no visibility."
>
> — Ankit Agarwal,
> VP of Global Systems and Security at Encora

The service account problem ran deeper than visibility alone. With account creation delegated across business units and no central ownership model, accounts accumulated over time with no record of their purpose, their owner, or where they were authenticating.

"The problem was who created the account and who is the owner—and when someone creates a new service account, nobody questions whether it is required or whether an existing one could be used. There was no thought process going on." said Ankit

Beyond account visibility, the security team also lacked any enforcement capabilities.

Privileged accounts had no MFA protection, and service accounts—many with unknown ownership—operated without any restriction on where they could authenticate. With no policies defining which sources and destinations these accounts could reach, every unmonitored authentication path represented a potential attack vector Encora had no way to detect or contain.

Finding the right Identity Security platform

Led by a proactive effort to address known weaknesses in its Identity Security posture, Encora started the search for a solution with a clear requirement: unified visibility and protection across its hybrid, decentralized environment. The security team evaluated several IAM solutions but found they didn't extend to the on-prem environment, leaving its AD infrastructure uncovered.

Silverfort's ability to cover every AD-managed authentication across a hybrid environment—without requiring infrastructure changes or application modifications—made it the only solution that matched Encora's requirements. The security team validated its core use cases of AD visibility, account discovery, and MFA enforcement through a proof of concept (POC). It confirmed that Silverfort could provide the exact level of granularity Encora required.

> We tried to have this discussion with Microsoft, but we could not get clarity on what it could provide for our environment. At that time, we could find only Silverfort doing that kind of visibility—because we were running in hybrid mode, and in hybrid mode you have to cover on-prem first.
>
> — Ankit Agarwal,
> VP of Global Systems and Security at Encora

The solution: Centralized visibility, granular MFA enforcement, and identity-based access control across every AD account

Deploying Silverfort across Encora's environment was straightforward. **From the moment the platform was live, the security team gained immediate visibility into account activity that had previously been invisible**, surfacing dormant accounts, password hygiene gaps, and unmanaged identities accumulated across the decentralized environment.

> "When we first installed Silverfort, the console provided a lot of insights: how many users had not changed their password, where password expiry was set, which accounts were still active but dormant. The governance and security teams were not ready to see that kind of observation."
>
> — Ankit Agarwal,
> VP of Global Systems and Security at Encora

Following a six-month maturation process, Encora worked systematically through the initial findings. They filtered, prioritized and built a repeatable remediation process with the Silverfort dashboard as the central reference point and the SOC integrated to triage ongoing alerts.

"I always say that deployment is only ten percent of the journey. Eighty percent depends on how you use and mature the solution over time." said Ankit

From unknown to controlled: Service account discovery and protection

With AD hygiene established, Encora focused on the service accounts that posed the greatest risk. **Silverfort surfaced over 100 previously unmanaged service accounts across its hybrid environment**, giving the security team a complete picture of what existed, who owned it, and where it was authenticating for the first time.

For each discovered service account, Encora applied virtual fencing policies, restricting each service account to its intended sources and destinations and eliminating the uncontrolled authentication paths that had accumulated over years of decentralized account creation.

> In a decentralized model, account management becomes people-driven rather than process-driven. Now with Silverfort, we get instant discovery. We can question who created an account, understand why, and immediately put boundaries on it. With the right proactive and reactive controls in place, the time to discovery reduces and your overall security position improves.
>
> — Ankit Agarwal,
> VP of Global Systems and Security at Encora

MFA enforcement and granular access control for privileged accounts

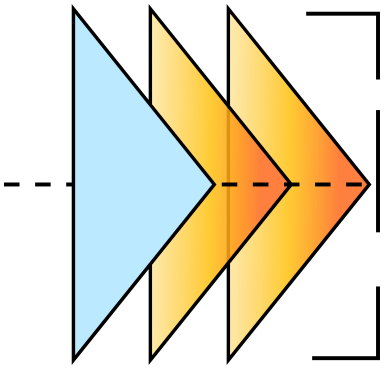
Silverfort also helped Encora close a long-standing protection gap around privileged accounts. The security team enforced MFA across 250 accounts, applying more than 100 granular policies across systems and access paths outside any security controls. This included privileged access over RDP, SSH, Windows logon, and web-based authentication, with precise policy enforcement replacing broad, one-size-fits-all controls.

Enforcing MFA protection was just the beginning. The security team also adopted Silverfort's Authentication Firewall to apply identity-based controls before authentication requests could proceed, limiting access to approved sources and destinations. The result was a measurably reduced attack surface and audit-ready controls that now support Encora's ISO 27001, SOC II, and cyber insurance requirements directly.

"When you talk about traditional MFA, broadly, the risk will not reduce from high to low, because you can still bypass MFA, get MFA fatigue, etc. With Authentication Firewall, we first try to see the source and destination from where the hits are coming, and we put a logical boundary on this. We approve only those which are legitimate, and then we go for the MFA. By combining both things, I reduce my risk from high to low."

— Ankit Agarwal,
VP of Global Systems and Security at Encora

Looking ahead: From AD security to a holistic identity platform



With its AD environment secured, Encora is now looking to expand its use of the Silverfort Identity Security platform. The security team is now looking to:

- Extend into the Privileged Access Security module to protect their privileged accounts
- Leverage Silverfort's SailPoint integration to bring real-time risk insights into governance workflows
- Explore how Identity Security controls can be extended to AI agents and non-human identities across its growing technology estate

"It is very difficult to move away from on-prem directly. Most organizations have this kind of structure with similar problems discovering human and service accounts. Silverfort is unique in this space as a holistic Identity Security platform. As for AI agents—how they interact, how they authenticate, how you put boundaries on them—that is definitely on our roadmap."

— Ankit Agarwal,
VP of Global Systems and Security at Encora

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