Silverfort

CASE STUDY

From visibility to runtime protection: How Godrej Industries Group secured 25,000 hybrid identities with Silverfort

BASED
Mumbai, India

INDUSTRY
Diversified Conglomerate

USERS
25,000+

ENVIRONMENT
Active Directory
Multiple AD domains
Entra ID, Microsoft Authenticator

GODREJ INDUSTRIES Godrej

Godrej Industries Group is one of India's largest diversified conglomerates, founded in 1897. Its businesses span consumer products, real estate, agribusiness, chemicals, and financial services—through companies including Godrej Consumer Products, Godrej Properties, Godrej Agrovet, Godrej Industries (Chemicals), and Godrej Capital. The Group's businesses operate across Asia, Africa, and Latin America and serve over one billion consumers worldwide.

THE CHALLENGE:

Protecting service accounts, privileged access, and legacy systems across Active Directory (AD) without runtime enforcement.

- Lack of real-time visibility into authentication activity for privileged and service accounts across on-prem AD
- Inability to enforce MFA for privileged access across legacy systems, command-line tools, RDP, SSH, and restrict service account activity to approved sources and destinations
- Lack of runtime protection against active identity threats, with existing tools limited to detection and reporting

THE SOLUTION:

Real-time protection across ~25,000 hybrid identities, with granular policy-driven enforcement aligned to Godrej's existing account classification model.

- Gained continuous visibility into authentication activity and cleaned up dormant service accounts were previously undetected
- Enforced MFA to protect privileged access across legacy applications, RDP, SSH, and PowerShell
- Restricted service accounts to their intended applications and servers, and blocked privileged access to domain controllers and tier-0 systems—preventing lateral movement at runtime

The challenge: Limited visibility without runtime protection left privileged access exposed and service account activity uncontrolled

Godrej Industries Group runs a hybrid identity environment that supports manufacturing sites, R&D, and commercial operations across multiple regions. The complex model works well for day-to-day operations but leaves a critical Identity Security blind spot: no real-time view into authentication activity, especially for the service and system accounts that quietly run applications and automated processes across the business.

> "The primary constraint we had was very limited visibility into identities, especially the ones which are not generally used by an individual but rather are hard coded somewhere in the application."
>
> — Satyavrat Mishra,
> Head of Corporate IT and Group CISO at
> Godrej Industries Group

Service accounts had accumulated with built-in exposure. They often had passwords that never expired, with credentials hard coded into applications that had not been touched in years. With no real-time visibility into how these accounts were used, Godrej Industries Group could not detect when one of these accounts was being used outside its intended purpose.

"If an application account gets compromised and somebody uses it to log into a system and then do privilege escalation, there was no visibility for that." said Satyavrat

Even where authentication activity was visible, the team had no security controls to enforce.

Privileged accounts lacked MFA across legacy applications, command-line tools, RDP, and SSH. Service accounts ran without any restriction on the sources and destinations they could authenticate to. By the time Godrej had enough signals and context to investigate an abnormal authentication, the access had already happened.

Finding the right Identity Security platform

Godrej Industries Group set out to find a platform that could enforce protection in real time across human and non-human identities (NHIs), on-prem and cloud. The security team previously used an identity solution that provided some baseline visibility coverage, but it had since been deprecated and could not provide runtime protection across all identities.

The security team evaluated several alternatives across the AD security and ITDR categories. Each surfaced posture issues or detected anomalies, but none could enforce protection at the moment of authentication itself. That was the distinction Silverfort delivered. A Proof of Concept (POC) confirmed what the team needed to see: the platform could enforce MFA, virtual fencing, and access policies inline at the point of authentication and across the hybrid environment.

> "Most of the tools could only pinpoint the problems. They could not give us the solution. We were more interested in getting to the solution itself rather than just receiving a score or a report."
>
> — Satyavrat Mishra,
> Head of Corporate IT and Group CISO at
> Godrej Industries Group

The solution: Real-time visibility, MFA enforcement, and identity-based access control across ~25,000 hybrid identities

Godrej Industries Group deployed Silverfort without disruption, and the platform began surfacing real-time authentication activity from the first weeks of rollout.

"Compared to many other solutions, it was pretty straightforward and far easier to implement." said Satyavrat

Within three months, the security team gained full identity coverage across its hybrid environment. For the first time, Godrej Industries Group had continuous, real-time visibility of authentication activity across all ~25,000 identities, including service and system accounts that had previously been the hardest part to cover. With that level of visibility in place, the security team began a structured cleanup of dormant accounts that had not been used in months and were no longer tied to any active system or process.

> "While we knew how many service accounts we had, we never really knew whether they were still needed. People come when they need a new account created, but nobody comes back to say an account is no longer in use. After looking at the report, we could do a complete cleanup."
>
> — Satyavrat Mishra,
> Head of Corporate IT and Group CISO at
> Godrej Industries Group

With the dormant accounts cleared, the security team focused on protecting the hundreds of service accounts that remained. Building on existing AD classification model, Godrej Industries Group applied virtual fencing policies on a per-account basis: each service account bound to the specific applications and servers it was meant to access, with interactive logon disabled across the board. Any authentication attempt outside the defined boundary is denied at the point of authentication.

> "For service accounts, we go one level below and bind each one to a particular application or server. If somebody tries to use that account somewhere else, it won't work—Silverfort throws an error saying login not allowed"
>
> — Satyavrat Mishra,
> Head of Corporate IT and Group CISO at
> Godrej Industries Group

Multi-layered approach to protect privileged access

Privileged human access required a different layer of protection. Rather than defining access-based policies protocol by protocol, Godrej Industries Group enforced MFA at the level of the account itself.

The team leveraged its existing AD classification model so that every privileged account, every domain administrator, and every third-party contractor inherited the right policy automatically based on its tagged type.

With this granular approach, Godrej could protect privileged access across its entire hybrid environment, including legacy applications, RDP, SSH, PowerShell, and command-line tools.

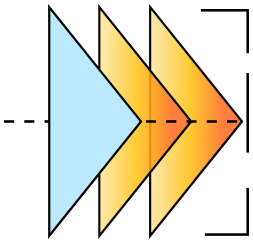
> "We've classified all ~25,000 identities. We mark each account with a type based on a custom field within Active Directory, so we don't have to figure out what kind of account it is after something has happened. We know just by looking at it—and that's what makes the Silverfort MFA policy work"
>
> — Satyavrat Mishra,
> Head of Corporate IT and Group CISO at
> Godrej Industries Group

On top of MFA protection, Godrej Industries Group used Silverfort's Authentication Firewall capability, giving them an additional control plane for privileged access. The security team applied deny and identity-segmentation policies to protect access to domain controllers and critical servers, enforcing a real Least Privilege model and proactively preventing lateral movement before it could begin.

"Authentication Firewall closed the last gap we had in privileged access. Even when an account is legitimate and an authentication is technically authorized, we now control exactly where it can go—and that's what gives us confidence in our least-privilege model."

— Satyavrat Mishra,
Head of Corporate IT and Group CISO at
Godrej Industries Group

Looking ahead: Continuous identity protection across an evolving hybrid environment



With runtime protection established across its hybrid environment, Godrej Industries Group continues to mature its Identity Security model—refining policies, extending enforcement to new applications as they come online, and applying the same classification-based discipline to every new account that enters the environment. Identity Security has become a continuous practice rather than a one-time project.

"For any organization that wants runtime protection across all their identities, this is the right solution. Compared to many other solutions, it was pretty easy to deploy. And it works in on-prem and hybrid environments—that matters in industries where SaaS isn't always an option."

— Satyavrat Mishra,
Head of Corporate IT and Group CISO at
Godrej Industries Group

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