

CASE STUDY

Strengthening privileged access control at scale: How JBPCO applies Vaultless PAM without added operational overhead



BASED

Texas, US



INDUSTRY

Manufacturing
(Automotive)



USERS

8,000+ Employees



ENVIRONMENT

Active Directory, OT environment,
Remote Desktop (RDP), Entra ID

JB POINDEXTER & CO

JB Poindexter & Co (JBPCO) is a manufacturing conglomerate operating across multiple business units in North America, primarily within the automotive sector. Its operations support a wide range of internal teams involved in day-to-day manufacturing and production activities.

THE CHALLENGE:

Reducing lateral movement risk by extending control over privileged access at scale

- Gaps in control over administrative access paths increased the risk of lateral movement across the environment
- Accumulated privilege drift and permission sprawl across Active Directory over time
- Limited capacity to manage and segment access consistently across a large, distributed environment

THE SOLUTION:

Implemented Vaultless PAM to reduce risk and improve control, with no operational friction

- Enrolled privileged users into Just-In-Time (JIT) access within one week, effectively reducing standing access across critical accounts
- Rolled out privileged access controls and applied security policies within 30 days
- Gained immediate visibility into remote desktop usage and enforced MFA protection for high-risk administrative actions like launching PowerShell prompts

The challenge: Reducing lateral movement risk and addressing legacy privilege sprawl at scale

JBPCO operates in a large and distributed environment, where administrative access is required across multiple sites and systems. Maintaining consistent control over how privileged access is used across the organization is therefore inherently complex, particularly at scale.

Led by Cyber Security SOC Manager Luke Hamilton, JBPCO's primary initiative was to reduce lateral movement risk and reduce the blast radius in the event of a cyberattack.

"With Silverfort, we were able to purchase the module and within a week enroll all of our most privileged users into just-in-time access and effectively have our most critical accounts disabled, unless they're in use."

— Luke Hamilton, Cyber Security SOC Manager, JBPCO

At the same time, JBPCO needed to address long-standing Active Directory privilege drift, where employees had accumulated permissions over time that were difficult to review and manage.

The organization's lean operating model added further complexity. With 95 sites, manually segmenting the environment or reworking access controls using traditional approaches would require significant time and effort.

"We really endorse lean teams, and for us to be able to segment the network across 95+ sites, it would have taken a couple of years."

— Luke Hamilton, Cyber Security
SOC Manager, JBPCO

Finding the right identity security platform

"It was really important for us to find something we could manage with the team we have and introduce controls without adding operational complexity."

— Luke Hamilton, Cyber Security
SOC Manager, JBPCO

"When we were evaluating platforms, we evaluated some of the larger ones that include vaults. But it became apparent very quickly that it was going to be a very large administrative overhead for the platform and it was going to require a lot of specialized knowledge to be able to set up the integrations and the automation necessary to make the implementation of a platform like that seamless.", said Luke Hamilton, Cyber Security SOC Manager, JBPCO.

Needing to implement privileged access controls without slowing down the business, JBPCO selected Silverfort's Vaultless PAM approach. The platform allowed the team to apply identity policies from a central control point, without requiring changes to existing workflows.

The solution: Rapid deployment & seamless user experience with Vaultless PAM

After performing a Proof of Concept (PoC), JBPCO transitioned and began rolling out privileged access controls across its environment. Policies have been implemented within 30 days, allowing the team to introduce controls in a structured and controlled manner, supporting a reduction in risk related to privileged access.

"With Silverfort, we were able to purchase the module and within a week enroll all of our most privileged users into just-in-time access and effectively have our most critical accounts disabled, unless they're in use.", said Luke Hamilton, Cyber Security SOC Manager, JBPCO.

This allowed the team to deploy and manage the platform without requiring significant changes to their existing environment.

Gaining visibility and applying controls to administrative activity

Following deployment, JBPCO gained complete visibility into permission usage and administrative activity across its environment, including remote desktop usage. This allowed the team to identify where access was broader than expected and begin applying more targeted security controls.

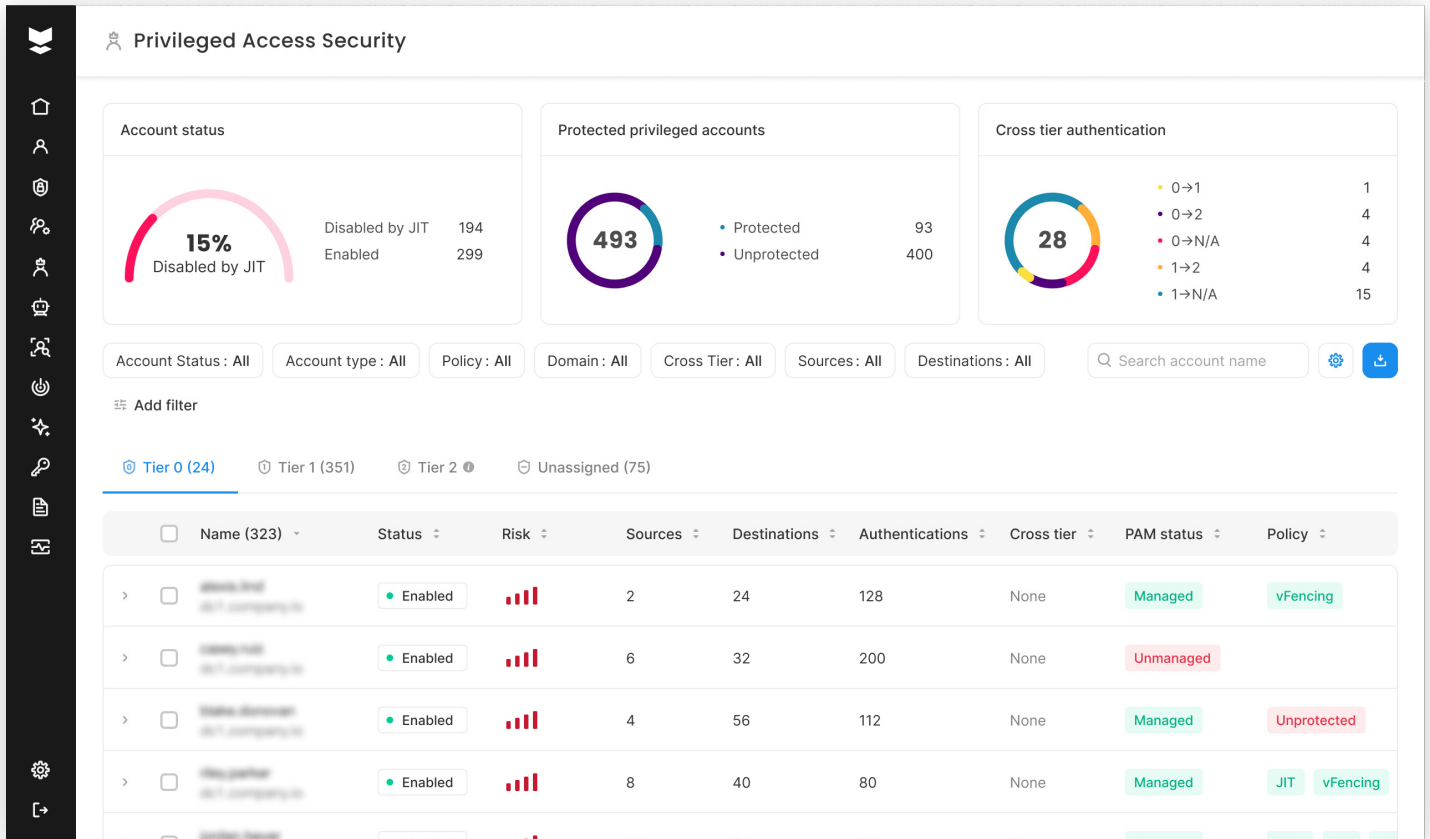
Using these insights, JBPCO implemented access-based policies requiring MFA for administrative PowerShell sessions, supporting more controlled use of administrative tools and reducing exposure to lateral movement.

"One of the pieces of feedback that we've gotten about Silverfort is that our IT people love it. We've received strong feedback because it fit our business and didn't create operational impact, while allowing us to reduce risk at a scale we wouldn't have been able to achieve otherwise."

— Luke Hamilton, Cyber Security
SOC Manager, JBPCO

The deployment was managed by a technical team of four people, supporting over 12,000 identities at scale.

Simulation of the Silverfort Privileged Access Security Module



Looking ahead: Securing AI agents and non-human identities

With human privileged access more tightly controlled, JBPCO is now extending its focus to non-human identities. The team is working on establishing behavioral baselines to restrict service accounts and applying virtual fencing policies to ensure they are only used within their intended scope.

At the same time, JBPCO is exploring how similar principles can be applied to emerging areas such as AI, where managing identity and access for agents is becoming increasingly important.

"Our next big focus is around agentic AI security and how we handle identities in that space and applying the principles of just-in-time access in those environments."

— Luke Hamilton, Cyber Security SOC Manager, JBPCO

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.