

Closing the Gaps:


How Productiv Secured SaaS Credentials and Privileged Service Accounts with Cerby



Managing access to an expanding portfolio of SaaS applications is a critical challenge for modern enterprises, especially when some apps can't be integrated and managed through a central identity provider (IdP).

For Productiv, a leading SaaS Management Platform, this challenge was no exception. While Okta secured most of their SaaS ecosystem, apps outside its coverage and shared service accounts introduced security blind spots and operational inefficiencies that IT couldn't overlook. As their business scaled, addressing these gaps became essential to maintaining governance and efficiency.

“We needed a way to secure all our SaaS apps, including those outside of SSO coverage, without sacrificing efficiency or visibility”, “Privileged service accounts were a particular challenge, and we wanted full auditability for every login and action.”

 Josh Mullis
VP of IT & InfoSec



The Challenges of SaaS Access Management

Productiv's IT team faced three critical challenges:

1. Shared Service Accounts:

These privileged accounts, essential for administering SaaS apps, were difficult to manage and secure. Multiple users could access the same credentials simultaneously, making it difficult to trace who logged in or what actions were taken by an individual administrator.

2. Multi-Factor Authentication (MFA):

MFA for shared accounts added another layer of complexity. Second-factor tokens, tied to individual users and devices, were cumbersome to share, introducing delays and frustration for users.

This challenge left the IT team with a difficult tradeoff between usability and security. While security always won, a better solution was needed.

3. Fragmented Credential Management:

Employees used a mix of enterprise password management tools and manual processes to log into apps outside Okta. This patchwork approach led to shadow IT, uneven security coverage, and challenges in enforcing policies across the organization.

Productiv needed a solution that would centralize access controls, enforce strong security, and provide complete visibility—all while staying cost-effective. That's when they turned to Cerby.



A Solution Built for Disconnected Apps and Shared Accounts

Cerby stood out for one simple reason: it solves challenges most identity solutions overlook. Productiv needed a way to manage shadow IT, secure disconnected apps, and eliminate the risks of shared credentials. Cerby addressed these challenges head-on, strengthening their overall security and governance strategy.

Securing Shared Service Accounts

By integrating with Okta, Cerby enabled workflows that extended least-privilege access to these shared accounts. Only authorized users with appropriate roles are granted access to check out shared credentials—and critically, only one person can use an account at a time. This granular control gave the IT team full traceability and auditability over privileged accounts, providing clear visibility into who accessed an account, when, and what actions were performed.

Simplifying MFA for Shared Accounts

Cerby also resolved long-standing MFA challenges for shared accounts. Instead of requiring team members to share second-factor tokens, Cerby centrally manages and autofills MFA, eliminating friction for users. This not only made MFA easy to use but also ensured it was consistently enforced across all privileged accounts.

Delivering a Unified Employee Experience

By syncing with Okta, Cerby provided employees with a single, secure platform to access all their work apps. Apps that don't support SSO are now accessible through the Okta dashboard via Cerby, enabling a seamless login experience. This eliminated the need to juggle multiple systems or figure out how to share a password securely, reducing both effort and frustration.

“When dealing with privileged service accounts and apps outside of SSO coverage, we needed better security, visibility, and auditability”, “Cerby delivered on all three.”

□ Josh Mullis
VP of IT & InfoSec



Results That Matter

Cerby's implementation delivered measurable results across Productiv's organization:



IT and Security

Shared service accounts are now fully auditable and secure. Centralized management of all apps—including those outside Okta—improved governance and eliminated risks.



Engineering

One-click password rotations for server accounts, automated by Cerby, saved hours of manual work and freed up engineering resources for higher-value tasks.



Finance

Sensitive banking credentials are now centrally managed and secured, giving IT full visibility and reducing risks.



Marketing

Plans are underway to use Cerby for managing shared social media and paid ad accounts, improving security and governance of the marketing tech stack.

A Partnership Built on Trust and Innovation

For Productiv, Cerby wasn't just another vendor—it became a trusted partner.

“Cerby is one of the few companies addressing the challenge of managing disconnected apps,” “Most solutions ignore this issue entirely. But by combining Cerby with Okta, we now have comprehensive access controls and governance across our entire app ecosystem, without gaps.”

□ Josh Mullis
VP of IT & InfoSec



What's Next?

Productiv plans to expand its use of Cerby to automate provisioning for apps that require costly license upgrades to enable SSO or SCIM functionality. This will ensure employees gain secure access on day one and lose access immediately upon departure, all while reducing IT's manual workload. Importantly, this approach will also help Productiv avoid the costly “SSO tax”, which they estimate can drive costs up to double or more for certain apps.

With Cerby, Productiv is bridging critical gaps in password sharing, security, and governance—building a scalable and secure foundation for the future.

About Cerby

Cerby is the only identity security platform built for disconnected applications, providing IT and Security teams with comprehensive control over apps that lack APIs or support for protocols like SAML or SCIM. Seamlessly integrating with existing identity providers (Okta, Azure AD, etc.), Cerby extends critical security automations—such as single sign-on, multi-factor authentication, and lifecycle management—to any application without incurring the costly “SSO tax.” Cerby automates essential tasks like user deprovisioning and password rotations, reducing manual work while closing security gaps. With Cerby, teams gain full control over their app ecosystem, strengthen security, and reduce costs.

