

Okta Privileged Access

Safeguard critical resources and achieve compliance objectives — without hindering productivity — with a privileged access management (PAM) solution that's fully integrated with Okta

Built on a foundation of identity controls, Okta Privileged Access empowers organizations to reduce risk with unified access and governance management for privileged resources — whether on-premises or in the cloud — resulting in better visibility, security and compliance, without compromising the user experience.

Okta Privileged Access is cloud-architected, fast to deploy and adopt and fully integrated with Okta.

Combating modern threats with identity controls

Abuse of privileges — whether by an external threat actor or by an insider — is a common attack pattern in today's cyber incidents. Accordingly, a wide range of regulations (e.g., Sarbanes-Oxley), frameworks (e.g., SOC 2), and standards (e.g., PCI) require identity controls, and cyber insurers are increasingly imposing Identity-related duty of care requirements.

While the specifics vary, these obligations tend to address three main areas: identity security, access controls, and separation of duties.

Okta Privileged Access applies similar identity controls, with a particular focus on protecting critical assets by — among other things — eliminating standing privileges, enforcing least-privilege access policies, implementing strict role-based access control (RBAC), and providing separation of duties between users who need to administer resources, those who configure access to privileged resources, and non-administrators.

Key capabilities and features

Just-in-Time (JIT) infrastructure access

Provides simple, centralized management of automated access controls that reduce the attack surface by eliminating standing credentials.

Features include:

- SSH and RDP tooling integration
- Dynamic Client Certificate architecture
- Server account lifecycle management
- Policy-based access controls
- Structured audit logs
- Extensive API for custom workflows and integration with automation tooling
- SSH and RDP session recording

Secrets management

Prevent unauthorized direct access by managing who can retrieve credentials, automating credential rotation, and minimizing exposure time of secrets.

- Secure storage for passwords, API keys, and tokens
- Policy-based access controls
- Protect non-federated service, shared, and break-glass accounts
- Scheduled and on-demand password rotations

Privileged accounts vaulting

Supports compliance requirements for eliminating standing access, secures shared accounts, and provides individual accountability for usage. Features include:

- Vaulting for privileged accounts: server local, Okta, SaaS service, Active Directory
- Scheduled password rotation
- Continuous monitoring for out-of-band password changes
- Policy-based access controls
- Brokered SSH and RDP sessions to shared/privileged local accounts
- Integrated request and approval
- Structured audit logs

Governance and auditing

Enforces business controls including multi-step approvals, business justification, and time-bound approval durations — with convenient, user-friendly integrations.

Features include:

- Integration with Okta Access Request
 - Ability to add request/approval into any privileged access access policy
 - Customizable multi-level approval builder
 - CLI integration for better SSH experience
 - Integration with Slack, Microsoft Teams, Web Inbox
-

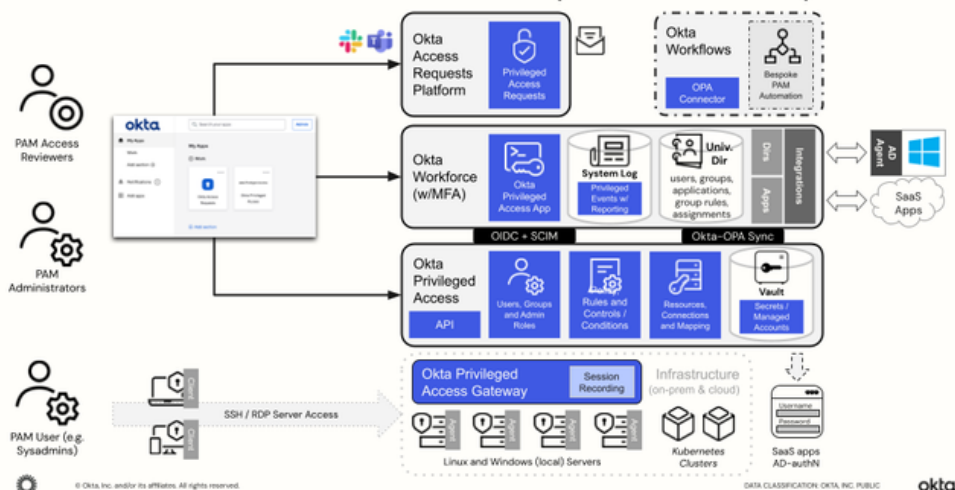
A unified architecture for holistic control over workforce identity

Using separate tools to manage your IAM, IGA, and PAM means admins have to configure and manage multiple connectors and configure policies in multiple solutions. Your organization can save time and strengthen security by consolidating these functions for holistic visibility and control. The Okta Platform is the foundation for an identity security fabric—going far beyond traditional Identity and Access Management.

Okta gives you an identity security fabric that brings together a complete set of secure identity products, delivering end-to-end protection across access management, governance, privileged access, and threat detection. What makes it even more effective is orchestration. This brings together all your user context, ecosystem signals, policies, and resources, enabling real-time, automated responses when threats arise.

The Okta Platform is bolstered by extensive integrations. Okta seamlessly connects with your entire tech ecosystem—ingesting risk signals, enriching context, and amplifying security outcomes across your stack. All of this, built on an enterprise-grade platform that's always on, delivering 99.99% uptime with zero planned downtime, built for scale, and securing billions of logins every month.

OPA Architectural Overview – components and capabilities



About Okta

Okta is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.