okta

Okta Privileged Access

Safeguard critical assets and meet growing regulatory, framework, standards, and cyber-insurance obligations — without hindering productivity — with a unified, cloud-native Workforce Identity solution

Built on a foundation of Identity, 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.

Unlike traditional privileged access management (PAM) solutions, Okta Privileged Access is:

- Passwordless first, using passwordless authentication to access resources with a cloud-based vault to support resources that require password-based authentication
- Cloud architected, rather than adapted from on-premises software
- Fast to deploy and adopt, with implementations possible in days or even hours instead of weeks or months
- Fully integrated with Okta's Workforce Identity Cloud (WIC), enabling it to leverage core Identity and Access Management (IAM) and Identity Governance Administration (IGA) capabilities

Whether an organization is implementing PAM for the first time, or has outgrown a legacy solution, Okta Privileged Access addresses today's requirements in a platform designed to keep pace with evolving needs.

Primary business outcomes

- **Stronger security:** Manage Identity risks to prevent attackers from finding and accessing critical systems
- **Faster compliance:** Quickly and easily implement Identity controls required by regulations, frameworks, standards, and cyber insurers
- **Enhanced productivity:** Allow your workforce to quickly and securely connect to critical resources by integrating with the tools they already use

Key capabilities

Just-in-time (JIT) infrastructure access

Session recording and audit

Secrets vaulting and brokering

Privileged access governance

okta

A unified solution for holistic control over Workforce Identity

Traditionally, organizations had to integrate multiple Identity solutions manually to implement necessary Identity controls. Such a siloed approach is expensive and inefficient to operate and often forces either/or choices between security and user productivity.

In contrast, Okta Privileged Access:

- Is part of a single control plane for managing access across all of an organization's applications, resources, and infrastructure
- Quickly and elastically scales with the same speed to deployment and ease of use as the organization's cloud infrastructure
- Empowers administrators to implement Identity controls that simultaneously strengthen security and enable increased workforce productivity

Combating modern cyber threats with Okta Privileged Access

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.

To that end, Okta Privileged Access equips organizations with a number of key capabilities, including:

JIT infrastructure access

- Reduces the attack surface and manages the risk of credential theft by eliminating standing credentials
- Automates access controls, allowing operations teams to focus on infrastructure and software — rather than the intricacies of IAM
- Provides simple, centralized management for server fleets and cloud-hosted databases

Secrets vaulting and brokering

- Supports compliance requirements for eliminating standing access to privileged accounts
- Provides scheduled credential discovery, password rotation, and continuous password verification checks
- Secures shared accounts and provides individual accountability for usage

Session recording and audit

- Supports compliance requirements for recording privileged access to servers via SSH/RDP
- Uses a proxy gateway architecture to protect servers from being exposed to raw internet traffic
- Gateway scans all incoming server access and includes high-availability (HA) configurations

Privileged access governance

- Enforces appropriate business controls with multi-step approvals, business justification, and time-bound approval durations
- Supports convenient requests and approvals through chat, email, or web interface
- Streamlines end-user interactions by integrating access requests within the CLI
- Assists with evaluating existing policies in IaaS services and to help design privileged entitlements for IaaS resources