Datasheet November 2024

okta

Okta Privileged Access

Safeguard critical assets and achieve compliance objectives — without hindering productivity — with a privileged access management (PAM) solution that's fully integrated into the Okta Workforce Identity Cloud (WIC)

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.

To help organizations quickly achieve objectives with minimal integration and administrative overhead, Okta Privileged Access is cloud-architected, fast to deploy and adopt, and fully integrated with Okta's Workforce Identity Cloud (WIC).

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 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

Session recording and audit

Supports compliance requirements for recording privileged access to servers via SSH/RDP, and prevents servers from being exposed to raw internet traffic. Features include:

- SSH and RDP session recording
- High-availability proxy gateway
- Tamper-proof session logs
- Additional controls, including network segregation
- Credentials are never exposed directly to the client
- Native integration with the Okta System Log

Secrets vaulting and brokering

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

- Vaulting of local server account passwords
- Continuous server local account discovery
- 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

Secure access to service accounts

Secure access and eliminate standing privileges to non-federated service accounts for top SaaS applications

- Manage service, shared, and break-glass accounts for top applications
- Create flexible request and approval flows for service accounts
- Secure passwords from applications with a vaulting service
- Control who can reveal or update a password for an account
- Automatic password rotation options
- Prove who had access to a specific account at a point in time

Privileged access governance

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
- Integration with IaaS services (AWS) to analyze and help customers implement entitlements to enforce least privileged access to IaaS resources

A unified architecture for holistic control over workforce Identity

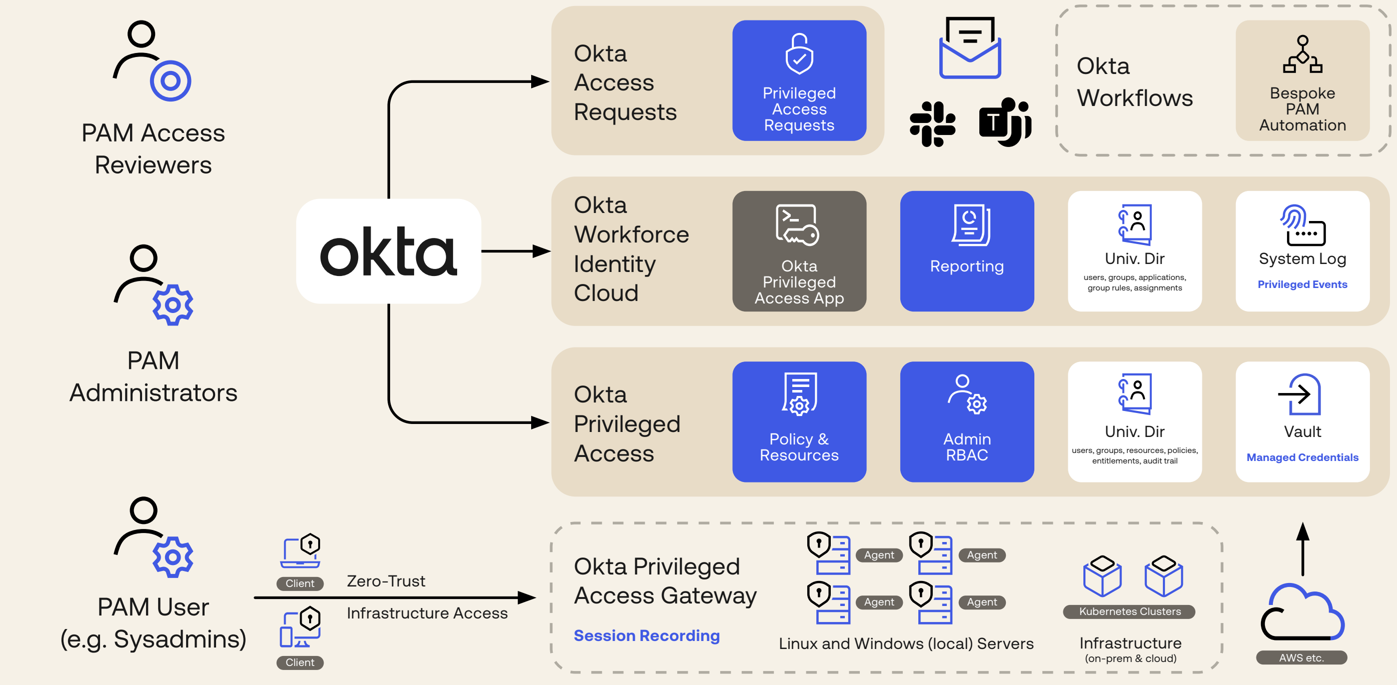
Leveraging Identity Threat Analytics, ITP delivers visibility into threats and analyzes anomalies to enable rapid, effective response. It strengthens threat mitigation capabilities through actionable insights, giving security teams the tools they need to analyze and act upon threat data in a timely manner.

- Okta Privileged Access provides passwordless authentication to access servers, databases, and IaaS servers (on-prem or cloud-hosted)
- A new powerful, cloud-based vault supports resources that require password-based authentication
- Okta Workforce Identity Cloud provides the user authentication for privileged access as well as the management of users and groups; the WIC also hosts the Okta Privileged Access application, provides the reporting interface, and also stores the audit trail in the Okta System Log

When privileged access governance controls are being used, the Okta Access Requests service provides a means to build approval flows and control the access requests. Request and approval flows may involve email and the web user interface, but for convenience can also leverage existing tools like Slack or Microsoft Teams.

These Okta Privileged Access infrastructure components exist in the organization's environment, either on-premises or in the cloud:

- **Privileged Access Client software**
  Runs on user workstations to manage access to servers or Kubernetes clusters
- **Privileged Access Agent**
  Is installed on servers (e.g., Linux and Windows local servers) to manage users, groups, and connections
- **Privileged Access Gateways**
  Provide network control points and implement additional functionality including session recording



Okta's forward-looking statement applies to this article.

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.