CyberArk Privileged Account Security Integrated with OneLogin Identity Management

Highlights

▌ Gain security around access control for privileged credentials

▌ Centralize access management across users, applications, and devices

The advent of ubiquitous cloud adoption has created the need for complex security infrastructures that protect both cloud-based and legacy systems. IT and Security teams struggle to prevent data breaches of highly sensitive corporate data, particularly privileged account access to key systems, without jeopardizing business productivity.

OneLogin and CyberArk work together to prevent costly data breaches and respond to security threats at the frontline. The joint solution allows organizations to establish user identities to ensure only authorized users can gain access to sensitive resources.

How It Works

OneLogin is a cloud-based identity and access management platform that centralizes access control of users, applications, and devices company-wide. By integrating with user directories like Active Directory, LDAP, Workday, and G Suite, OneLogin empowers organizations to define and execute access policies, like single sign-on (SSO), multi-factor authentication (MFA), and password reset based on user privilege level.

CyberArk facilitates the secure environment - on-premises, in the cloud, or in a hybrid environment - to protect privileged account credentials (including OneLogin credentials) that unlock your most sensitive data, while OneLogin ensures secure and trackable authentication into CyberArk.

1. Directory integration to Active Directory, LDAP, Google or HCM Directories (OneLogin)
2. Authentication policy creation, enforcement, and management (Single Sign-On, Multi-Factor Authentication, IP based, etc.) (OneLogin)
3. Secure environment for storing and managing privileged account credentials and the data they protect. (CyberArk Privileged Account Security solution) (CyberArk)
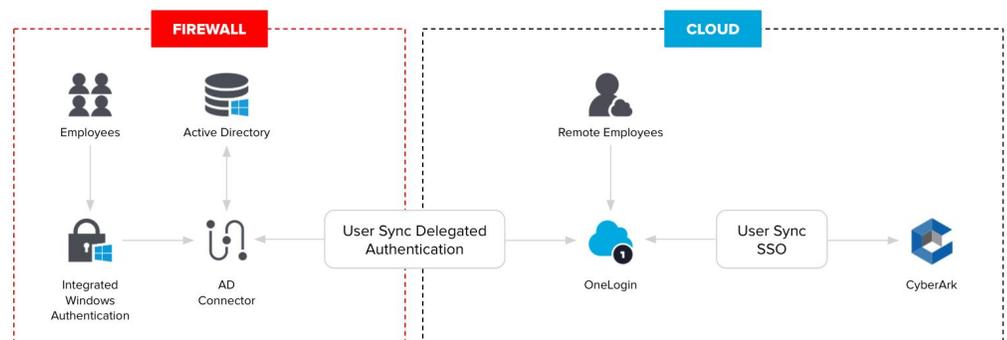
OneLogin Solution

- Secure application access across corporate desktops, web, and mobile

- Create and enforce authentication policy creation and enforcement

- Gain analytics and reporting on user management and login activity

- Integration with Active Directory, LDAP, G-Suite, and HCM solutions

CyberArk Solution

- Protect, manage and audit privileged credentials (e.g. passwords, SSH keys API tokens, etc.)

- Monitor, control, and isolate privileged sessions

- Analytics and alerting on malicious privileged account activity

- Apply least privilege access control for UNIX, Linux and Windows

- Enforce privilege security on the endpoint

- Secure and manage privileged credentials used by applications

OneLogin Products:

▮ Cloud-Based Identity and Access Management / Authentication Security

▮ OneLogin Desktop / Endpoint Management

CyberArk Product:

▮ CyberArk Privileged Account Security Solution

Summary

OneLogin's directory sync enables secure authentication into CyberArk, providing an extra layer of security around stored credentials. The real-time aspect ensures user permissions are updated immediately based on AD security groups and, in turn, that unauthorized CyberArk access is prevented and approved access is easy and secure.

CyberArk provides the industry's most comprehensive solution to protect privileged accounts from misuse at the identity perimeter. The CyberArk Privileged Account Security solution is a unified, enterprise-class solution that helps organizations manage and secure privileged accounts. It allows organizations to secure credentials, including passwords and SSH Keys, control access to these accounts, and isolate and record privileged sessions. Built on a single platform, the solution centralizes all privileged activity and provides centralized privileged account activity monitoring, protection, and control.

Joint OneLogin + CyberArk Solution

- Ensures only authorized, privileged users can access their accounts within CyberArk. Customers can enforce SSO Identity Management with the CyberArk solution to enable centralized, secure access to resources across the organization
- Reliable and comprehensive password protection
- Control and visibility for CyberArk IT / Security administrators (eg: instant kill switch to CyberArk, activity reports, etc.)
- Improved security without sacrificing productivity and user experience