CYBERARK® IDENTITY SINGLE SIGN-ON
SECURE ACCESS EVERYWHERE

OVERVIEW

CyberArk Identity Single Sign-On

Cloud-based IDaaS solution that enables you to secure access to applications and infrastructure with one set of credentials.

- Modern Single Sign-On
- Contextual Access Management
- Secure Directory Services
- VPN-less Access to Legacy Apps
- Real-Time Access Intelligence

FEATURED HIGHLIGHTS

Single Sign-on
Strengthen Security and Simplify Authentication

- Simplify access with one set of credentials
- Reduce the risk of poor password practices
- Integrate with CyberArk Identity MFA to protect user credentials

As organizations adopt cloud and hybrid infrastructure and embrace an increasing variety and volume of SaaS applications, effectively managing and controlling access to corporate resources presents significant challenges. Today, strong enterprise security hinges on the ability to securely authenticate identities and control access for every person, application and machine across the extended enterprise. CyberArk Identity Single Sign-On is a cloud-based Identity-as-a-Service (IDaaS) solution that simplifies identity management and reduces reliance on passwords, providing secure access to all applications and IT services via a single set of user credentials.

ACCESS MANAGEMENT CHALLENGES

Password sprawl reduces productivity

Today's workers rely on a wide variety of applications to perform their jobs. Many employees are forced to memorize and track a dizzying array of frequently changing passwords. Overwhelmed by password sprawl, many users take risky shortcuts like using the same password for all applications, using weak passwords, repeating passwords, or writing passwords on paper. Bad actors can take advantage of lax password management practices to mount cyberattacks and steal confidential data.

Account and password management increases helpdesk costs

Many businesses are hampered by disjointed identity management systems and practices. Each application and service has a distinct set of user accounts, credentials and password rules. Onboarding users, resetting forgotten passwords and re-activating locked accounts is a manually intensive, time consuming proposition that burdens the helpdesk and diverts valuable IT staff from more critical business issues.

Manual access management creates compliance gaps

With dozens — or hundreds — of apps in use, controlling which users have access to which apps is untenable. User accounts and credentials often remain in place long after employees change roles or leave the organization, exposing the business to data loss, compliance gaps and regulatory fines.

SMARTER AND SECURE ACCESS

CyberArk Single Sign-On (SSO) provides easy to manage, one-click access to all enterprise applications — cloud, mobile and legacy — helping organizations improve user experiences, strengthen security and reduce risk. The solution uses behavioral and contextual analytics to assess risk, automatically adapting access controls to streamline user interactions and reduce user frustration.

The optional CyberArk Identity App Gateway service lets you extend CyberArk SSO benefits to on-premises web apps like SharePoint and SAP. without VPN deployment hassles, administrative burdens or security risks. Unlike with a VPN, with App Gateway, users can only connect to their assigned on-premise apps and nothing else.

CyberArk Single Sign-On provides security, simplicity and control. IT Teams gets one place to manage all accounts and devices. Users get single sign-on across cloud, mobile and legacy apps from any device anywhere.

Security

- Reduce security risks posed by weak, reused or improperly managed passwords.
- Enable secure, remote access to on-premises apps — without the risks and hassles of VPNs.
- Implement adaptive access policies that adjust automatically based on risk and user behavior.

Simplicity

- Save time and resources by centralizing authentication and identity management functions.
- Deploy thousands of pre-integrated cloud and mobile applications. CyberArk Identity App Catalog includes many pre-configured applications that support SAML and OIDC protocols.
- Reduce helpdesk tickets for password resets and access requests with self-service tools and automated workflows.

Visibility and Control

- Justify investments and demonstrate compliance with granular access reports for apps, users, and devices.
- Enforce uniform access control policies for all enterprise applications and resources, across data centers and clouds, using a single authority.
- Improve IT visibility with centralized access monitoring, auditing and reporting for all applications and services.

www.cyberark.com

FEATURED HIGHLIGHTS
[CONTINUED]

Contextual Access Management
Adaptive Access Controls

- Leverage machine learning and artificial intelligence to assess risk and streamline access security access requests
- Use behavior analytics to identify and block suspicious activity, while simplifying access for legitimate users
- Optimize end-user experience while enhancing security

Secure Directory Services
Identity Federation from Anywhere

- Federate identities across on-premises and cloud-based directories
- Use any combination of directories, including Azure AD, Active Directory, LDAP and Google Directory
- Create and store user records in the CyberArk Identity Cloud Directory

CyberArk Identity App Gateway
VPN-less Legacy App Access

- Reduce attacks by providing app-specific access controls
- Eliminate security gaps with uniform access control policies across legacy and cloud apps
- Avoid VPN-orginated attacks and malware

User Behavior Risk Insights
Improve Visibility

- Build custom dashboards to track and visualize access activity and improve forensics
- Eliminate the need to review and analyze activity logs and historical data manually
- Generate reports to identify access risk and gain insights into user behavior