Identity Security Platform Overview integrating MFA (Multi-factor Authentication) and SSO (Single Sign On)

Seema Kalwani

seemakalwani@gmail.com,
Independent contributor, IL, USA

Abstract
CyberArk Identity Security Platform provides a one shop integration of multiple features layering different functionalities allowing for consumers to access different avenue from a single user-friendly, look-a-like interface. The platform is allowing for building a secure environment where in the tool learns and adapts limiting access to resources functioning with zero trust. The underlying pieces of the platform are its ability to connect to multiple directory services, allow for validating identity by using multi-factor authentication, manage a complete identity life cycle and incorporate Single sogn-on.

Keywords: PAM, CyberArk, Identity Security Platform, MFA, SSO, SaaS

I. Introduction to Identity Security Platform

Identity Security Platform (ISP) is a full-fledged solution for enterprises and organizations to implement security in their environment quickly and hassle free. In this article we are discussing approach and importance, benefits and exploring the identity interface elements.

(1) Approach and importance of identity security platform

(2) Benefits of CyberArk security identity platform shared services

(3) Identify the user interface elements of identity platform

II. Approach and Importance of Identity Security Platform

A. *Lifecycle*

Identity security secures the identity throughout the cycle of accessing critical assets.

1) It authenticates the identity accurately

2) authorizing the identity with proper permissions and providing access to the privileged access in a structured manner

3) It makes sure entire authentication and authorization process is monitored and audited.

B. *Who are the users*

Identity Security Platform is used by the IT Administrators, developers, cloud engineers, workforce employees, third-party users, customers or any non-human identity. Users can access the platform in a secure manner across any type of application or system (on-prem or in the cloud) from anywhere and using any _device.

C. *Shared Services*

The identity security platform is a cloud native SaaS shared services solution for customers running the CyberArk software as a service, on-premises or in their own cloud.

D. Examine CyberArk Identity Security Approach

Previously workplaces were limited to office, apps and data were in the data center. One could use firewalls and VPNs to keep access secure. Today apps and workers are everywhere, and types of identities are exploding. There are 4 capabilities that form the backbone of the CyberArk identity platform

1) Directory Services
2) Multi-factor Authentication (MFA)
3) Identity Lifecycle Management
4) Single Sign-On (SSO).

All these capabilities are tied together with a layer of artificial intelligence (AI) and Machine Learning (ML) using the User Behavior Analytics (UBA) Service. These not only provide risk-aware access but also provide in-sight into security incidents.

E. Zero Trust

Zero Trust is a security framework that authenticates and continually validates the user's identity irrespective of where and which device they access the organization's environment and assets. Identities zero trust model is the most secure way to power next generation access. Let's see how it happens

1) Verify the user – The user verification is done with increasing certainty starting with a password and increasing with MFA.

2) Validate their device – What is known about the device they are accessing from? Is it a normal PC? Are they at a public computer? What is the current security posture? Based on the knowing more correct risk tradeoff can be made.

3) Limit access and privilege – After verifying the user and validating their device we must limit access and privilege. This ensures the user has the right to perform the task at hand but limits unnecessary access thereby constraining dangerous lateral movement inside the network or between endpoints. The concept or least privilege has been around a long time and is critical part of Zero Trust Security.

4) Learn and adapt – Lastly the system must learn and adapt. Modern machine learning can now be applied to dynamically react to our rapidly changing environment resulting in controls that both reduce overall risk while at the same time increasing the user experience. Appropriate controls applied for the appropriate amount of risk using User Behavior Analytics.

F. Advantages of Zero Trust Security Model

The major drivers for customers adopting the Identity Security Platform are to

1) Defend against attacks by providing a consistent Zero Trust Security Model for all access within a unified access control engine.

2) The Identity Security Platform also helps to enable the digital business by being able to deploy new appliances and services more quickly knowing that access is secured for all identities.

3) Business can also optimize lower total cost of ownership and streamlined procurement of security tools.

4) Also helps by simplifying administration and deployment for faster time to value.

5) The Identity Security Platform and the shared services (ISPSS) also provide a unified experience of administering the different CyberArk solutions to provide a fluid and seamless deployment.

6) ISPSS will help to meet audit and compliance with unified auditing and reporting across CyberArk Services.

7) Customers can choose to use CyberArk Identity Security platform as their Identity Provider (IdP) or integrate with their existing IdP

III. Benefits of identity platform shared services

A. *Shared Services*

The Identity Security Platform shared service is a cloud native SaaS solution for customers running CyberArk's software as a service on premises or in their own cloud. Shared services include:

1) A unified identity management, authentication and authorization layer enabling organizations to scale the protection of identities with a seamless administrator experience

2) AI powered identity security analytics uniting user behavior and privilege threat analytics to enable customers to detect, respond to potential security incidents more quickly

3) An integrated identity agent to provide robust zero trust controls on end-points with strong identity assurance via adaptive multi-factor authentication (MFA), least privilege and session protection.

4) API and standards first design enabling easy integration of third-party applications into the CyberArk Identity Security Platform.

B. *SSO and MFA*

SSO and MFA are two built-in features designed to enforce secure access to a variety of applications used within your organization. Single-sign-on is an authentication method where users can login to multiple applications from different devices using a single set of credentials. It works best on a concept of trust relationship between applications known as service providers and identity providers. Users' identity attributes are shared across these trusted systems, so when user's login to the platform they are automatically granted access to all apps they are provisioned for. As a result, the authentication process is significantly simplified.

C. *MFA*

MFA is an authentication method that uses two or more distinct mechanisms to validate a user's identity rather than relying on a simple username and password combination. The different mechanisms can be code, SMS message, answers to personal security questions, fingerprint, voice or facial recognition and others. Latest MFA solutions at CyberArk also supports adaptive authentication methods using contextual information and business roles to determine which authentication method to apply to a particular user in a particular situation. CyberArk MFA is an excellent tool that prevents unauthorized access to applications and sensitive data helping organizations prevent against identity theft, cyberattack and data breaches.

- MFA is an authentication method
- Requires the user to provide two or more verification factors to access.
- Is a core component of a strong identity and access management (IAM) policy.
- Requires one or more additional verification factors

D. *Authentication Profiles and Rules*

1) Authentication Profile – The application can specify which authentication mechanisms or factors users must provide to access the service.

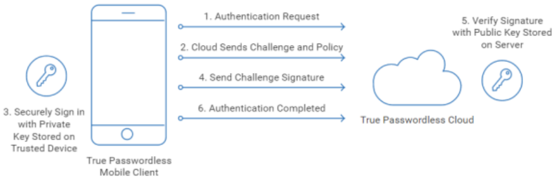
2) Authentication rule – If and when MFA is required or not. Example – Application can create a rule to require that user provide a password and text message confirmation code if they are coming from an IP address that is outside of organization's corporate range. To specify this requirement, application needs to create a rule and associate it with an authentication profile.

IV. Password less Authentication

1) A person can login to a computer system or an online service without being required to enter a password or knowledgebase secret.

2) Modern methods describe a true password less authentication involve a cryptographic key pair to authenticate a user. Example - With password less authentication, a person uses their smartphone, hardware

token or computer instead of a password to access local and online services. In either case, their personal device is used with public-key cryptography (PKC) to enable secure authentication to the system. Most password less login methods combine some form of multi-factor authentication (MFA) into the system.


1. Authentication Request
2. Cloud Sends Challenge and Policy
4. Send Challenge Signature
6. Authentication Completed
5. Verify Signature with Public Key Stored on Server
3. Securely Sign in with Private Key Stored on Trusted Device
True Passwordless Mobile Client
True Passwordless Cloud

A. *FIDO2 Authenticators (MFA)*

FIDO1 is an authentication standard hosted by FIDO Alliance. This standard includes the web authentication (WebAuthn) API, which is a specification written by the World Wide Web Consortium (W3C) and FIDO, with participation from additional third parties. The WebAuthn API is backward compatible with Universal 2nd factor (U2F) keys. How it works?
1) CyberArk leverages the WebAuthn API to enable password less authentication to the CyberArk Identity using either external or on-device authenticators.

2) Supported multi-factor FIDO2 authenticators are something you are. Popular examples are biometric authenticators integrated into device hardware, such as Mac Touch ID, Windows Hello and fingerprint scanners.

3) FIDO2 authenticators are either on-device or external security keys that provide password less authentication.

B. *SSO Variations*

Secure Single Sign-on (SSO) combines several different login screens into one. With SSO the user must enter their login credentials only once on a single page to access all the applications.

1) Uses – SSO is often used in a business context, when user applications are assigned and managed by an internal IT team. Remote workers who use various applications also benefit from using SSO. SSO is an important aspect of many Identities and Access Management (IAM) or access control solutions. User identity verification is crucial for knowing which permissions each user should have.

2) Example – Imagine if students who had already been allowed at the main gate of the college by verifying their identity cards were asked to show their identification card to enter each room inside the college. Some students would quickly become frustrated with the continual checks and might even attempt to circumvent these measures in absurd ways. Ideally, identity checks should be performed only once at the main gate. This is somewhat like an SSO system instead of establishing their identity over and over, users establish their identity once and can then access several different services or applications.

3) Smart cards contain cryptographic credentials that allow users to authenticate without usernames and passwords. However, physical cards require a dedicated reader and attempting to use smart cards with mobile devices is a real challenge. With derived credentials, the cryptographic credential is stored securely on a mobile device, in compliance with current smart card regulations. This means no need for a dedicated reader for mobile devices and much more flexibility for users. Our derived credential solution allows mobile authentication. This new capability extends CyberArk Identity's integration of identity-based security to mobility, offering SSO in even the most highly regulated environments. Derived credentials can be configured for a) Simple certificate enrollment protocol (SCEP) with Microsoft's network device enrollment service (NDES) b) Windows enterprise certificate authority c) Custom CA – CSR is provided, and client can work with CA of their choice to get the certificate.

V. Identity Lifecycle Management

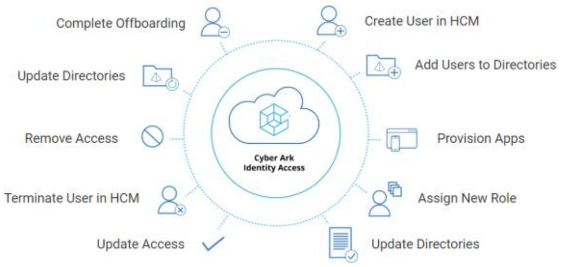
Identity lifecycle management facilitates automation of

1) User access provisioning

2) Approval workflows

3) Access governance.

It enabled dynamic provisioning and revoking of access to pre-integrated cloud applications. It allows users to request access and define approval workflows. It also enables auditing of accounts, entitlements and devices by drilling down to the user role or application level.



A. *Dynamic access*

Automatically grant and revoke access to hundreds of pre-integrated cloud applications from CyberArk App catalog.

B. *Policy based provisioning*

Use roles-based access control (RBAC) to automatically provision the right level of access and permission to your users.

C. *Centralized management*

Control user access entitlements within aps by mapping roles to the appropriate user groups.

D. *Custom App integration*

Extend provisioning workflows to custom applications using SCIM (System for cross-domain identity management) protocol.

***Conclusion*: CyberArk Identity Security Platform is providing a robust solution encompassing connectivity to various applications in-built, out-of-the-box, cloud, on-prem, code the custom applications and much more in a secure way. The biggest advantage is the connectivity with other products in the organization and letting them ingest PAM data is made easier via RESTAPI calls. In tight networks like banks, credit card companies the implementation might take long due to security and firewall hardening in the environment. A first glance at CyberArk's offerings, various modules and deployment might be overwhelming yet prospects of integration and customization are huge.**

References

[1] CyberArk, “Benefits of CyberArk Solution and how to use it”, https://training,.cyberark.com/pages/108/privilege-cloud-administrator (accessed November 21 2024)
[2] CyberArk, “Breaking down the bussiness benefits and cost savings of CyberArk Privileged Access Management as a service”, https://www.cyberarlk.com/resources/blog/breaking-down-the-bussiness-benefits-and-cost-savings-of-cyberark-privileged-access-management-as-a-service (accessed November 21 2024)
[3] CyberArk, “Unified identity security platform”, https://www.cyberark.com/products/ (accessed November 21 2024)

[4] One identity, “What is Unified Identity Security Platform”, https://www.oneidentity.com/what-is-a-unified-identity-security-platform/ (accessed December 10 2024)

[5] Sailpoint, “What is identity security?”, https://www.sailpoint.com/identity-library/what-is-identity-security (accessed December 10 2024)