CYBERARK®
The Identity Security Company

Six Ways to Place Secure Access at the Heart of Your Key Initiatives

Unraveling the Connection Between Transformation and Threat

Fifty-eight percent of security decision-makers believe they will suffer an identity-related compromise linked to digital transformation, with nearly all (99%) agreeing that this type of security incident is inevitable in the year ahead, according to the CyberArk 2023 Identity Security Threat Landscape Report.

As businesses launch transformational initiatives such as cloud migrations, they amass a vast trail of digital identities used by their workforce and external partners to access business-critical applications required to do their jobs. Each of these identities can be privileged under specific circumstances, making them the gateway for attackers to breach an organization's network and wreak havoc.

Organizations use 75 SaaS applications on average and believe this number will increase by 68%.[2]

Adopting a Security-first Mindset to Safeguard Growing Identities

While it's impossible to contain the surge of identities that are expected to grow by 2.4x this year[1], it's imperative for enterprises to implement an integrated identity security strategy that offers stronger protection against modern attack methods like multi-factor authentication (MFA) fatigue attack and session hijacking via cookie theft.

Six Best Practices for Securing Access for Users Driving Digital Initiatives

1 | **Combat Credential Compromise with Intelligent Single Sign-on (SSO):** Build upon traditional SSO tools' design with user behavior analytics capabilities that apply context and block risky access attempts in the event of suspicious user activities.

2 | **Balance Protection and Productivity with Adaptive Multi-factor Authentication (MFA):** Unlike regular MFA tools, adaptive MFA leverages users' history of login behavior and applies context to discern typical activities from risky ones. It then uses insights to take automated actions like offering easy authentication for legitimate users (e.g., QR codes) and more difficult factors in the event of suspicious access attempts (e.g., number-matching challenges).

3 | **Enable Enterprise-grade Password Protection:** For applications that do not support SSO or modern identity protocols, applying intelligent privilege controls to everyday users' passwords can give IT security teams the much-needed controls and visibility that traditional password managers typically don't provide. Here are few examples:

- Storing passwords in secure, encrypted vaults
- Controlling who can share, view or edit passwords
- Simplifying auditing with in-depth reporting on employees' app usage

[1,2] CyberArk, "2023 Identity Security Threat Landscape Report," June 2023

4 | **Secure Users' High-Risk Web Sessions:** With 52% of workforce users having access to sensitive data[3] – and often the ability to take risky actions, it's important to extend controls traditionally reserved for IT users to employees' web sessions. This includes:

- Capturing in-app activities via step-by-step recording with a clear audit trail.
- Identifying when a session is left unattended and requiring reauthentication.
- Preventing employees from taking risky actions like downloading sensitive data.

5 | **Automate Identity Management to Reduce IT Security Burden:** 68% of IT security decision-makers say workforce churn will create security issues and 74% are concerned about confidential information loss from users such as ex-employees[4]. Organizations can reduce the burden on their IT security teams and eliminate risks stemming from manual processes with an automation-driven identity management approach, ensuring:

- Manual, complex tasks are automated.
- Employees' onboarding and offboarding is secure.
- Just-in-time access is applied to apps and resources based on users' roles.

6 | **Seamlessly Safeguard Business-to-business (B2B) Identities:** Like employees, external users have access to sensitive data and often serve as entry points for threat actors. This includes vendors, partners and clients who access enterprise applications. Organizations can combine SSO and adaptive MFA to enable a secure and user-friendly experience, while applying centralized identity administration, automated workflows, and overall, a security-first approach to identity management.

84%

of IT security decision-makers believe outsourcing to vendors and suppliers increases security risks/attacks.[5]

Scaling Scare-free with an Integrated Identity Security Strategy

At a time when cloud migration, product digitization and SaaS deployment are top priorities among global enterprises, there's no doubt digital identities will continue proliferating, making the already porous attack surface even more vulnerable. However, by placing identity security at the core of digital initiatives – offering seamless and secure access to workforce and external B2B identities – organizations can protect everything their internal and external users are working so hard to build.

LEARN MORE

Read our whitepaper, Secure Access for the Identities Driving Your Key Initiatives, for an in-depth look at the six best practices in this piece.

If you'd like to speak with a CyberArk team member about your organization's security needs, please contact us here

[3] CyberArk, "2022 Identity Security Threat Landscape Report," April 2022

[4,5] CyberArk, "2023 Identity Security Threat Landscape Report," June 2023

CYBERARK®
The Identity Security Company