CYBERARK®
The Identity Security Company™

DATA SHEET

CyberArk Vendor PAM

Third-Party Privileged Access: Seamless. Efficient. Secure.

The Challenge

Modern enterprises engage numerous external third parties, such as vendors, consultants, business partners, system integrators, and maintenance service providers for essential business functions. To successfully carry out their tasks, third-party users often require privileged access to IT infrastructure, internal and web-based applications with sensitive data, operational technology (OT), and industrial control systems (ICS).

In many cases, however, organizations struggle to properly secure and provision access for their vendors and contractors.

Enterprises must, therefore, defend against attacks targeting third parties, while enabling them to provide the required services. Conventional approaches to achieving this goal include treating third-party identities like employees' and stitching together disparate agent and password-based products to protect external access. Such approaches are inefficient in terms of both the effort and time required to provision access. For example:

> Consequently, a third-party breach becomes a stepping stone for attackers targeting the harder-to-get-into enterprises. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.[1]

- **Processes and tools designed to authenticate company employees and corporate devices aren't well suited for third-party users, particularly those requiring short-term access.** Providing corporate workstations to every external user is not feasible. Adding external parties to the corporate directory can be costly and slow, as it takes days or weeks, to properly provision and de-provision access. Meanwhile, introducing new machines or identities in the directory also increases the attack surface.
- **Deploying VPN clients on third-party laptops adds IT management overhead and holds back access provisioning.** Bolting token-based multi-factor authentication (MFA) on top of VPN exacerbates these issues. Identity management schemes based on user IDs and passwords are impractical in the context of frequently changing third-party personnel and access requirements. VPN and passwords also introduce security flaws like overprovisioning standing access with VPN and increasing risk of credential theft with passwords.

With growing reliance on remote working and outsourced operations, IT and security teams alike must find innovative ways to grant external parties secure access to critical systems without disrupting operations.

[1] Source: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

The Solution

CyberArk Vendor PAM is a SOC 2 type 2 compliant and **SOC 3 certified** service that helps organizations defend against attacks targeting third-party access, while driving operational efficiencies and satisfying audit and compliance requirements. With this comprehensive, SaaS-based solution for third-party remote access, you can achieve the following:

- Enable third-party user productivity, while protecting critical systems and assets.
- Ensure third-party remote access' inherent security and alignment with Zero Trust and least privilege principles.
- Reduce the burden on IT related to secure remote access provisioning, maintenance, and deprovisioning.
- Gain full visibility and record user activity to streamline compliance pertaining to third-party access.

Vendor PAM eliminates the need for legacy approaches to securing third-party access, such as VPN clients, passwords, and agents that can add risk, create administrative complexity, and frustrate end-users. The solution combines Zero Trust access, biometric MFA, just-in-time provisioning, and privileged credential and session management for security, visibility, and audit compliance. With Vendor PAM, authorized third parties can quickly authenticate using their existing smartphones' facial or fingerprint recognition and are provisioned just-in-time, least-privileged access to sensitive enterprise resources and web applications managed by CyberArk Privileged Access Manager (CyberArk PAM).

Vendor PAM's Offline Access capability provides authorized users the ability to securely obtain credentials during network or power outages, in air-gapped environments, and other situations in which they can't reach CyberArk PAM. Access credentials are securely stored on an authorized third-party's smartphone, so the user can get a hold of them immediately after completing biometric authentication, with credential usage recorded for audit and compliance purposes.

29%

of all breaches in 2023 were attributable to a third-party attack vector.[2]

98%

of organizations utilize a thirdparty that has experienced a breach.[3]

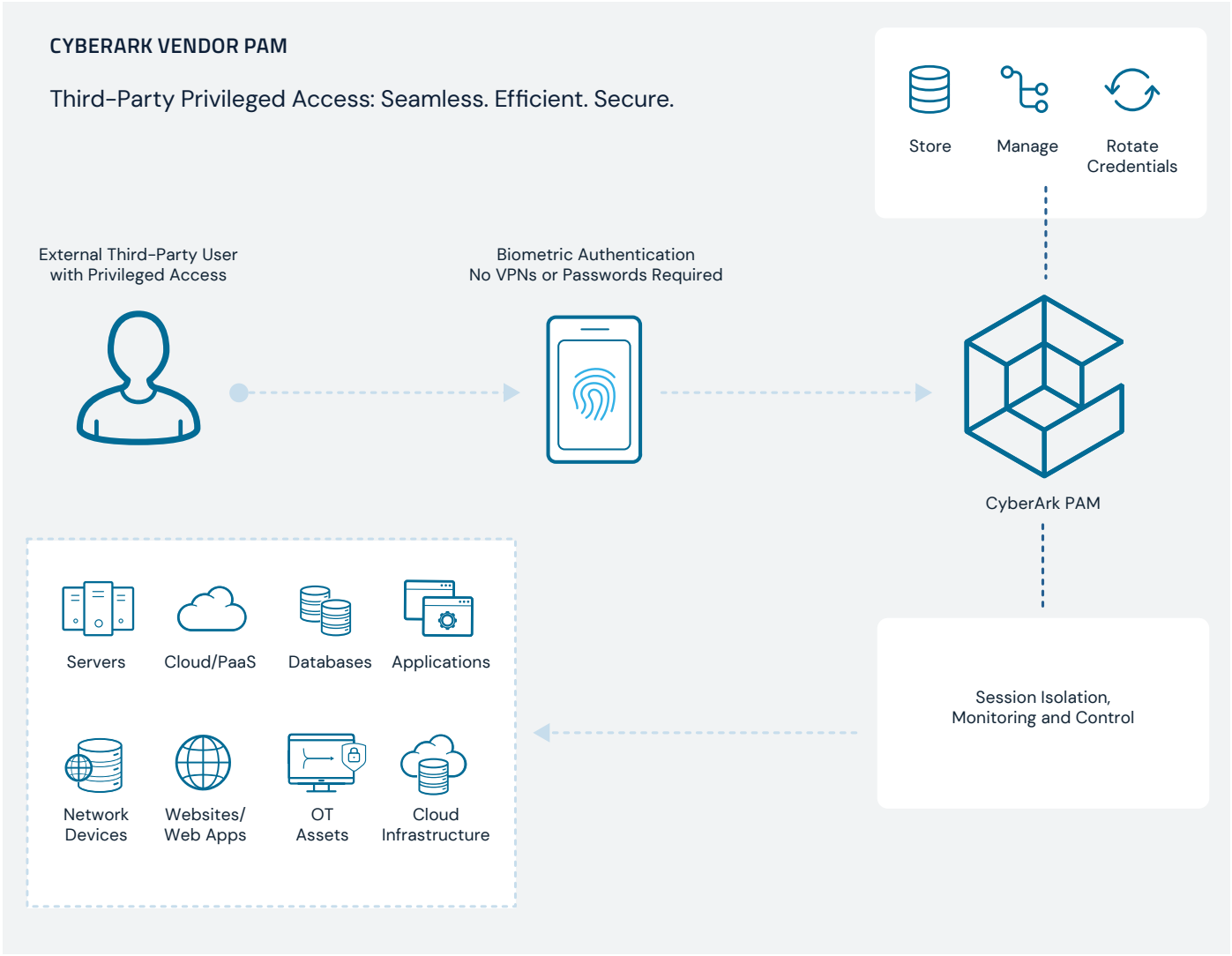
91%

of organizations are concerned about third-party risks.[4]

How It Works

When an authorized external third party attempts to log on to the CyberArk PAM's web portal, a one-time, ephemeral QR code is generated and displayed on their workstation. Utilizing the CyberArk Mobile app, the user scans the QR code and simultaneously verifies their identity via facial or fingerprint recognition. Once access has been granted, the third party enters the CyberArk web portal via an isolated, end-to-end encrypted, and monitored web-browser session. Credentials are never shared with the end user's workstation or visible to the end user during privileged sessions.

[2,3] CyberArk, "2024 SecurityScorecard Global Third-Party Cybersecurity Breach Report".
[4] CyberArk, "2024 CyberArk Threat Landscape Report".



Vendor PAM helps you mitigate risks by efficiently managing privileged account access rights and proactively monitoring and controlling privileged account activity. With Vendor PAM's REST APIs, your team can automatically provision and manage users, perform bulk actions like inviting multiple vendors at once or deactivating users automatically, and easily access data for audit and compliance reporting. Taking advantage of CyberArk PAM's core capabilities, your analysts can swiftly identify suspicious actions and respond to threats coming from 3rd parties.

Benefits

- Defend against attacks by reducing the risk of privileged account compromise:
    - Leverage Vendor PAM in tandem with CyberArk PAM to securely authenticate external access, reduce risk of credential theft, isolate privileged sessions to prevent the spread of malware, and monitor them to swiftly detect and stop misuse.
    - Implement just-in-time, least privilege access and utilize biometric authentication to validate identities in accordance with a Zero Trust security model.
    - Automatically deprovision access once it is no longer needed.
- Drive operational efficiencies by leveraging existing CyberArk PAM infrastructure and automating access-related IT workflows. Avoid the complexity and cost of shipping corporate devices, provisioning and deprovisioning directory accounts, managing passwords, and installing agents and VPN clients.
- Enable the digital business by rapidly onboarding and simplifying access for authorized third parties. Onboard a new user in less than 2 minutes and make authentication as easy as taking a biometric reading on the user's existing smartphone.
- Satisfy audit and compliance requirements, as mandated by FIPS 200, HIPAA, PCI DSS, NERC CIP, CFATS, and other regulations, by, recording, and monitoring privileged access sessions in real time, while creating a comprehensive audit trail.

About CyberArk
CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®