PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
DO ESTADO DO AMAZONAS

Erika Soares Rodrigues <erika.rodrigues@tjam.jus.br>

Pregão Eletrônico N° 90040/2024 (SRP) - Solução PAM - Genos Tecnologia

1 mensagem

Nilton Pereira | Genos Tecnologia <nilton@genostecnologia.com.br> 4 de setembro de 2024 às 16:58
Para: "colic@tjam.jus.br" <colic@tjam.jus.br>

Boa tarde,

Pregoeiro,

Tudo bem?

Segue documentos (datasheet) do fabricante Cyberark,

Att,

2 anexos

vendor-pam-datasheet.pdf
422K

epm-for-linux-ds-en.pdf
337K

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. In fact, 41% of organizations surveyed by CyberArk work with over 100 third parties each. 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. Consequently, a third-party breach becomes a stepping stone for attackers targeting the harder-to-get-into enterprises. For example, 15% of the data breaches under investigation by the U.S. Department of Health and Human Services as of February 2022 involved "Business Associates" who had access to protected health information (PHI). According to SANS 2021 Survey: OT/ICS Cybersecurity, external remote services are the most frequent attack vector in OT incidents. So, it comes as no surprise that 77% of security leaders surveyed by CyberArk viewed third-party risk as a top 10 security concern.

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:

- **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.

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.

96% of organizations allow third parties to access critical systems.

86% of organizations cited that onboarding third party vendors takes more than 1 business day.

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).

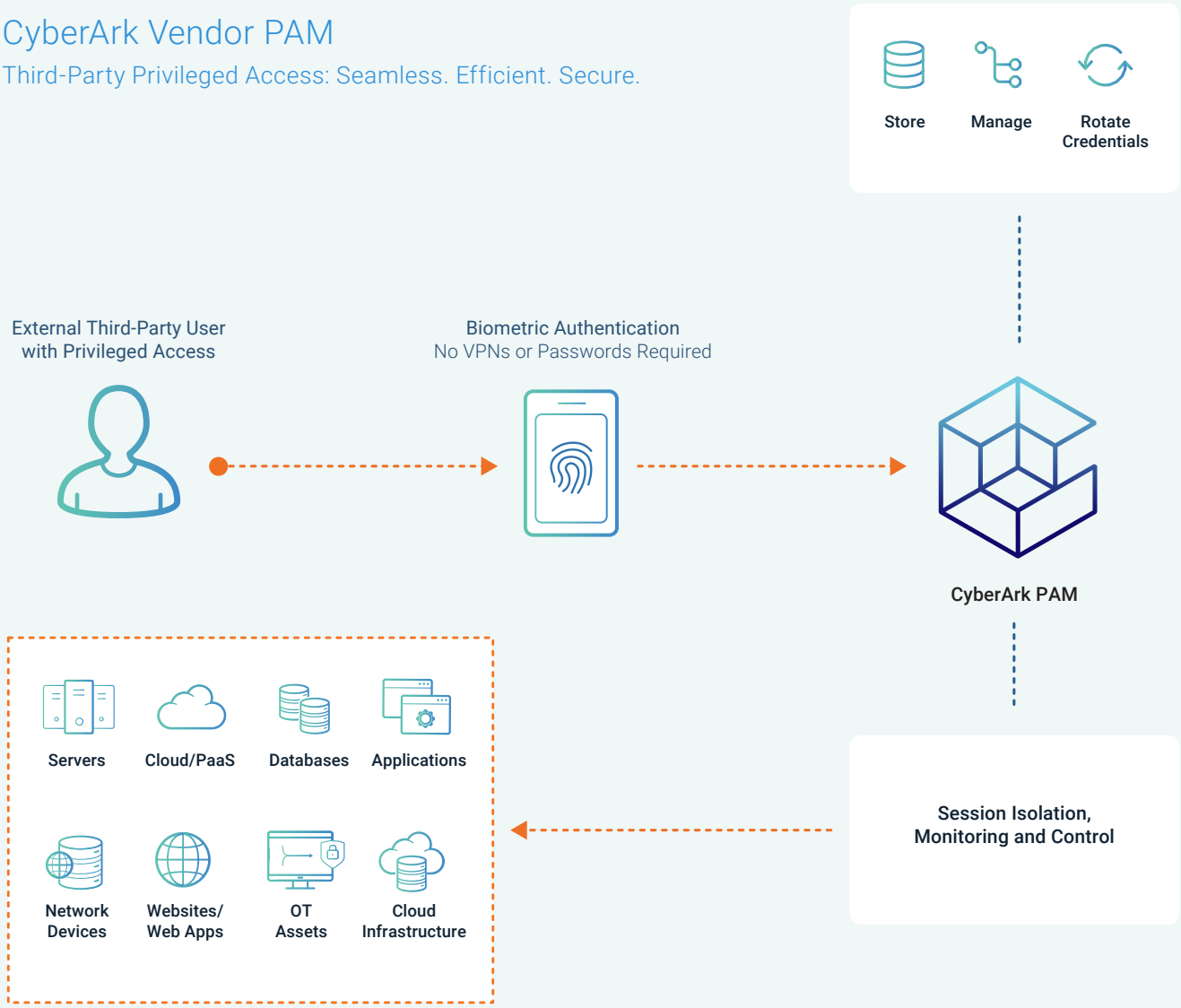
Vendor PAM's Offline Access capability provides authorized users the ability to securely obtain credentials during network or power outages, in air-gapped environments, and other situations in which they can't reach CyberArk PAM. Access credentials are securely stored on an authorized third-party's smartphone,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

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.

CyberArk Vendor PAM

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



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 isolating, 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 privileged access management, 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®
The Identity Security Company

CYBERARK®

DATA SHEET

CyberArk Endpoint Privilege Manager for Linux

The Challenge

Linux is ubiquitous — modern IT implementations, applications and DevOps pipelines are predominately Linux based. In fact, 43% of the top 1 million websites are powered by Linux, compared to just 23% for Windows.[1] Linux systems run business-critical applications and contain confidential data, and are a high-reward target for threat actors. Adversaries are increasingly setting their sights on Linux-powered assets, using privileged Linux accounts as means to get to them.

Many organizations allow users to work as superusers (using "su" or even working under root). IT administrators, application developers, database administrators and others have permanent superuser privileges. Threat actors routinely abuse privileged or over-privileged Linux accounts to launch attacks and exfiltrate data.

Linux offers a native way of reducing the risks associated with privileged accounts by enforcing least privilege. The Linux "sudo" command gives administrators and other entitled users the minimum set of privileges they need to perform their jobs. sudo is short for 'superuser do', as in a sudo user can do what a superuser can do. It lets you temporarily elevate a user to run specific commands without logging in as root.

In short, Linux's sudo:

- Provides native least privilege capabilities
- Is often overprivileged
- Is difficult to manage at scale
- Can be circumvented
- Lacks central reporting necessary for audits
- Stores logs locally, subject to tampering

sudo is a powerful tool. But configuring sudo access control lists (ACLs), particularly on a large scale, is no easy matter. sudo configuration files (sudoers) are notoriously long and complex, and frequently misconfigured. Threat actors can take advantage of configuration mistakes to gain privileged access.

HIGHLIGHTS

- Enforce least privilege and implement foundational security controls across Linux servers and workstations — at scale and with a native user experience
- Tightly control the commands and tasks each Linux user is permitted to execute based on role
- Strengthen security with advanced controls, such as enforcing policies on commands within scripts or restricted shells
- Centralize and unify privilege management for Windows, macOS and Linux endpoints across the enterprise
- Avoid manually intensive and error-prone administrative processes, and free up staff to focus on other tasks
- Simplify audits, improve compliance with government and industry regulations, and demonstrate cyber readiness for insurance underwriters
- Accelerate time to value with a SaaS solution that delivers cloud agility, economics and ease-of-operations

[1] World Wide Web Technology Surveys, February 2022

Moreover, most Linux distributions provide no native capabilities for provisioning, administering or auditing sudo configurations across systems. Many organizations usually rely on manual processes to manage privileges across Linux endpoints — a time-consuming, error-prone approach that squanders resources and is difficult to scale.

In addition, sudo provides no centralized event reporting capabilities to assist with compliance audits or security investigations. Events are logged locally on each machine. It is difficult for IT and security professionals to aggregate and correlate events across systems to isolate security incidents or examine compliance-related activity. In addition, system log files can be accidentally modified or intentionally tampered with by users with elevated privileges. Finally, there's no ability to enforce policy within restricted shells or scripts.

The Solution

CyberArk Endpoint Privilege Manager™ for Linux provides foundational endpoint security controls and is designed to enforce the principle of least privilege for Linux servers and workstations. The solution eliminates manually intensive, error-prone sudo administrative processes, allowing endpoint security managers to centrally configure sudo and enforce least privilege across Linux systems, at scale, based on policy.

CyberArk Endpoint Privilege Manager for Linux is an integral component of CyberArk Endpoint Privilege Manager — a comprehensive endpoint security solution that provides single pane-of-glass administration and centralized, policy-based privilege management for Windows, macOS and Linux endpoints.[2] With Endpoint Privilege Manager, security professionals can centrally manage geographically dispersed, heterogenous endpoints in a consistent manner from a single SaaS console.

Endpoint Privilege Manager can provide visibility and control over all enterprise endpoints, including remote endpoints that infrequently connect to the corporate network. A flexible reporting engine and detailed event journal make it easy to provide evidence for compliance audits, to support forensics investigations, and to demonstrate cyber readiness and proof of required security controls to insurance underwriters.

Endpoint Privilege Manager REST APIs allow you to tie activity and event auditing into your existing security information and event management (SIEM) platforms. And Endpoint Privilege Manager's policy engine is accessible via API for integration with external policy orchestration and automation tools.

Endpoint Privilege Manager is delivered as a SaaS solution for rapid deployment, simple operation and easy integration with other cloud-based services. A SaaS deployment model helps you accelerate time to value and reduce TCO by avoiding on-premises equipment expenses and operations hassles.

CAPABILITIES

- Simple sudo policy management and enforcement (elevate or block individual specific commands and parameters based on policy)
- Configurable policy audit reports for compliance and forensics (determine when policies were triggered and by whom, and identify corresponding applications and endpoints, actions performed, etc.)
- Sudo with password prompt or passwordless
- Standard sudo command syntax for smooth adoption
- REST APIs for policy automation and external system integration
- Agent CLI for support and status monitoring
- Local logging with multiple verbosity options
- Integral agent downloader and installer
- Upgrade or uninstall agents directly from the EPM console

[2] CyberArk Endpoint Privilege Manager is available for workstations and for servers

CYBERARK®