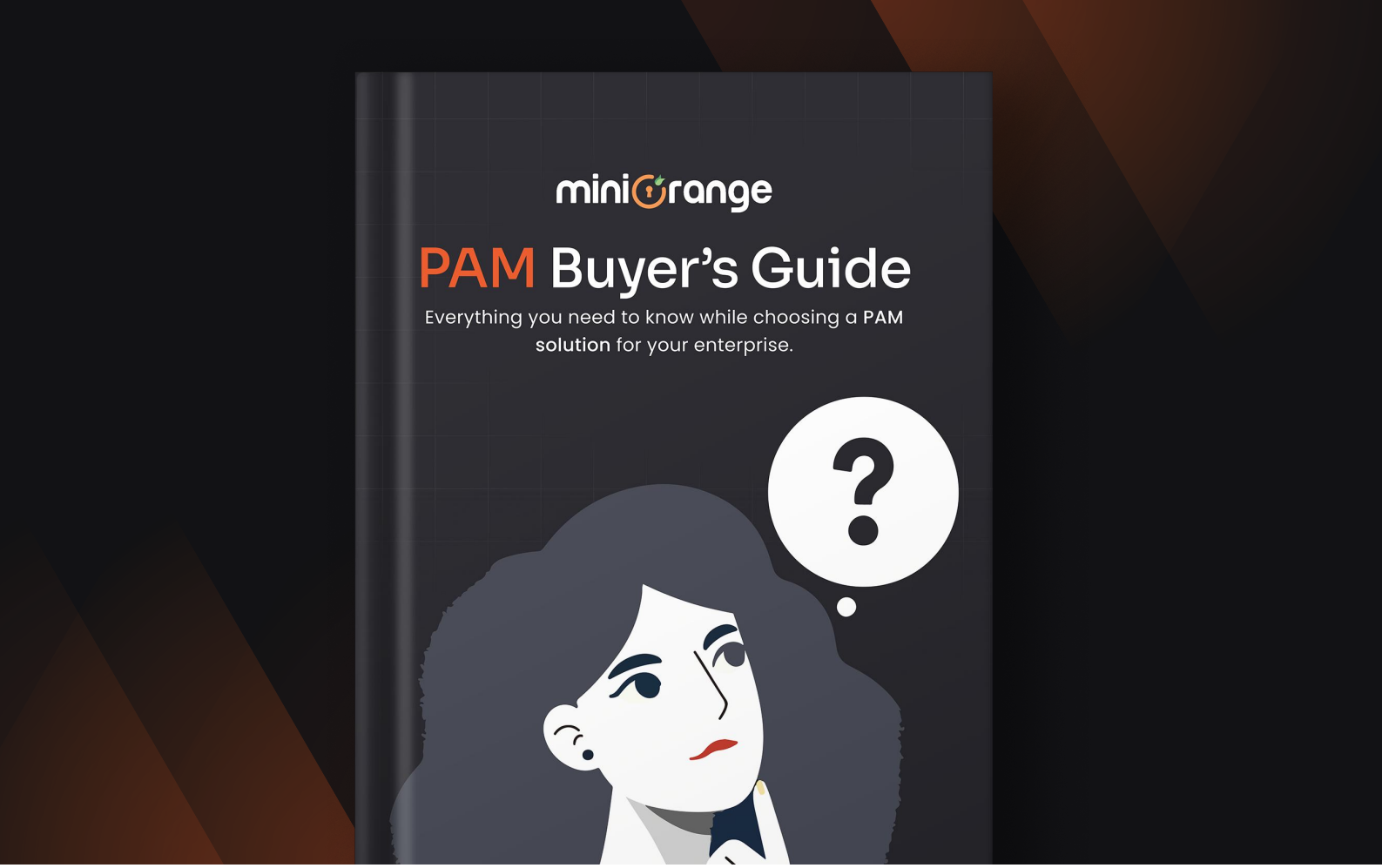


Introduction

In today's cyber landscape, protecting privileged accounts is crucial as they function as superusers or administrators with access to critical systems and data. The miniOrange Privileged Access Management solution offers robust security measures to safeguard these accounts, ensuring the integrity and security of your organization's IT ecosystem.

The Attack Surface Is Rapidly Expanding

Cybercrime is expected to cost $10.5 trillion annually by 2025, a 300% increase from 2015. Despite significant efforts, data breaches continue to rise, with a 20% increase from 2022 to 2023 and twice the number of victims globally in 2023 compared to 2022. Ransomware activity in the Middle East surged by 77% in the same period.

Types and Categories of Modern Privileged Identities

To safeguard against evolving threats and meet compliance demands, miniOrange PAM controls, monitors, and audits privileges and access for various entities, including:

On Premises

- Shared admin accounts
- Service accounts
- Desktops, servers, network devices
- Applications, databases
- Hypervisors, virtual devices
- Machine identities

Cloud Infrastructure

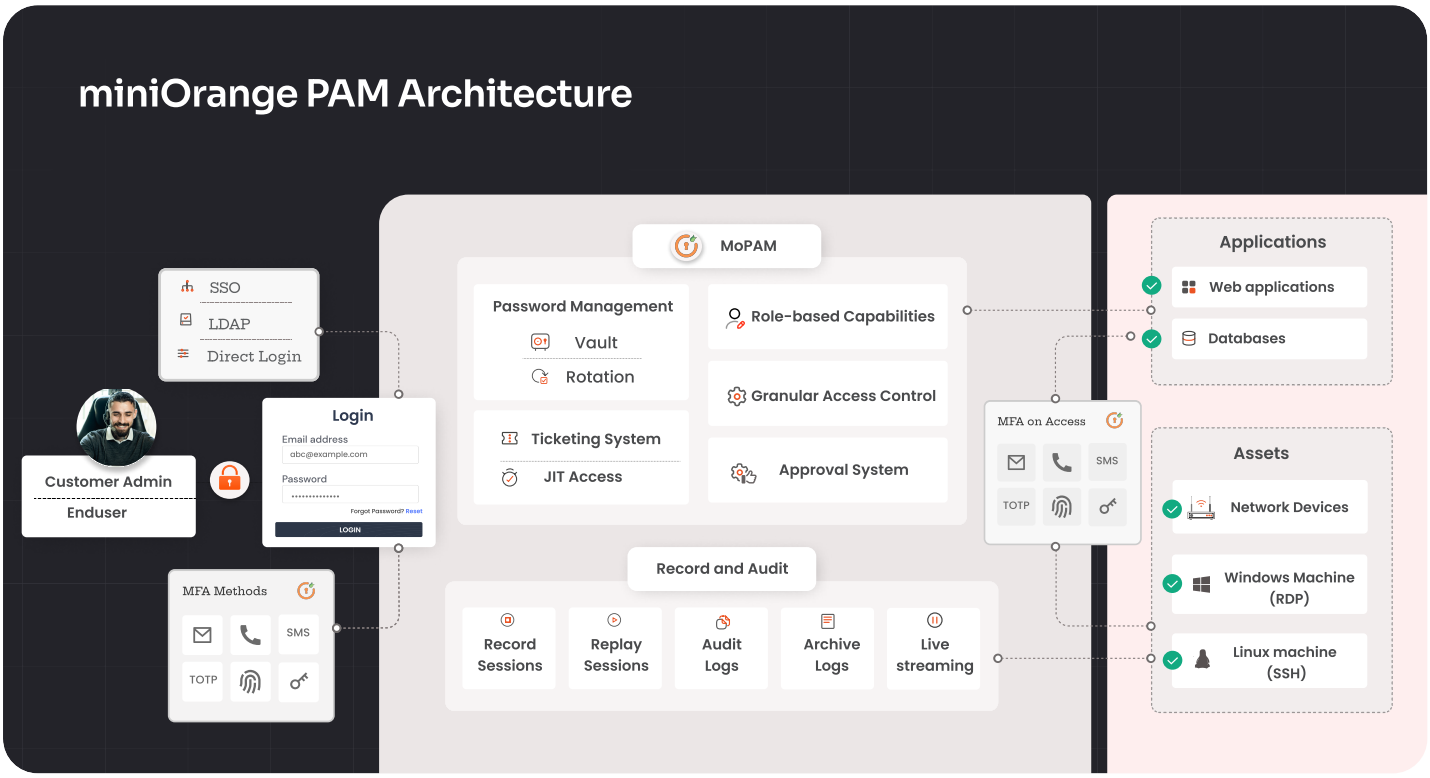
- Cloud management platforms
- SaaS applications
- Cloud-based entitlement

Internet Of Things

- Industrial control systems
- OT and SCADA
- Mobile workstations
- BYOD, printers, sensors, and endpoints

Dev SecOps

- DevSecOps tools
- CI/CD pipelines
- Mobile workstations
- Micro-services, container platforms



About miniOrange

miniOrange is a leading Identity and Access Management (IAM) platform dedicated to securing workforce, partners, and customer identities. We provide cutting-edge cybersecurity solutions trusted by top global brands across diverse industries. With a mission to simplify and strengthen the world's complex identity and security challenges, miniOrange offers robust protection, seamless access control, and unmatched support.

Our comprehensive suite of solutions, including Privileged Access Management, ensures that organizations can manage and secure their digital identities effectively, enhancing productivity and safeguarding critical assets around the clock.

24/7
Customer Support

20,000+
Customer

Competitive
Pricing

Key features of miniOrange PAM

Password Vault and Rotation

The Password Vault and Rotation feature of miniOrange PAM centralizes the management of user accounts by implementing strong passwords and **Multi-Factor Authentication (MFA)**. This ensures that privileged account credentials are regularly **rotated** and securely managed using industry-standard encryption.

Session Monitor & Control

Session Monitor & Control provides real-time visibility through **live session streaming**, allowing prompt responses to threats. It also **records sessions** for compliance and investigations, terminates suspicious activities instantly, and sends **alerts** for unauthorized behavior detection, all accessible via an intuitive dashboard.

Privilege Account and Session Management (PASM)

Privilege Account and Session Management (PASM) acts as a gatekeeper, defining access duration and reasons for administrator access. It facilitates secure access to essential systems and imposes time-based or functionality-based restrictions on each session, ensuring controlled and **monitored** privileged access.

"The password vault and session monitoring capabilities are top-notch. We now have real-time visibility and control over privileged sessions, which is critical for our compliance requirements."

— Security Administrator, Healthcare Organization

Privilege Account and Delegation Management (PEDM)

Privilege Elevation and Delegation Management (PEDM) assigns time-limited access to restricted resources based on user privilege levels. This avoids granting standard users permanent access to sensitive resources, minimizes risks linked to overly privileged users, and ensures security by adhering to the **principle of least privilege.**

Just-In-Time (JIT) Privileged Access

Just-In-Time (JIT) Privileged Access dynamically grants access rights to users for a limited duration, precisely when needed. This minimizes security risks associated with standing privileges, streamlines operations, and restricts the time window for potential misuse of elevated privileges.

Endpoint Privilege Management(EPM)

Endpoint Privilege Management supports **Windows, Mac,** and **Linux,** removing local admin rights to mitigate the risk of security breaches. It enforces the least privilege principle and deploys effective endpoint security controls to protect sensitive data and prevent unauthorized access.

"miniOrange PAM has transformed the way we manage privileged access. The intuitive interface and robust security features have significantly enhanced our security posture."

— Security Administrator, Healthcare Organization

What sets miniOrange PAM apart?

"miniOrange PAM offers robust security features including password vaulting, session monitoring, and real-time threat response, ensuring that privileged accounts are well-protected against unauthorized access and potential breaches.way we manage privileged access. The intuitive interface and robust security features have significantly enhanced our security posture."

- **Boost Security:** Protects against unauthorized access and potential breaches.
- **Compliance:** Ensures compliance with industry standards and regulations.
- **Operational Efficiency:** Streamlines access management and reduces administrative overhead.

Certificate Lifecycle Management

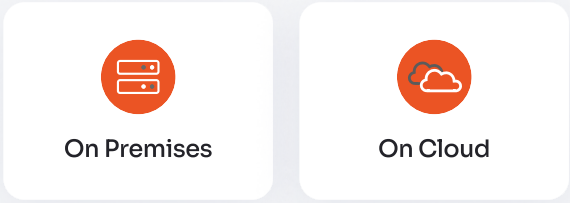
miniOrange PAM includes automatic discovery and onboarding of certificates, encrypted storage and management, automated rotation and renewal, and comprehensive lifecycle management. Detailed logs track all certificate-related activities.

Real-Time Trust Analysis to Ensure Zero Trust Privilege

The PAM solutions provide mechanisms to evaluate access requests based on multiple parameters. Trust scores for users and devices, dynamic access policies, and automated request processing help maintain a zero-trust privilege environment. Comprehensive audit trails provide detailed logs of privileged activities..

Deployment Options

Flexible deployment options include **on-premises** for complete control, **cloud** for scalability and reduced overhead, or a **hybrid** approach combining flexibility and resilience . We offer detailed training sessions for IT staff and administrators, along with **extensive documentation** and resources for self-help.



Get Started with miniOrange PAM

Discover how miniOrange can benefit you. Schedule a free call with our experts today.

Talk to Our Expert | Book a Demo