Defa3
Cyber Security

Protect Your Data with Privileged Access Management (PAM)

Securing Sensitive Access Points Across Your Organization

Privileged accounts are a primary target for cyber attackers. Whether it's internal misuse or external compromise, uncontrolled privileged access creates significant risk. Privileged Access Management (PAM) helps organizations enforce strict access controls, monitor high-risk activities, and reduce the attack surface across users, systems, and applications.

Defa3
Cyber Security

Humans Remain the Weakest Link

Privileged users often have unrestricted access across environments. PAM enforces least-privilege access, ensuring users have only what they need to perform their roles. This minimizes insider threats and limits potential damage from compromised credentials.

Defa3
Cyber Security

Privileges Extend Beyond Humans

Modern IT environments rely heavily on non-human entities like applications, bots, and automated services. These accounts require elevated access and often operate without visibility. PAM discovers, secures, and governs these accounts across cloud, on-premise, and hybrid infrastructure.

Defa3
Cyber Security

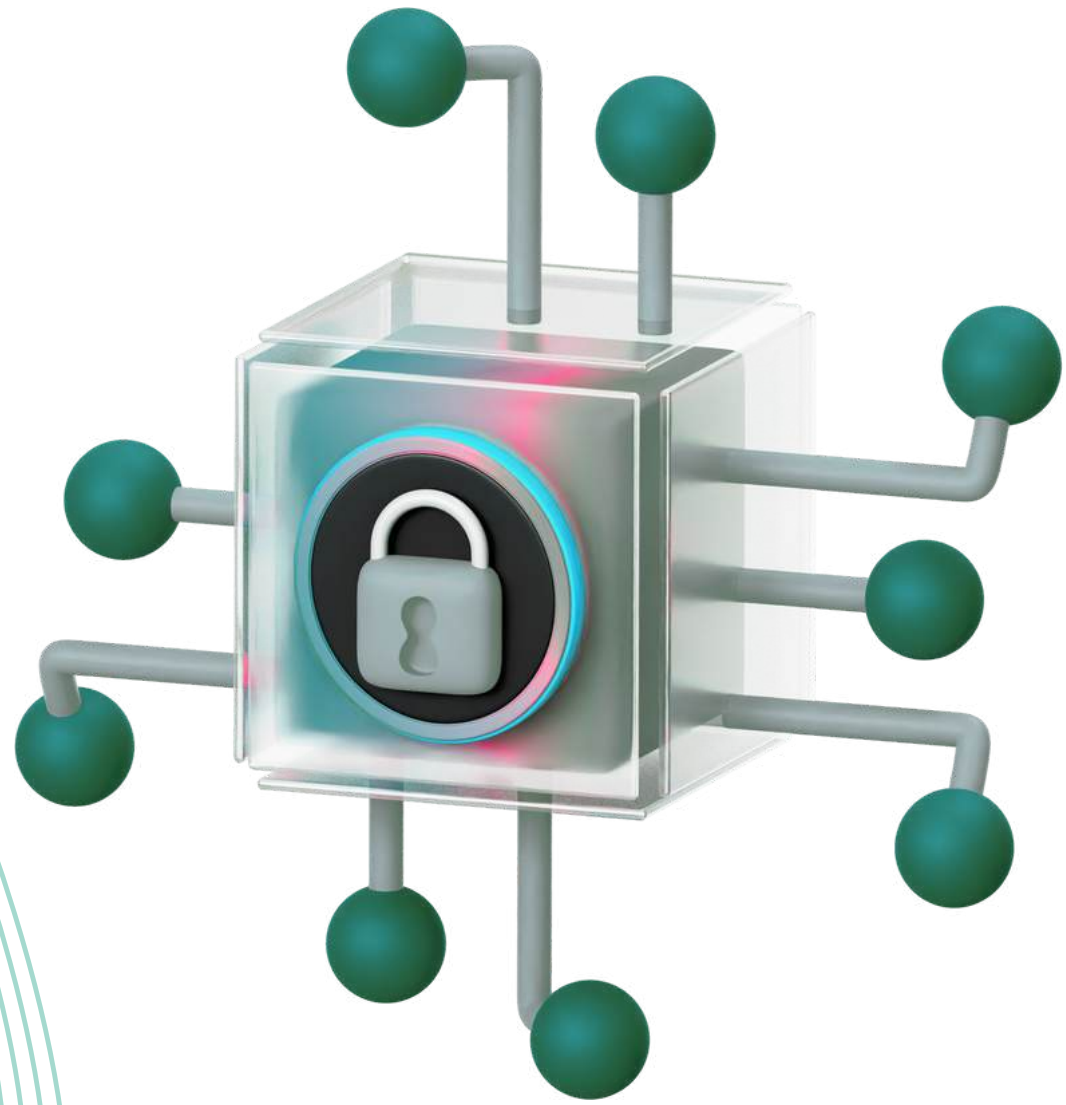
Endpoints Are High-Risk Entry Points

Most endpoints carry local admin privileges by default. These privileges can be exploited by attackers to move laterally, escalate access, and compromise core systems. A robust PAM strategy includes removal of unnecessary local admin rights and applies granular access controls across all endpoints.

Defa3
Cyber Security

Visibility and Real-Time Response

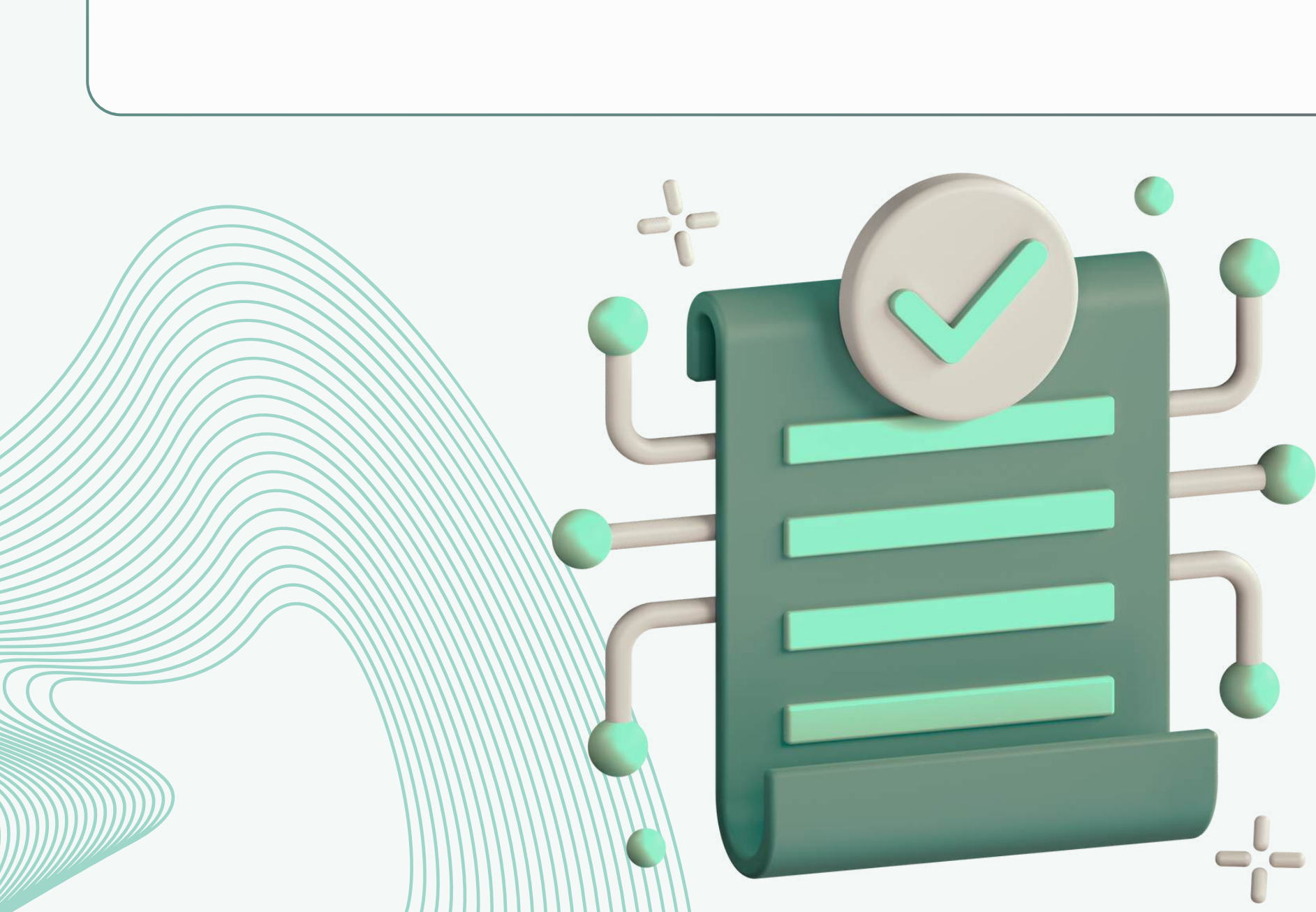
PAM enables security teams to continuously monitor privileged sessions, detect anomalies, and respond to suspicious behavior in real time. This operational visibility is critical for early threat detection and incident response.



Defa3
Cyber Security

Compliance and Audit Readiness

Regulatory standards such as ISO 27001, PCI DSS, and NIST require stringent control over privileged access. PAM provides detailed logs and access records, simplifying audit preparation and ensuring alignment with compliance mandates.



Key Outcomes of a Mature PAM Program

1. Reduced risk of privilege-based attacks
2. Controlled and monitored access across all environments
3. Decreased operational complexity
4. Improved compliance posture
5. Enhanced visibility across users and systems

Defa3
Cyber Security

www.defa3.com +971454706666 sales@defa3.com

Found this useful? Follow us!