IdentityShield

ELEVATE SECURITY WITH CUTTING-EDGE PRIVILEGED ACCESS MANAGEMENT

PRESENTED BY

Pradeep Kumar

ABOUT ME

- 5 Years of Experience in the Security Domain
- IAM and PAM Expert
- Learning Musical Beats of Cyber Security Everyday

AGENDA

1 What is a Privileged Account

2 The Risk Associated with Privileged Account

3 What is PAM

4 Important Features

5 Integrations

6 Architecture and Demo

7 So why PAM

WHAT IS A PRIVILEGED ACCOUNT?

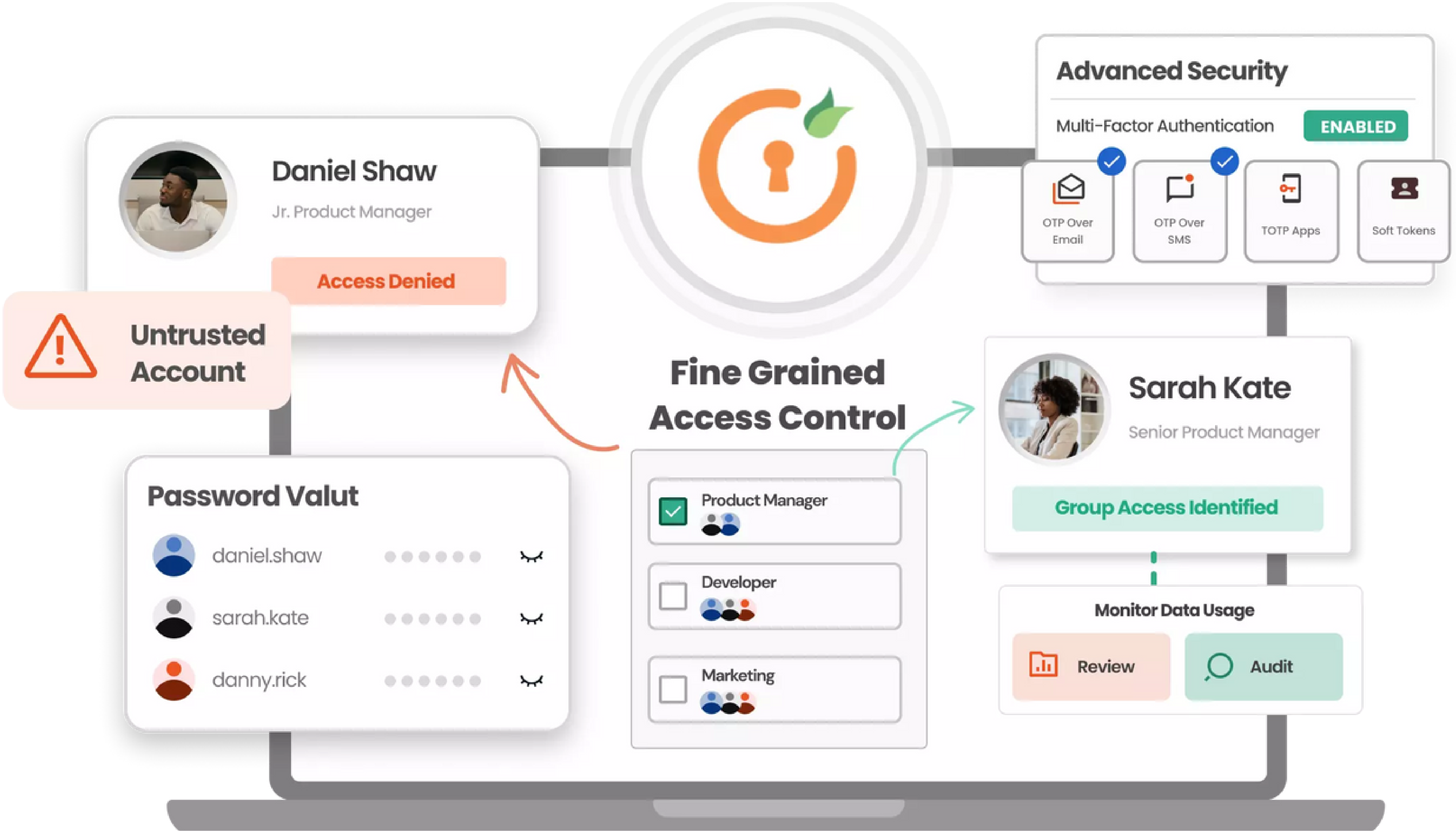
- The Accounts that have more Access or Rights than the usual or Ordinary user accounts. They are essential to the organizations.
- Example: Root user in Linux machine/databases, Administrator user in Windows machines, etc
- Because they contain the highest level of Access, these accounts are most vulnerable to Attacks

THE PRIVILEGED ACCESS PROBLEM

81%	Hacking related breaches leveraged either stolen and/or weak passwords
64%	All data breaches involve identity theft
3rd	Most prevalent cause of data breaches.

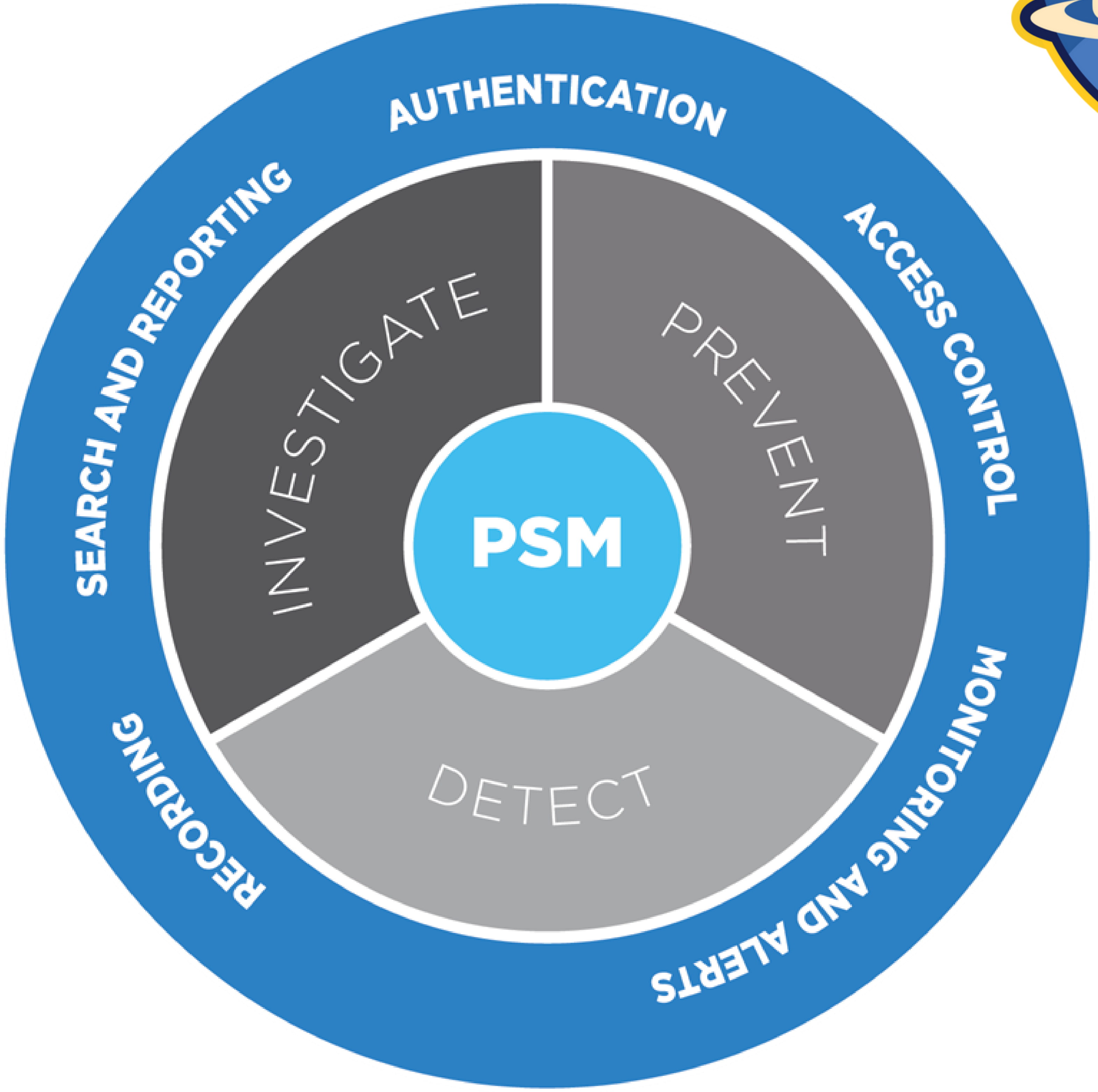
WHAT IS PAM?

A set of technologies that allow organizations to identify, secure and monitor accounts that have elevated privileges to minimize risks and ensure compliance.



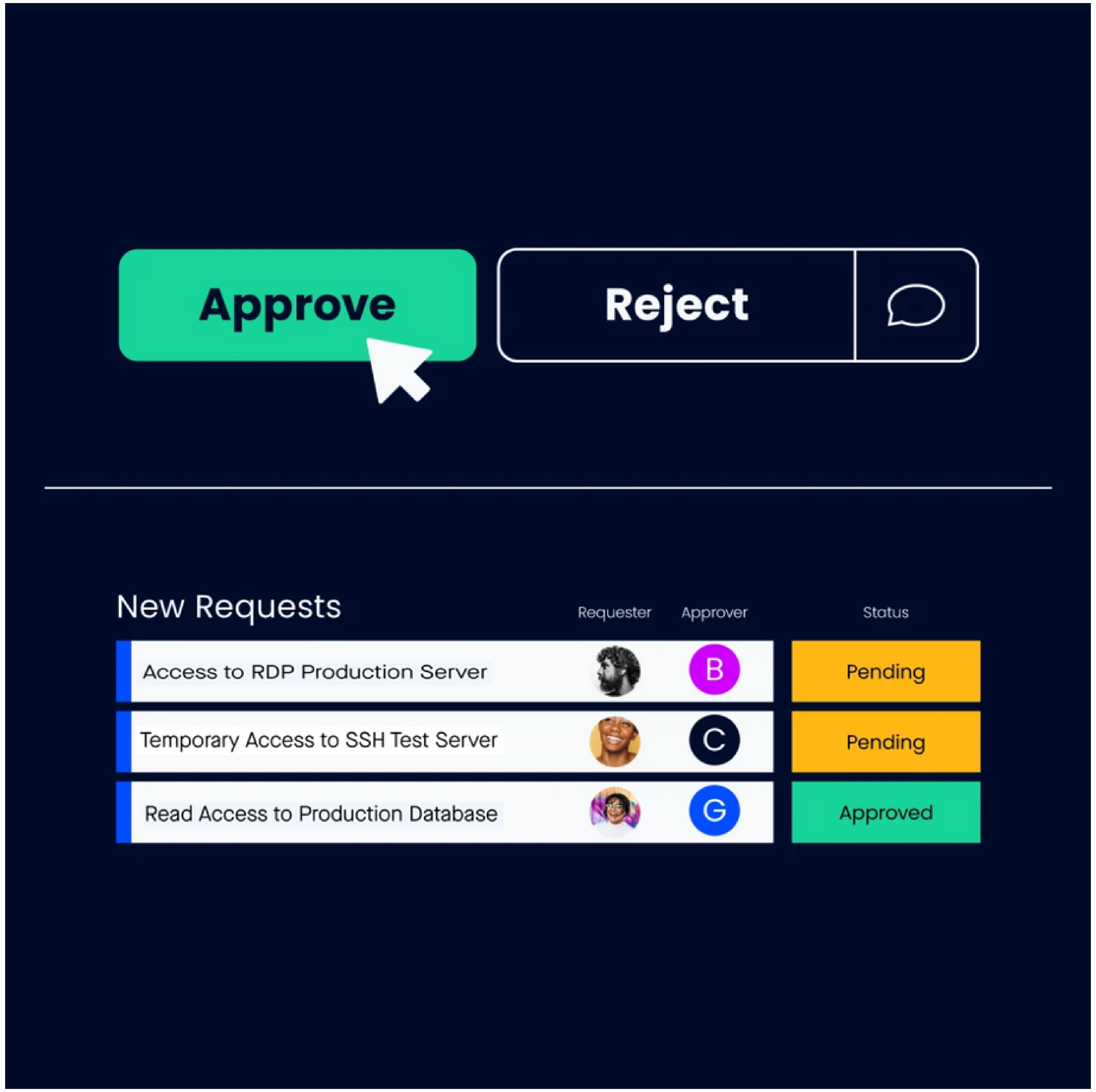
PRIVILEGED SESSION MANAGEMENT

- Record all user Sessions
- Real-time Notifications
- Access Control
- Continuos Authorization
- Behavioral Analysis of All Events and Activities
- Blocking malicious activity



TICKETING/ APPROVAL SYSTEM

- Just In time Access (JIT)
- Restricting Access with Zero Access
- Managing Records of Given Access
- Real-time Elevation and delegation of Privileges

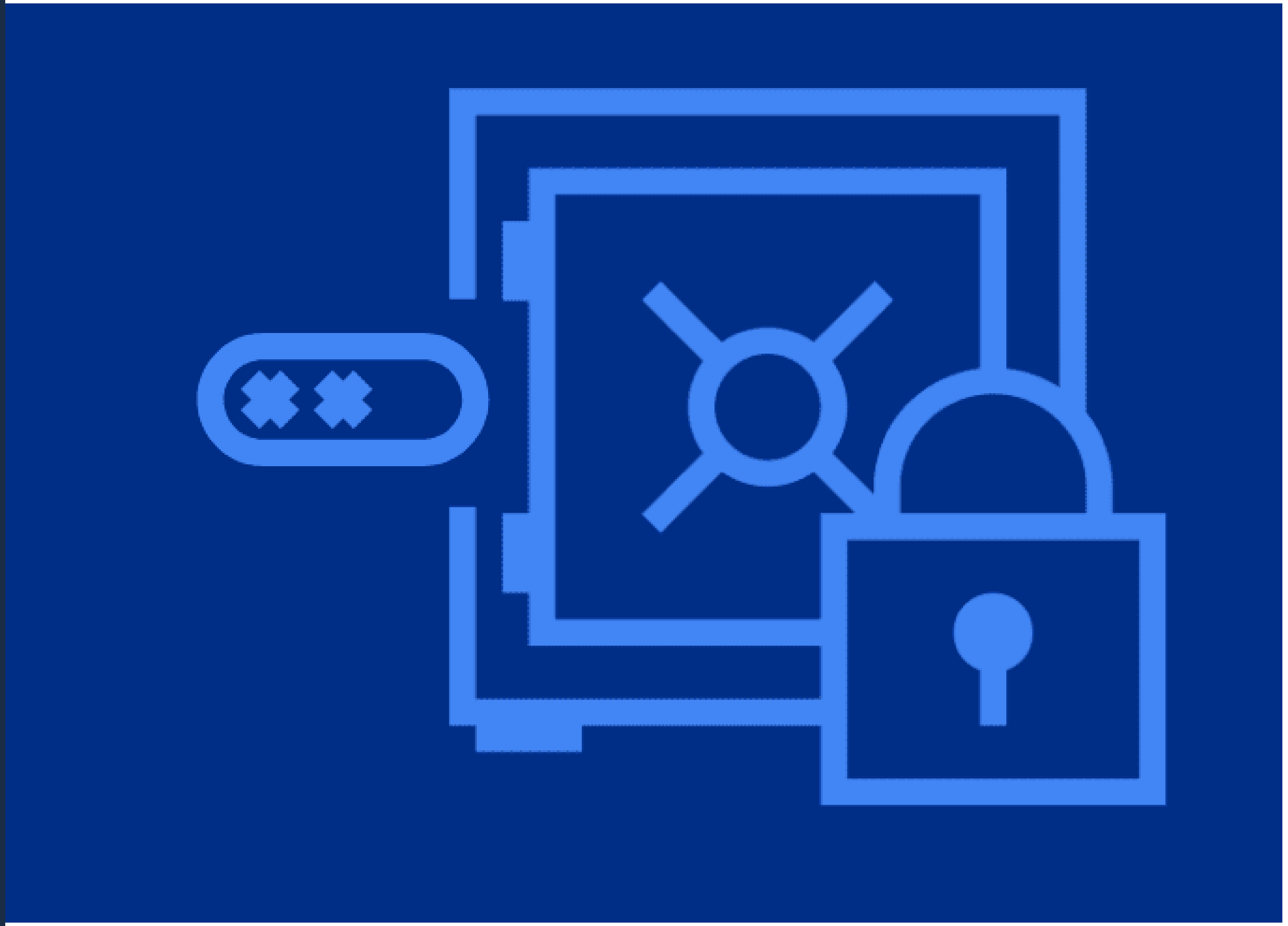


New Requests

	Requester	Approver	Status
Access to RDP Production Server		B	Pending
Temporary Access to SSH Test Server		C	Pending
Read Access to Production Database		G	Approved

PASSWORD VAULTING

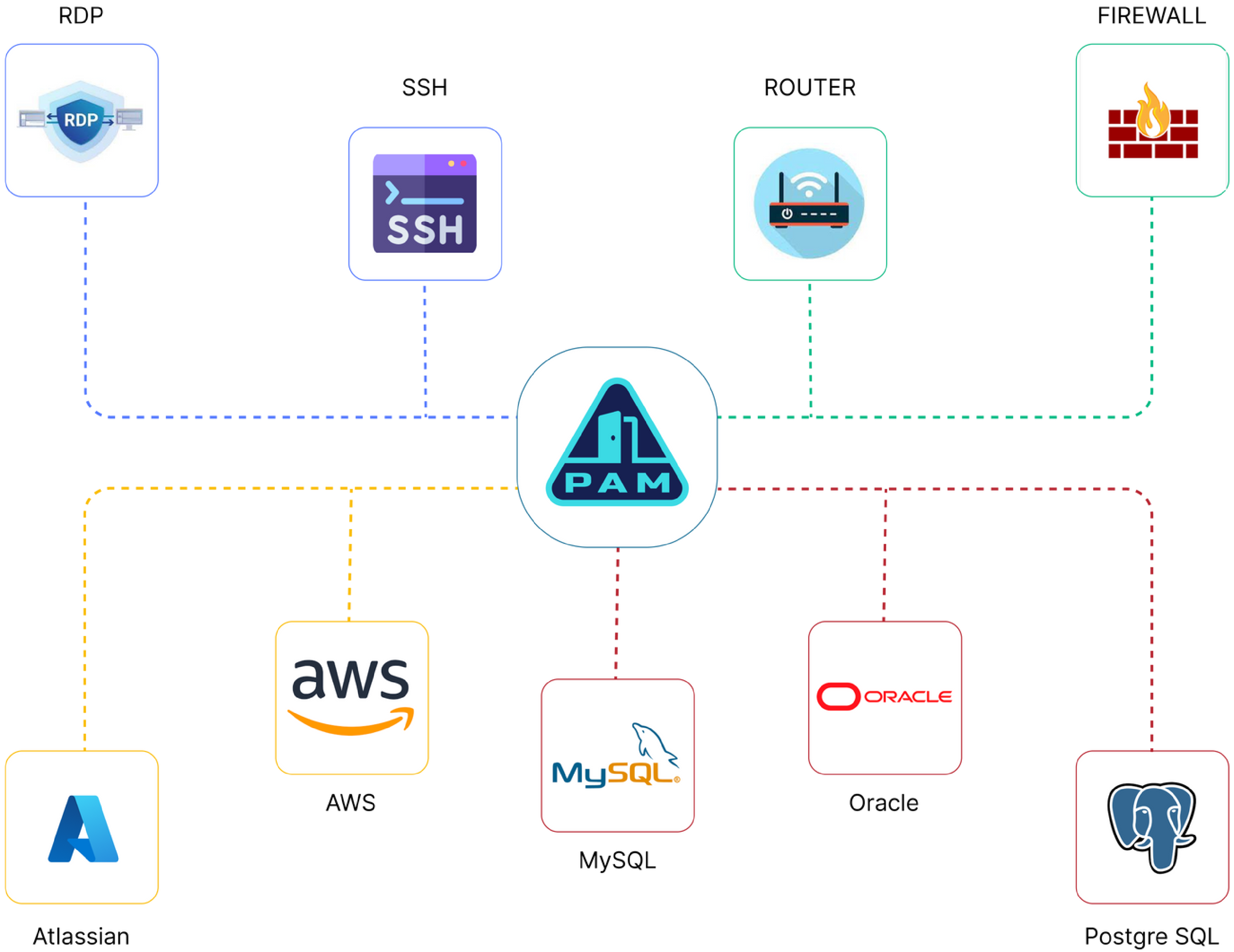
- Securely Storing Passwords, Secrets and Certificates
- Multiple Encryptions Algorithms
- HSM integration
- Password and Certificate Rotation



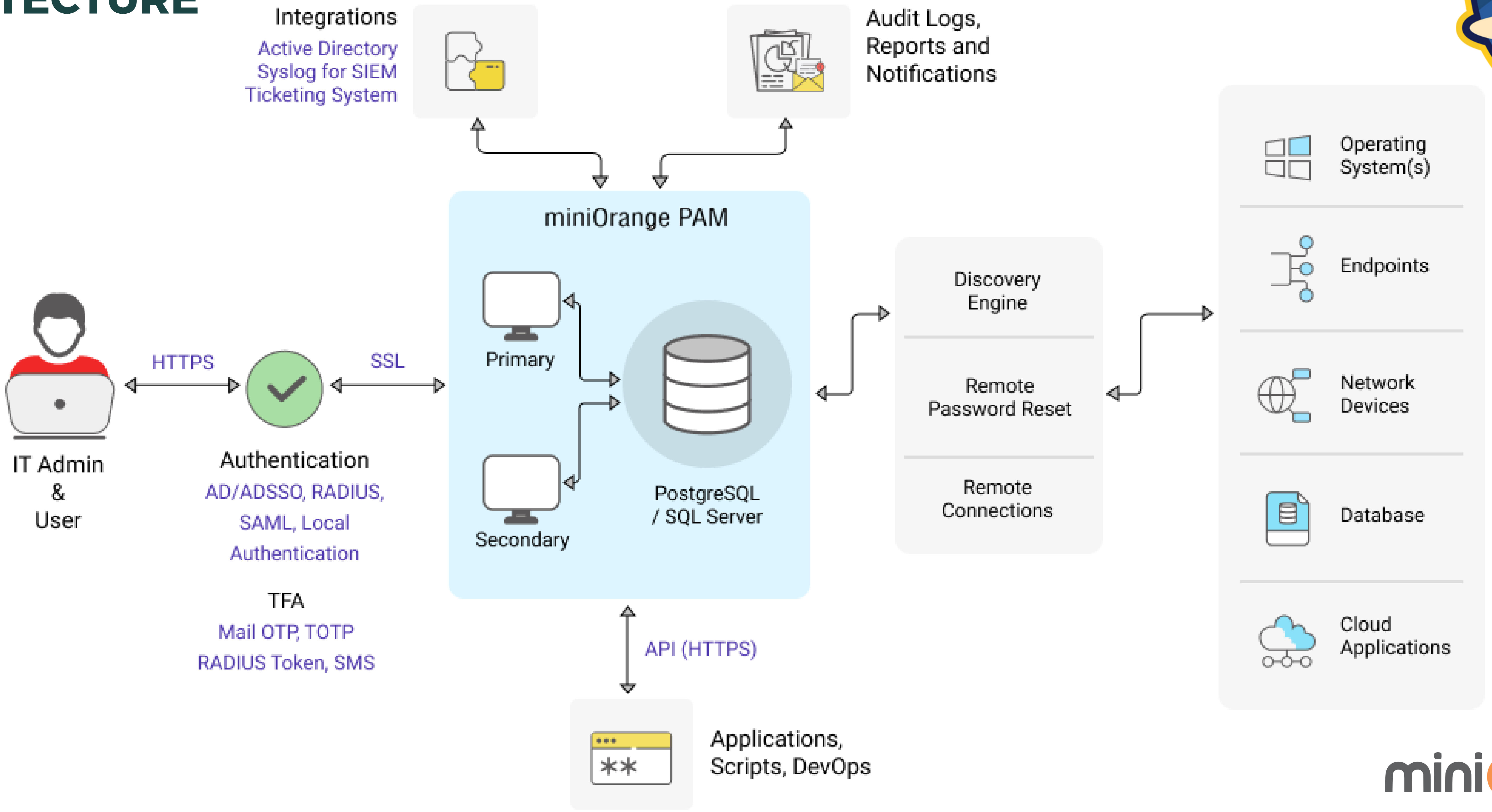
ANALYTICS & BLOCKING

- Analyzing all the Activities
- Detecting Malicious Activities
- Alerting and Notification
- Blocking Malicious Activities

INTEGRATIONS



ARCHITECTURE



SO WHY PAM

Why PAM

- Monitor and Record every Session
- Analytics to detect suspicious behavior and stop malicious activity
- Real-time alerting
- Approval System and many more.
- Compliance Requirements (GDPR, HIPAA, PCI, DSS, etc)

QUESTIONS & ANSWER!

Any Questions?

IdentityShield

THANKYOU

FEEDBACK

EMAIL

pradeep@xecurify.com

LINKEDIN

@pradeepparchani

CALL US

+91 8209449104

miniOrange