COMBIS

HT Grupa

30SEC
Security Operations Center

IBM SECURITY VERIFY PRIVILEGED ACCESS MANAGEMENT

Ivan Petrović, IBM Hrvatska

Zagreb | 24.05.2022.

What is Privileged Access Management

Privileged Access Management is a domain of Identity & Access Management focused on the special requirements for **managing powerful accounts** within the infrastructure of an enterprise.

Privileged Access Management is a information security requirement irrespective of industry, company size or location.

Types of Accounts

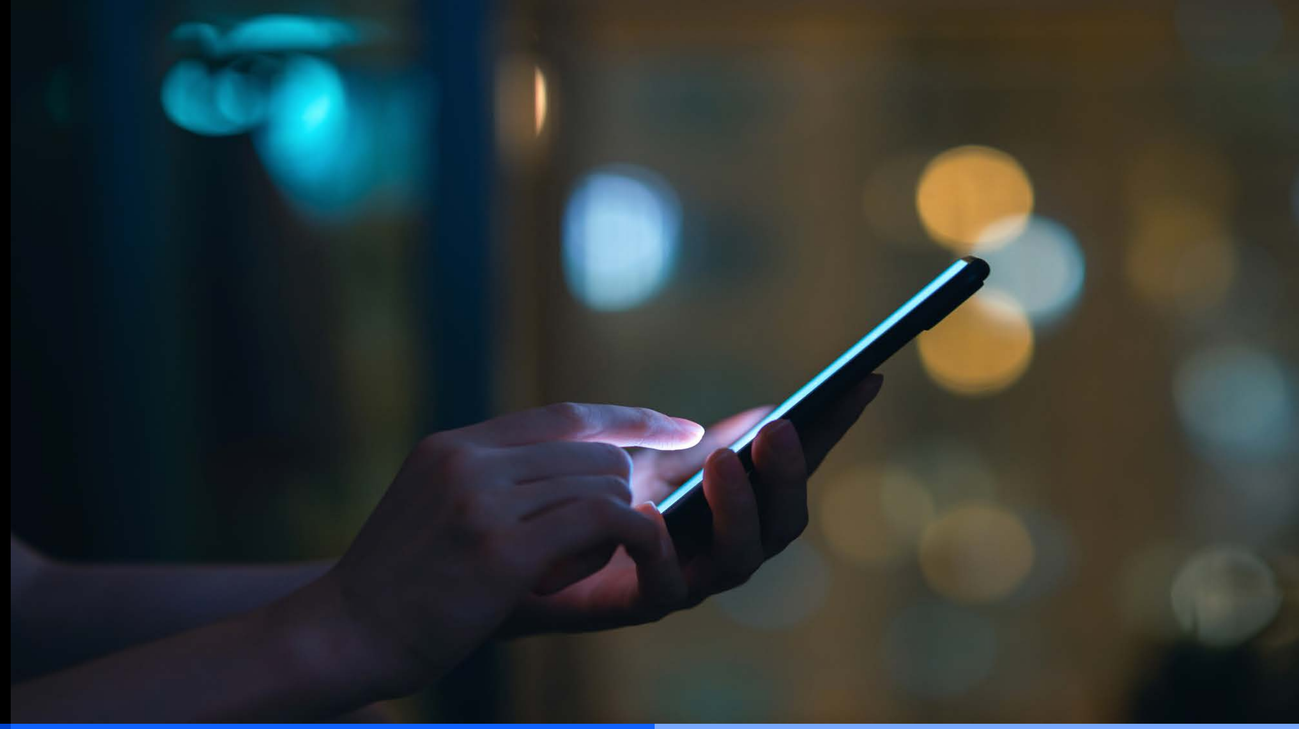
User Account

- Used by one person.
- Password that enables you to access the account and conduct your business.
- Passwords exist to protect your information from anyone else accessing your user account without your permission.

Privileged User

- Human or non-human
  - Systems Administrators
  - Security Administrators
  - Web Application Administrators
  - Service Accounts
  - Applications
- Allow IT professionals to manage applications, software, and server hardware.
- Passwords to control access.

Across the IAM landscape, privileged users are the biggest risk – protecting privileged accounts is mission critical



2X

Machine identities are growing at twice the rate of human identities and need protection

40%

of incidents involved an employee with privileged access to company assets

$3M

Average organizational cost savings in terms of reducing or eliminating insider risks via solutions like PAM

70%

By 2022, 70% of organizations will implement PAM for all use cases in the enterprise, up from 40% today

Why do customers purchase Privileged Access Management

1. Protect against internal and external threats
2. Meet compliance mandates and industry best practices
3. Automate scalable security processes and be more efficient

Why do customers purchase Privileged Access Management

1. Protect against internal and external threats
    - Privileged Accounts = keys to the kingdom
    - One compromised privileged account can allow access to IT network
2. Meet compliance mandates and industry best practices
3. Automate scalable security processes and be more efficient

Why do customers purchase Privileged Access Management

1. Protect against internal and external threats
2. Meet compliance mandates and industry best practices
    - These can include HIPPA / SOX / FISMA / FERC / NERC / GDPR / PCI / NIST etc
    - Must demonstrate Privileged Accounts are Secured, Controlled, Monitored & Audited
3. Automate scalable security processes and be more efficient

Why do customers purchase Privileged Access Management

1. Protect against internal and external threats
2. Meet compliance mandates and industry best practices
3. Automate scalable security processes and be more efficient
    - Manage and Control Privileged Accounts
    - Password Rotation to change passwords every 30/45/60/90 days
    - Service Account management
    - Requests for Access
    - Audit and Reporting, Monitoring and Key Logging
    - Remove “Default Passwords”
    - Requests for Privilege Elevation

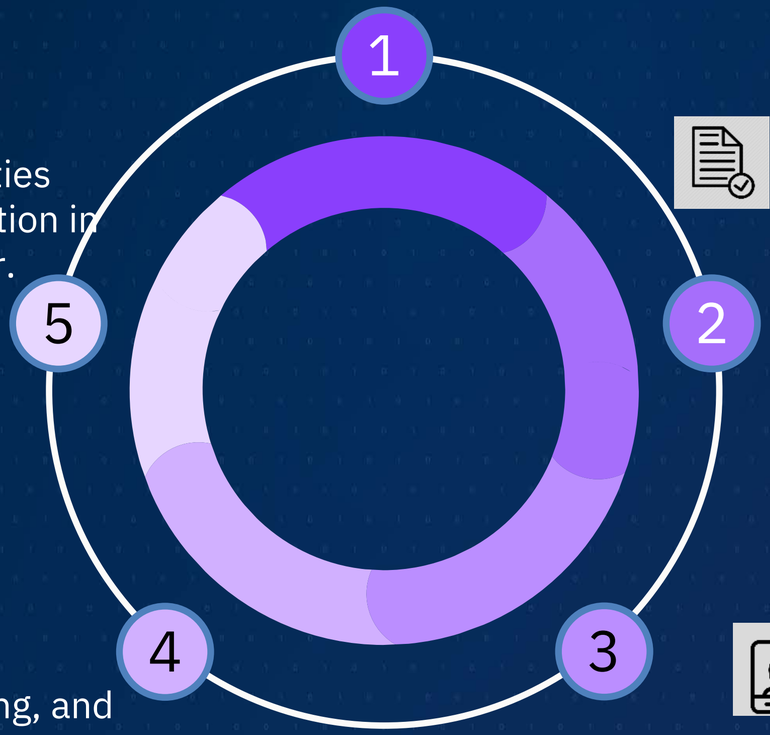
Where does “PAM” fit into the Digital Trust Framework?

Perform Assessment

- Automated Discovery of Privileged Accounts
- Discovery of local admin accounts, service accounts & applications in use on endpoints

Take Action

- Reporting and Alerting capabilities enable organizations to take action in the case of anomalous behavior.



Define Policy

- Secure Vault – Store privileged credentials in an encrypted, centralized vault.
- Manage Secrets – Provision and deprovision, ensure password complexity, and rotate credentials.

Monitor Behavior

- Implement session monitoring, and recording to monitor behavior

Establish Identity

- Assign access to specific privileged users
- Set up Role Based Access Control workflow for access requests, and approvals for third parties.

IBM Security Verify Privilege Vault (Thycotic Secret Server)

End User Served	IT & Security Admins, External users
Capabilities	Vaulting, Auditing & Privileged Access Control
Delivery Method	On-Premises Cloud

IBM Security Verify Privilege Vault allows you to discover, manage, protect, and audit privileged accounts across your organization.

Establish a Secure Vault

Store privileged credentials in an encrypted, centralized vault.

Discover Privileges

Identify all service, application, administrator, and root accounts to curb sprawl and gain full view of your privileged access.

Manage Secrets

Ensure password complexity and automatically rotate credentials.

Delegate Access

Set up RBAC, workflow for access requests, and approvals for third parties.

Control Sessions

Implement session launching, proxies, monitoring, and recording.

Privileged user access to target systems

Common access solutions <u>without PAM</u>:

- VPN ACLs based on groups
- Jump servers and/or *RDP Gateway*

1 .Internal or external user

- Intranet
- VPN

2. Apps & Services

- SSH
- RDP
- Web
- Application clients (e.g. SQL)
- API

Application

Unix Server

Windows Server

Database

Network equipment

Introducing Privileged Access Management – step 1.

1. Discover privileged accounts
2. Credential management (passwords & SSH keys)
   - credential takeover
   - credential vault (secrets)
   - credential rotation policies

IBM Security Verify Privilege Vault

Secrets

Credential management

Discovery

Internal or external user

- Intranet
- VPN

- SSH
- RDP
- Web
- Application clients (e.g. SQL)

Application

Unix Server

root

Windows Server

Administrator

Database

SYS

Network equipment

admin

IBM Secret Server Credential Management

Active Directory
Local Accounts
Service Accounts

All Linux/Unix
Distributions
SSH Key Management

MS SQL | Oracle
MySQL | Sybase
ODBC/JDBC

AS400 / OS390
zOS (RACF)
SSH & Telnet Compatible

Dell DRAC | HP iLO
VMware Hypervisors
SSH & Telnet Compatible

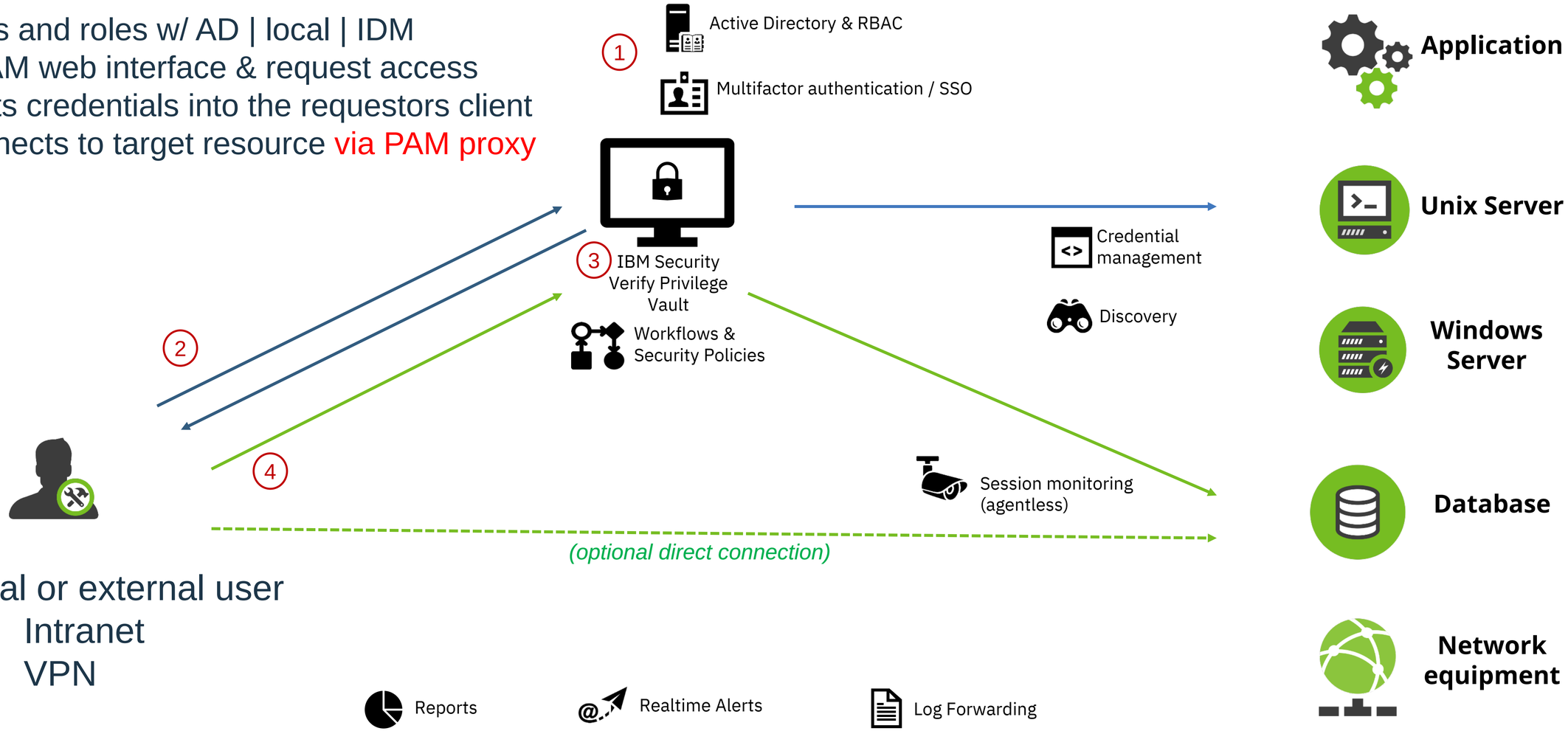
AWS IAM | Office 365
Google | Salesforce

Cisco | SonicWall
Juniper | F5
Blue Coat

PowerShell
SQL Queries
SSH Scripts

Introducing Privileged Access Management – step 2

1. Sync users and roles w/ AD | local | IDM
2. Access PAM web interface & request access
3. PAM injects credentials into the requestors client
4. Client connects to target resource via PAM proxy



Internal or external user

- Intranet
- VPN

IBM Security

Home
Recent
Shared With Me
Favorites
Inbox
Reports
Secrets
Personal Folders
Malik Merchant
Critical Accounts
Infrastructure
Active Directory
AS400 & Mainframes
Databases
Oracle DB
SQL Server Accounts
Linux Systems
Centos
Ubuntu
Networking

Infrastructure > Linux Systems > Centos

MM

6 Items | Active | All Templates

NAME	SECRET TEMPLATE	FOLDER	HEARTBEAT	OUT OF SYNC	LAST ACCESSED
centos1.iamlab.ibm.com\centosadmin1	Unix Account (SSH)	Infrastructure/Linux Systems/Centos	UnableToCo...	No	
centos1.iamlab.ibm.com\centosadmin2	Unix Account (SSH)	Infrastructure/Linux Systems/Centos	UnableToCo...	No	
centos1.iamlab.ibm.com\centosadmin3	Unix Account (SSH)	Infrastructure/Linux Systems/Centos	UnableToCo...	No	
centos1.iamlab.ibm.com\centosuser1	Unix Account (SSH)	Infrastructure/Linux Systems/Centos	UnableToCo...	No	
centos1.iamlab.ibm.com\centosuser2	Unix Account (SSH)	Infrastructure/Linux Systems/Centos	UnableToCo...	No	
centosuser3 (Session Recording)	Unix Account (SSH)	Infrastructure/Linux Systems/Centos	UnableToCo...	No	19 days, 18 hours ago

Summary: Do you really need Privilege Access Management?

Do you know how many privileged accounts you have and where are they located?

How are you securing and auditing access to privileged accounts?

How easily can you rotate privileged account passwords?

What is your process when an IT admin leaves the organization?

How are you monitoring IT admin access in sensitive systems?

How do you control and limit 3rd party access to sensitive systems?

How are you providing compliance for GDPR, PCI, HIPAA, NIST and other regulation to secure privileged access within your environment?

Does your SIEM strategy have insights into privilege account usage and activity?

HVALA NA PAŽNJI

30SEC
Security Operations Center

Platinum
Business
Partner

IBM

COMBIS
HT Grupa