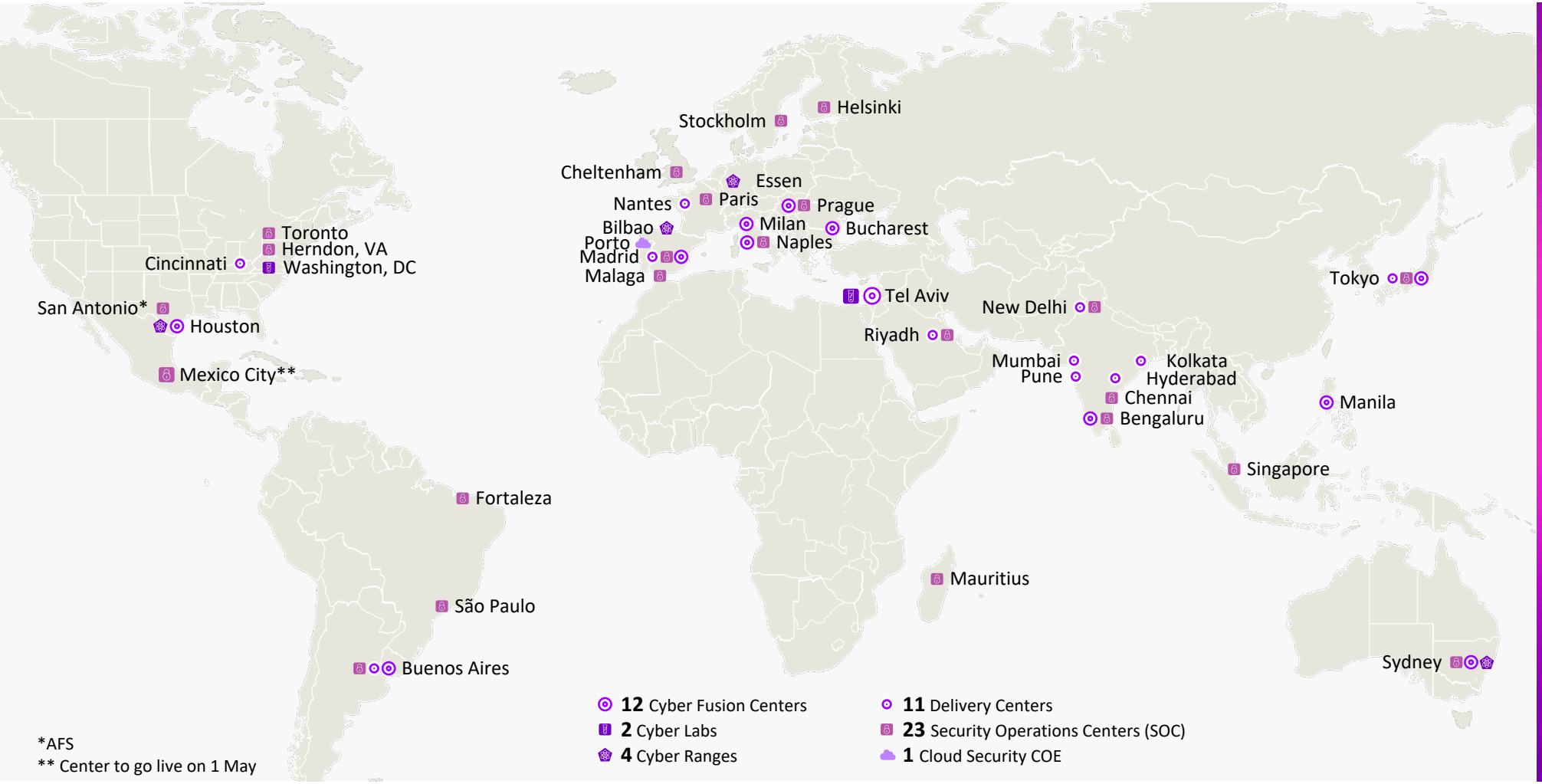
Modern PAM

Ragnhild Marie Holen
Accenture
April 2024

Global scale and local focus

One team enables a seamless experience from transform to run



*AFS
** Center to go live on 1 May

20,000+
Cybersecurity professionals

4,500+
Clients served

25
Years of service

67
Countries served

Readers guide for the PAM Capability Model

What is the first line of defense for any IT?

Identity Security

Protect New Identities – Human and Machine

Protect New Environments

Prevent new attack methods whether on-prem or in the cloud

Trends in Securing Digital Identities:

84% of Organizations experienced an identity-related Security breach in 2023

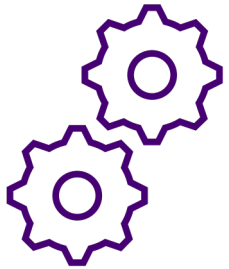
Principles

Key design principles for modern PAM

Adaptive and user-friendly processes and tools

Just-in-Time and least privilege access

Compliance and Audit



Automation

Modern PAM value drivers

What Good Looks like

VALUE DRIVERS

TARGET

OPERATIONAL EFFICIENCY

- ✓ **Expedited deployment**, increased **scalability/resiliency** , accelerated **expansion** and reduced complexity
- ✓ **Reduce costs** through self-service, automation and effective license management
- ✓ **Increasing employee productivity**

END-USER SATISFACTION

- ✓ Providing **seamless access to applications**
- ✓ Focus on "core business" by making **standard functionalities** available to development teams
- ✓ **Time to value** ; Scalable, secure and quicker access via just-in-time provisioning

RISK & COMPLIANCE

- ✓ **Securing digital assets** by strengthening and future-proofing the security perimeter
- ✓ Ensuring **effective control mechanisms** to facilitate **audit/legal compliance**
- ✓ **Central separation of roles,** capacities and responsibilities
- ✓ Zero trust framework for standing privileges in the Cloud and legacy on-prem

ECOSYSTEM ENABLEMENT

- ✓ Enhance **ecosystem connectivity**
- ✓ **Shortening time-to-market** for new applications
- ✓ Enable **analytics & insights**
- ✓ **Reduced security incidents**

Modern PAM Capabilities

Privileged Access Management

Pls note - Grey shaded capabilities are often overlapping with broader Identity and Access Management capabilities

PAM CAPABILITIES

Privilege Identity Management and Governance

Account Discovery & Onboarding
- Acct Discovery
- Acct Onboarding
- Entitlements Management

Account Lifecycle Management and Governance
- Privileged Account creation
- Access Provisioning
- Access Certification and Review
- Access Request and Provisioning

Access Management
- Authentication with MFA
- Authorization

Privileged Access Controls

Foundational PAM Controls
- Native Tool brokering
- Remote PAM
- Browser based Session Mgmt
- Session Isolation and Monitoring
- Credential Validation
- Credential Rotation

Zero Standing Privilege Access
- Privileged Elevation
- Ephemeral Access

Secrets Management
- Vaulting and Rotation
- Policy Enforcement
- Centralized Management

Endpoint Least-Privilege
- Privilege elevation
- Endpoint management
- Command based restrictions
- Local account credential rotation

Compliance & Threat Response

Threat Detection
- Analytics
- Deception
- Identity Threat Monitoring
- Threat Alerting

Threat Remediation
- Session Termination
- Risk Reduction
- Automated Remediation
- Privilege Entitlement Remediation

Compliance & Review
- Session recording / logging
- Automated session review
- Session termination
- Audit and Reporting

Privilege Identifies

Contractors | Employees | Application Admins | Traditional IT | 3rd Parties | Cloud Ops | DevSecOps | Engineering Teams | Data Scientists | Bots | Workloads | Apps | IoT/OT

Personas

Workforce	Infrastructure	Developers	Machines
Endpoints, Data, Biz Apps	Data, Apps, Cloud, Workloads, CI/CD Tools	Data, Apps, Workloads, Code Repos, Cloud Services	Devices, Data, Apps, Workloads, Code

Access Targets

Privilege Access Functions

What functions require privileged access?

We consider Privileged access to be any access (either on-prem or Cloud), that provides an individual with system privileges beyond the capabilities routinely granted to normal users. Typically, we consider an account privileged if an account has the capability to execute **one or more of the following**:

Can bypass, modify, or disable technical or operational security controls via the ability to

- Install Software
- Install/Modify system processes
- Create/modify System Configuration
- Create/modify System Access Controls
- Perform Access Administration Activities

Can access CSI, Sensitive Personal Information, information subject to compliance, Sarbanes Oxley:

- Execute system utilities, bypassing app logic/authorisation
- Modify database objects, tables, configurations and functionality
- Read, modify or delete the files or email of other users
- Monitor the privileged activity of employees
- Monitor unencrypted network traffic

Client challenges often include identifying where these privileged access types and functions intersect with their infrastructure and applications in the modern organization. This is where Accenture can help.

Modern PAM leverages Persona Approach

Enterprises are increasingly adopting Persona approach to drive efficiencies and standardization in Access Governance for Privilege Identities

Steps	Application Team/User	Operations Team	Cloud Platform
Traditional journey	User raises the request via E-mail or Snow Ticket, providing information of the Cloud Role and Resource.	Request is processed by the Operations team manually	Requested roles are manually configured on the Cloud Platform. Either user is assigned directly to a cloud resource or added in the AD/AAD Group
Steps	IGA Platform	PAM JIT Platform	Cloud Platform
Persona Journey	List of the Personas are available for the consumption	JIT Policy provides Just in time access on the cloud using ephemeral accounts	Roles are assigned real-time on cloud using JIT Policies.

Potential Benefits

Operational Efficiency

Automated cloud assignment brings efficiency

JIT-Access

Users get roles on the cloud or on-prem Infrastructure for the limited period

Automated Provisioning

Persona assignment is automated process leading efficiency and no human errors

Standardization

Users in the Persona have same roles based on the principles of least privilege.

Benefits of using personas

Using personas rather than access roles brings several benefits, mainly in later phases of implementing IAM in the Cloud.

- **Abstraction** - Personas are **business friendly** ways of describing persons interacting with use cases, they prevent low-level discussions around what access rights belongs where.
- **Automation** - It increases **automation possibilities** by moving away from tailor made custom roles and enabling a small set of access
- **Access Control** - Combined with CIEM, it increases the **ability to enforce least privilege** as there is more granularity in access than just owner or contributor.

PAM Maturity model

PAM Maturity

Know your Privileges

Level 0 Non-Existent

- Privileged access management is not in place.
- No inventory of privileged account exists.
- No PAM standards or processes being followed.

Vaulting and Rotation

Level 1 Informal

- PAM tool is purchased and main components are installed.
- Credentials are vaulted and rotated with baseline policy
- Lack of formal privileged account inventory.
- Lack of audit reporting.

Formalized Account On-boarding

Level 2 Repeatable

- The organization follows a consistent process to onboard privileged accounts.
- Basic account policy and workflow is configured but not standardized.
- Apply role-based access to privileged accounts on need-to-know basis
- Ad-hoc audit and reporting being performed.

Standardized PAM

Level 3 Defined

- A formalized account mgmt process (onboarding/modify/retirement) is defined.
- User access workflow is defined in accordance to enterprise policy and SoD is in-place.
- Privileged account inventory is complete and onboarded into PAM tool.
- Account discovery is performed on a periodic basis.

Enhanced Privilege Access Governance

Level 4 Measured

- Privileged user activity is fully monitored with session recording.
- More advanced feature such as just-in-time (JIT) privileged access are utilized to enforce least privilege controls on applications and endpoints.
- PAM tool is fully integrated with ITSM/IAM systems to track & monitor requests for privileged account management.

North Star PAM

Level 5 Optimized

- PAM tool is fully integrated with applications and DevOps tools to eliminate hardcoded/embedded credentials.
- PAM tool is integrated with SecOps organization to monitor, detect, and respond to malicious privileged activity.
- Automated reports are continuously reviewed to validate compliance with policies and regulations.

Automation

Security Maturity

Cloud Privileged Access Management

Privileged Access in Cloud – Control Methods

For privileged access use cases in Cloud, we have considered control methods and corresponding environments

USE CASE	METHODS	ENVIRONMENTS
PAM for the Management Layer	Secure access CSP service **IN** the cloud with Native, Zero Standing Privilege access	aws, Azure, Google Cloud
PAM for the Platform Layers	Secure access for workloads **ON** cloud infrastructure (IaaS) with Dynamic, Just-In-Time access	Linux, kubernetes, Windows Server, redis, PostgreSQL, docker
PAM for the Application Layers	Vaulted Secure access to applications	SAP, servicenow, Microsoft SQL Server, ORACLE, JBoss by Red Hat

Privileged Access in Cloud – Environments

For each use cases and related environments, we have mapped corresponding personas and related privilege functions

USE CASE	ENVIRONMENTS	EXAMPLE PERSONAS
PAM for the Management Layer	aws, Azure, Google Cloud	Developer, Cloud Foundation Admin, Security / Audit Manager, Machine Identities
PAM for the Platform Layers	Linux, kubernetes, Windows Server, redis, PostgreSQL, docker	Platform Admin, Operations Manager, Machine Identities
PAM for the Application Layers	SAP, servicenow, Microsoft SQL Server, ORACLE, JBoss by Red Hat	SRE Team, Operations Manager, Machine Identities

Privileged Access in Cloud – Solution Components

To secure privilege access in Cloud, we recommend corresponding capabilities controls mapped to environments and personas

USE CASE	ENVIRONMENTS	EXAMPLE PERSONAS	PAM CAPABILITIES CONTROL
PAM for the Management Layer	aws, Azure, Google Cloud	Developer, Cloud Foundation Admin, Security / Audit Manager, Machine Identities	Ephemeral Access Privileged Elevation Entitlements Management
PAM for the Platform Layers	Linux, kubernetes, Windows Server, redis, PostgreSQL, docker	Platform Admin, Operations Manager, Machine Identities	Centralized Management Privileged Elevation
PAM for the Application Layers	SAP, servicenow, Microsoft SQL Server, ORACLE, JBoss by Red Hat	SRE Team, Operations Manager, Machine Identities	Credential Validation Credential Rotation Browser based Session Mgmt