Grab n’ Go - Privileged Access Management

March 23, 2021
Covering today...

1. Introduction
2. What is PAM?
3. Why this matters?
4. Our approach & experience
5. Your Next Steps
**Introduction**

**Johnny Shin**  
Partner, Cyber Risk  
IAM Practice Leader, Denmark / Nordics

- Over 20 years of Information Security and IAM experience
- Worked in consulting services serving clients in financial services, manufacturing, pharma, and energy industries
- Moved to Denmark a year ago from the US

**Annant Gujral**  
Senior Manager Cyber Risk  
IAM and PAM SME, Denmark

- 10 years of consulting experience in IAM and PAM
- Experience on multiple IAM & PAM products serving clients globally; across industries such as FSI, Telecom, Logistics, Retail and Energy
32,217 BC
FIRST ACCESS CONTROL SYSTEM

Today...
Covering today...

1. Introduction
2. What is PAM?
3. Why this matters?
4. Our approach & experience
5. Your Next Steps
Definition....

*Privileged Access Management*

/ˈpəm, ˈpaa(ə)m/

“Protection and management of accounts which have elevated permissions to critical and high valued corporate resources.”
Welcome to the backstage
Backstage passes are managed in a specific manner as they provide a higher level of access.
Welcome to the management plane
Privileged access to the management plane requires specific controls to protect the crown jewels.

Manage the system
- Admins
- IT Systems
- Vendors

Use the system
- Business Applications
- Personal account + credential
- Personal account + password
- Shared account + password
- Alternative credentials (e.g. SSH-keys)
- Trust mechanisms & bypasses

Actors
- Personal account + credential
- Personal account + password
- Shared account + password
- Alternative credentials (e.g. SSH-keys)
- Trust mechanisms & bypasses

PAM habitat

IAM habitat

Actors
- Customers
- Business users & Partners
Why PAM matters?
The characteristics of a management plane.

• Each digital system has a management plane typically accessible via different access paths. Examples:
  • IT Infrastructure
  • Applications
  • Industrial control systems
  • Consumer IT

• Digital systems are geographically spread.

• Management planes are used a lot by Vendors, Partners, Admins, and mostly by other systems.

• Each component requires therefore a set of controls ensuring the overall management plane is sufficiently secured.
In Summary

Protection of access to Production Infrastructure (SAs, Developers, DBAs)
- Enable MFA
- Integration with PAM
- Behavior analytics and insider prevention

Protection of access to Source Code Repository (e.g. GitHub)
- Controlling developers’ access to source code repository
- Enable MFA
- Integration with PAM
- Behavior analytics and insider prevention

Protection of credentials stored in source code
- Removal of credentials stored directly in the source code
- Integration with PAM secret vault

Protection of the privileged service accounts used in the DevOps pipeline
- Integration of the DevOps tools (Kubernetes, Ansible, Jenkins, Azure DevOps, etc.) with PAM secret vault
Covering today...

1. Introduction
2. What is PAM?
3. Why this matters?
4. Our approach & experience
5. Your Next Steps
Why do we need to care?
Key PAM drivers

**COMPLIANCE**
There is increasing regulatory emphasis on securing privileged access.

**RISK**
80%* of breaches involve misuse of high privileged accounts resulting in accessing highly sensitive data.

**CONTINUITY AND COST**
Losing privileged accounts typically involves downtime for correction.

**AUDIT**
Stringent requirements on the auditability of privileged access require specialized PAM tools.

Covering today...

1. Introduction
2. What is PAM?
3. Why this matters?
4. Our approach & experience
5. Your Next Steps
The controls – PAM is not solved by implementing a tool

More than one tool is required to bring the six key areas influencing the effectiveness of PAM. Control maturity can be re-used as metric on how well PAM is under control.
Having a PAM Framework is important to navigate through the interdependencies, common pitfalls and areas of improvement and optimisation.
Risk driven – Protect against 7 key threats
Reducing the likelihood of these threats is directly related to the benefit realized to the organization through the deployment of PAM.

1. **Unauthorised access by movers or leavers**
   Individuals maintaining their levels of access after their has changed, impacting the confidentiality, integrity and/or availability of the application or its data.

2. **Unauthorised access by breached or stolen credentials**
   Unauthorised individuals obtained access to the environment impacting the confidentiality, integrity and/or availability of the application or its data.

3. **Third parties having unsupervised and/or excessive access**
   Third parties accessing the environment in an unsupervised way impacting the confidentiality, integrity and/or availability of the application or its data.

4. **Errors due to the continuous usage of privileged access**
   Human errors enabled through the usage of high privileges impacting the confidentiality, integrity and/or availability of the application or its data.

5. **Unable to ensure availability of the system**
   Service disruption via the management plane and its high privileged credentials impacting the availability of the application or its data.

6. **Infringements to regulatory requirements**
   Non-compliance to regulatory requirements (e.g. GDPR) impacting the trust of auditors and customers.

7. **Inability to perform fraud/forensic analysis**
   Not being able to perform forensic analysis, fraud & dispute analysis due to non-repudiation impact.
Covering today...

1. Introduction
2. What is PAM?
3. Why this matters?
4. Our approach & experience
5. Your Next Steps
Take the PAM Journey in 3-STEPs

**STEP 1**

**Accelerated PAM Assessment**

- Most of the work delivered as a value-add with only a partial charge to the client
- Conduct an IAM/PAM workshop to define the current posture
- Deloitte to provide findings and recommended ‘to-be’ report
- Must have CIO / CISO sponsor this assessment with the full collaboration and support from the IT/ Business Teams

**STEP 2**

**PAM Proof of Value / Pilot**

- Engage 8-12 weeks PoV / Pilot to demonstrate the value
- Partner with the solution vendors to accelerate the solution baseline deployment
- Prioritise the key capabilities and limit the scope for the demonstration
- Finalise the business case and strategic roadmap for full deployment

**STEP 3**

**PAM Capability Release and Onboarding**

- Full capability design and implementation leveraging the baseline environment already established
- Prioritise the capability release and business/ system onboarding plan
- Establish governance model across the business, IT, Security, and Internal Compliance
- Establish metrics to measure the progress
Contact Information

Johnny Shin
Partner, Cyber Risk
Identity and Access Management Practice Leader, Nordics

Email: johshin@deloitte.dk
Phone: +45 3093 4480

Annant Gujral
Senior Manager Cyber Risk
IAM and PAM SME, Denmark

Email: agujral@deloitte.dk
Phone: +45 5222 6986
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 263,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication is for internal distribution and use only among personnel of Deloitte Touche Tohmatsu Limited, its member firms, and their related entities (collectively, the "Deloitte network"). None of the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2021. For information, contact Deloitte Touche Tohmatsu Limited