PAM
Privileged Access Management

Neo Vedder

Por que PAM é tão importante?

- 63% das violações envolvem credenciais de dados (Relatório 2022 Verizon Data Breach Investigations)
- 80% das violações de segurança envolvendo credenciais privilegiadas (Forrester Research)
- Reconhecimento do Gartner por 2 anos seguidos como projeto #1 em segurança da informação.
- 280 dias é o tempo médio para identificar e controlar uma violação - Ponemon Institute

O que é PAM

- ➔ Gestão de credenciais para garantir que apenas usuários autorizados tenham acesso aos sistemas e informações que precisam para desempenhar suas funções.
- ➔ Auditoria completa de acesso, incluíndo vídeo e transcrição das sessões.
- ➔ Granularidade de autorizações: fluxo de aprovações, gestão de quando, onde e como.
- ➔ Gestão de colaboradores externos e momentâneos (tokens)
- ➔ Compliance para GDPR, HIPAA, PCI DSS...
- ➔ Grande redução de superfície de ataque
- ➔ Controle de IoTs que normalmente não possuem gestão de usuário
- ➔ Controle de sistemas legados, com baixa segurança de IAM

Líderes

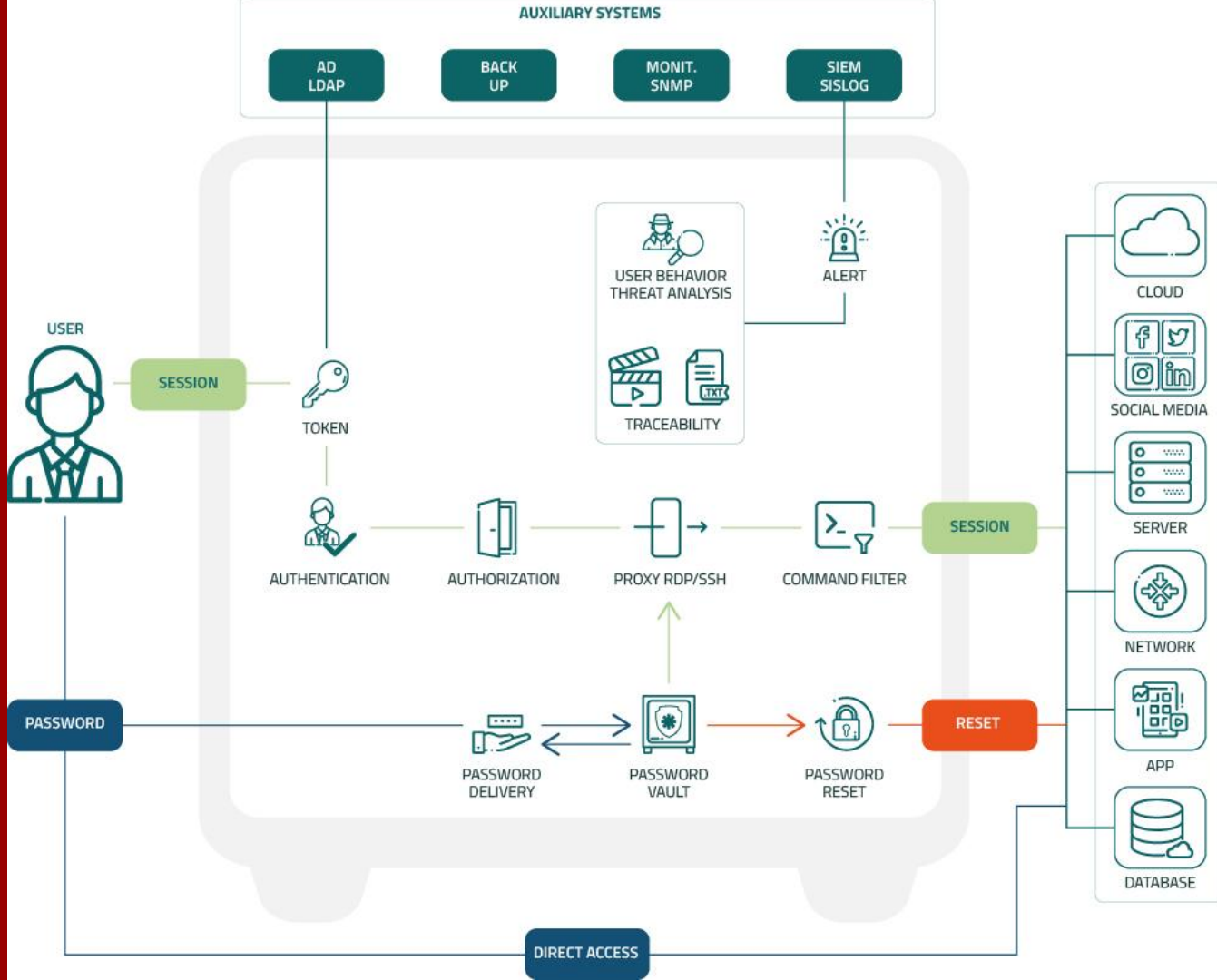
Figure 1: Magic Quadrant for Privileged Access Management

Source: Gartner (July 2021)

Figure 1 : Magic Quadrant pour la gestion des accès privilégiés

Source: Gartner (July 2022)

ARQUITETURA



Desafios e implementação

- Ambientes heterogêneos
- Resistência dos usuários (encaram como perda de liberdade)
- Restrições orçamentárias
- Baixa expertise em práticas de PAM (MFA, rotas de acesso)
- Medo da dependência tecnológica (mas sem um PAM é impossível implementar - Gartner)

PDCA do PAM

- Planeje e comunique as metas, objetivos e prazos
- Configure e personalize alinhado com as políticas e procedimentos
- Personalize para suas necessidades e requisitos
- Treine e eduque sobre o uso e importância

REPITA

- Revisão regular dos privilégios
- Monitoramento das atividades para estabelecer padrões de comportamento e identificar ameaças
- Auditorias para garantir conformidade com regulamentos
- Tunning diante de novas ameaças

senhasegura

- RBAC
- MFA impositivo
- Granularidade do serviço que a credencial pode usar
- JIT Access
- Rotacionamento por prazo e/ou por uso
- Gravação e indexação da sessão

Maiores benefícios

- Curto prazo de existência do acesso por conta do rotacionamento.
- Monitoramento em tempo real
- Rollback, auditoria e trilha de uso

#1 Revogação instantânea

OBRIGADO