Columbus

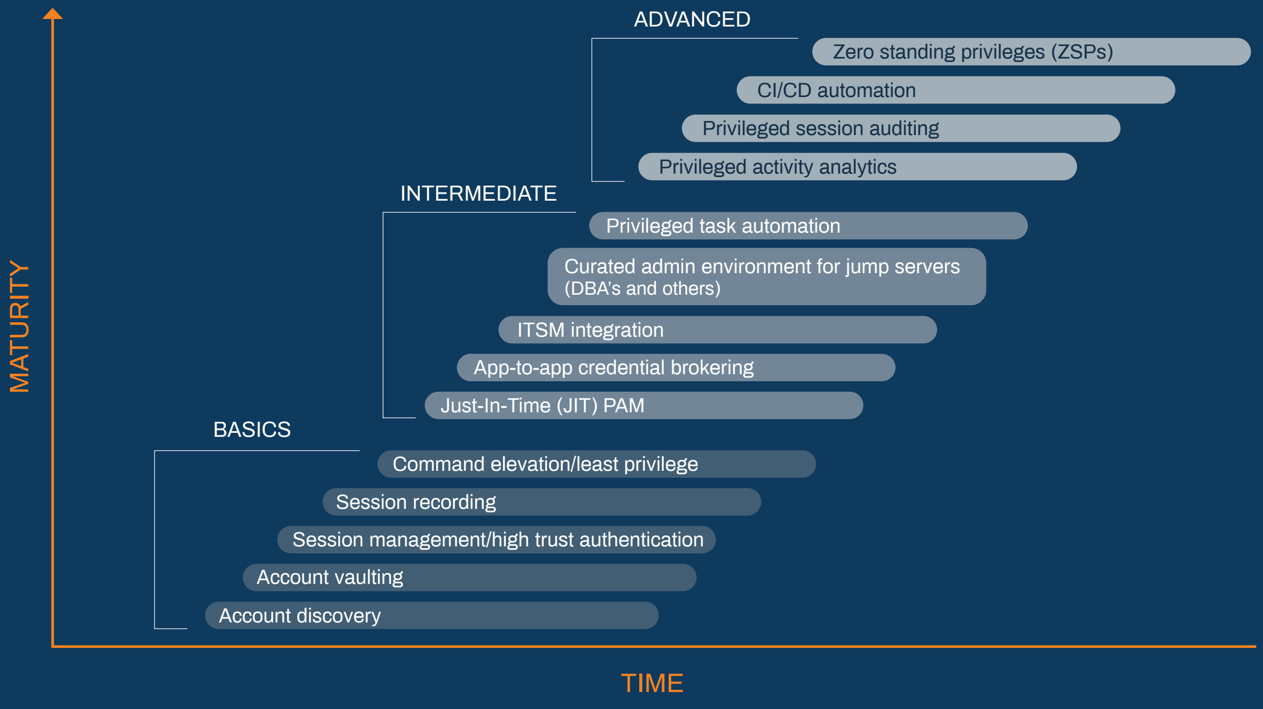
Privileged Access Management

Privileged Access Management (PAM) is your corporate weapon to “stop attackers in their tracks”.

A compromised privileged user account can cause extensive data leaks and, in the worst-case scenario, irreparable damage to the organization’s infrastructure, intellectual property and reputation.

PAM is designed to prevent security breaches by consistently subjecting privileged user access to more control, providing proactive enforcement of security policies, and targeted monitoring and recording of privileged user activity across virtual, cloud-based and physical environments.

Inventory and use cases



ADVANCED

- Zero standing privileges (ZSPs)
- CI/CD automation
- Privileged session auditing
- Privileged activity analytics

INTERMEDIATE

- Privileged task automation
- Curated admin environment for jump servers (DBA’s and others)
- ITSM integration
- App-to-app credential brokering
- Just-In-Time (JIT) PAM

BASICS

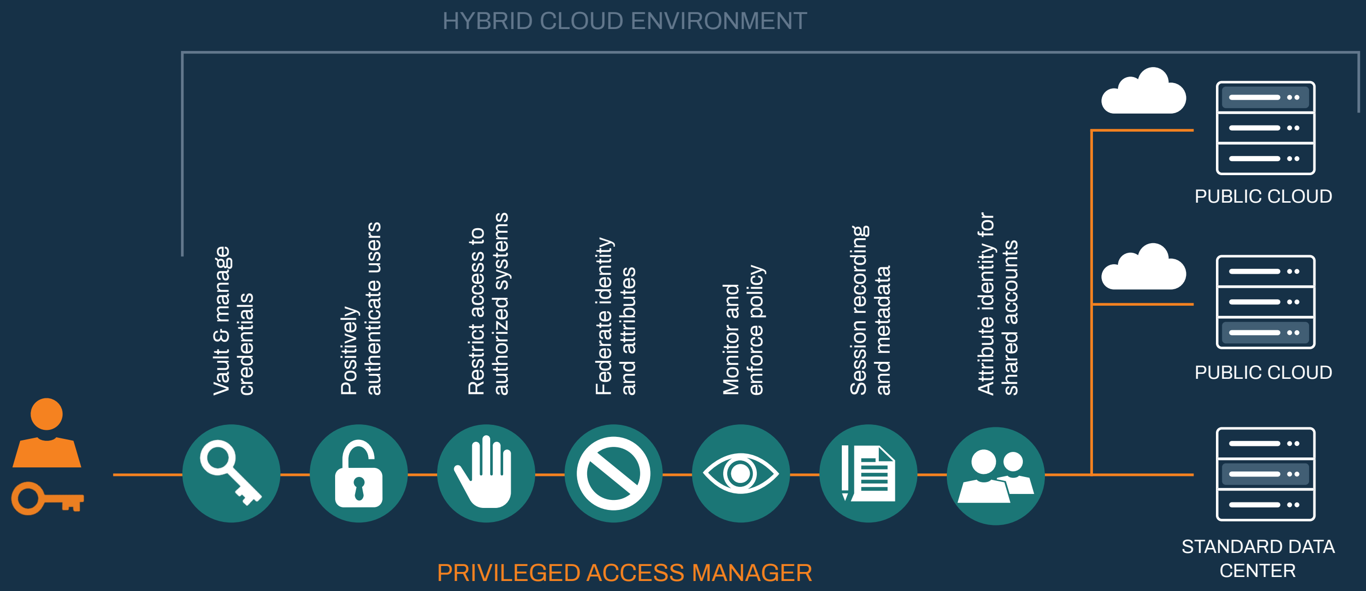
- Command elevation/least privilege
- Session recording
- Session management/high trust authentication
- Account vaulting
- Account discovery

Columbus

Your gains from PAM

By implementing a PAM-solution you are able to detect and stop threats in realtime and keep unauthorized users out of your environment. PAM can easily be deployed as-a-Service, or you can host it in your own environment.

PAM “in action”


HYBRID CLOUD ENVIRONMENT
Vault & manage credentials
Positively authenticate users
Restrict access to authorized systems
Federate identity and attributes
Monitor and enforce policy
Session recording and metadata
Attribute identity for shared accounts
PUBLIC CLOUD
PUBLIC CLOUD
STANDARD DATA CENTER
PRIVILEGED ACCESS MANAGER

Implementation of PAM

We offer four specific implementation plans (levels) for PAM deployments. Our packages are designed to achieve the basic outcome and fit your preferred deployment technology and project scope.

The basic outcomes include: Account discovery, account vaulting, password rotation, session management/recording, integration to relevant IT-Services and log management.

Our risk-based approach will help determine which tier will work best for you.

TIER 1 - MINOR	**20 DAYS**
TIER 2 - MEDIUM	**30 DAYS**
TIER 3 - LARGE	**40 DAYS**
CUSTOM	**TBD**

kontakt.dk@columbusglobal.com