

Governance

PRIVILEGED ACCESS MANAGEMENT

GovPAM

Control privileged access. Keep actions accountable.

Bring privileged accounts, asset permissions and session oversight into one operational workspace. Give authorized users a controlled route to critical systems, with the evidence security teams need to review their activity.



Know the assets and accounts

Organize managed systems and the credentials used to access them.



Control the path to privilege

Apply authentication, permissions and approval controls.



Review what happened

Use session records, replay and command audit where supported.

CAPABILITIES

Put privileged access under control.

Privileged access needs a clear connection between the user, the asset, the account and the action. Governance (GovPAM) brings those controls into the daily work of administrators and security operators.

CAPABILITY	WHAT IT ENABLES
Assets & accounts	Maintain managed asset and account records, platforms and connection context. Give operators a structured view of the systems they protect.
Credential management	Manage account secrets, passwords and SSH keys with native permission controls. Place sensitive credentials behind a controlled management process.
Asset authorization	Define who can access selected assets and accounts, and the actions permitted. Keep privileged access aligned with operational responsibilities.
MFA & approvals	Apply configured multi-factor authentication and access or command approval workflows. Add verification and accountable decisions around sensitive access.
Session oversight	Review session activity, recordings and command records; terminate active sessions when required. Support investigation and operator accountability with activity evidence.
Organization & audit	Use organization-scoped administration, permissions and audit workspaces. Delegate operations while retaining a record of privileged activity.

✓ Access that fits the environment

Support browser-based access to configured systems, including SSH and RDP through the appropriate deployed gateways. Session, file-transfer and command controls depend on the protocol and target platform.

IN PRACTICE

A controlled route to critical systems.

Carry the same access context from the initial request through the privileged session and its review.

01 Establish the access boundary

Organize assets and accounts, then define the users, groups and actions permitted for each scope.

02 Verify the user and request

Apply the configured authentication policy and approval steps before sensitive access proceeds.

03 Connect through the managed route

Launch an authorized session using the supported connection components and asset permissions.

04 Review and respond

Inspect session evidence and command activity, investigate exceptions and terminate access when needed.

WHERE IT HELPS

Infrastructure teams

Give administrators an authorized route to servers and managed systems.

Security operations

Review privileged sessions and investigate unusual activity.

Delegated operations

Scope access for internal teams and approved external operators.

Connect privilege to identity governance

Add Protect Identity IGA to govern who is eligible for PAM. Approved eligibility provisions a normal GovPAM identity; asset permissions remain explicitly managed in GovPAM. Offboarding disables the managed account and queues termination of its active sessions.

The shared workspace connects product navigation and subscriptions. Each product retains its native authentication and authorization responsibilities.

YOUR NEXT STEP

See a privileged access journey.

Build a demonstration around one of your critical systems and the people who need to administer it.

01 Choose the target system

Identify an asset type, supported protocol and account to bring under management.

02 Define the access rule

Explore user eligibility, permissions, authentication and approval requirements.

03 Review the session evidence

Follow the connection through activity records and the investigation workflow.

Deploy GovPAM for your access priorities.

Install Governance (GovPAM) independently or pair it with IGA and M365 x Azure Security Scan. Each product has its own subscription within the Protect Identity offering.

Each customer installation has its own service configuration, state, databases and keys. Choose one, two or all three products, with separate subscriptions.

LET'S PLAN YOUR DEMONSTRATION

Book a GovPAM demonstration

Bring control, visibility and accountability to privileged access.

sales@protectidentity.co.za

Deployment scope depends on managed assets, supported target platforms, gateway components, storage and configured security policies.