PRODUCT SHEET

Advantal™

ADVANTAL'S PRIVILEGED ACCESS MANAGEMENT (PAM)

Secure, Controlled, and Auditable Privileged Access for Enterprise Infrastructure

Overview

Advantal PAM provides a centralized privileged access control layer for servers, databases, network devices, applications, and web-based administrative systems. Administrative access is routed through controlled and encrypted access paths so that organizations can govern how privileged access is requested, approved, monitored, and audited.

The platform supports bastion-style privileged session brokering, secure credential handling without unnecessary exposure to end users, and policy-driven session control for critical administrative activities. Its architecture is suited for enterprise environments that require centralized privileged governance across distributed infrastructure without disruptive redesign of the underlying environment.

Core Capability Areas

Privileged Access Control and Secure Session Brokering

- Enterprise Privileged Access Management solution with integrated secure session proxy for bastion-style administrative access
- Secure remote access over encrypted channels using TLS 1.2 and 1.3
- Controlled brokering of privileged sessions across critical infrastructure
- Secure session management for RDP, SSH, database, and web-based administrative access
- Live session monitoring and manual session termination by authorized administrators
- Granular command filtering and control for supported SSH and database sessions

Agentless Onboarding and Discovery

- Agentless onboarding approach for supported Windows, Linux, network, and database targets
- Protocol-based secure access without mandatory endpoint-side agent deployment
- Discovery of privileged accounts including shared, service, application, local, domain, and SSH key-based accounts
- Improved onboarding readiness through centralized visibility of privileged identities and systems
- Deployment model aligned for onboarding of minimum 500+ target systems without architectural redesign

Credential Vaulting and Password Lifecycle Management

- Secure credential vault with AES-256 encryption for privileged account password storage
- Policy-based password complexity enforcement and secure credential governance
- Automated password rotation with time-based and on-demand execution
- Controlled password retrieval through governed workflows and full audit trails
- Support for API-based credential access and controlled credential injection for applications and DevOps use cases
- Secure backup and restore of vault data with alignment to enterprise backup practices

Privileged Session Recording, Audit, and Compliance

- Full session recording using video and text-based capture, where applicable
- Searchable and indexed session activity logs for investigation and review
- Tamper-proof audit logs for administrative and user activities
- Centralized auditability for session activity, access requests, approvals, administrative changes, and policy events
- Audit-ready evidence for compliance verification, security operations, and forensic analysis

Governance, Access Approval, and Least Privilege

- Role-Based Access Control with hierarchical role definitions
- Least-privilege policy enforcement aligned to user responsibility and access scope
- Segregation of duties through role and policy assignment
- Configurable multi-level approval workflow for privileged access requests
- Just-in-Time privileged access with time-bound authorization and automatic expiry
- Controlled maker-checker style governance for sensitive privileged operations

Enterprise Identity and Security Integration

- Integration with enterprise directory services including AD and LDAP
- Support for centralized synchronization of users and groups
- MFA support through enterprise identity and authentication ecosystems including LDAP, AD, RADIUS, SAML, and OIDC-aligned models
- Integration with SIEM and SOAR platforms through Syslog and API-based mechanisms
- Integration-ready architecture for enterprise monitoring, logging, ticketing, and security operations workflows

High Availability, Scale, and Operational Readiness

- High availability architecture with local redundancy
- Support for optional DR and geographic redundancy models
- Scalable architecture aligned to support minimum 5000 users and 50 privileged administrators
- Web-based centralized administration console with secure access controls
- Rollout approach aligned to ensure infrastructure systems are integrated with PAM before production go-live
- Support for perpetual and subscription-based licensing models based on project and procurement requirements

- Minimum 5 years OEM support with 24x7x365 support coverage and software updates

Functional Coverage Snapshot

Advantal PAM is designed to help enterprises govern privileged access across the following functional areas:

- Secure privileged session proxy and bastion-style access
- Agentless onboarding of target systems
- Privileged account discovery
- AES-256 encrypted credential vaulting
- Automated password rotation and policy-based password governance
- RDP, SSH, database, and web session management
- Session recording, live monitoring, and termination control
- Command filtering and command-level policy enforcement
- RBAC, segregation of duties, and multi-level approvals
- Just-in-Time access and time-bound privileged control
- AD/LDAP integration and MFA enforcement
- SIEM, SOAR, Syslog, and API integration
- HA, DR, secure backup, and restore support
- Centralized web administration and enterprise-scale deployment

This coverage aligns to the purchaser's required PAM capability profile while preserving the authentic strengths already present in the existing Advantal PAM datasheet, including agentless access, directory integration, MFA, workflow-based approvals, session recording, AES-256 vaulting, command controls, HA/DR direction, web administration, SIEM/API integrations, and OEM-backed support.

Deployment and Support Approach

Advantal PAM is suited for enterprise environments that require controlled privileged access governance, centralized administrative visibility, and secure operational rollout. The platform supports phased onboarding, policy assignment, access validation, and privileged governance setup so that critical infrastructure access can be controlled before production use.
The solution is backed by an enterprise delivery and support approach that includes implementation alignment, long-term operational continuity, and OEM support for issue resolution, updates, and platform lifecycle support.

Why Advantal PAM

Advantal PAM combines privileged access security, operational governance, and enterprise-grade control in one unified platform. It helps organizations reduce credential exposure, secure remote administration, enforce least privilege, monitor privileged activities in real time, and maintain complete auditability across critical operations.

With support for agentless onboarding, encrypted credential vaulting, privileged account discovery, approval-based access, session recording, SIEM/SOAR integration, resilient architecture, and OEM-backed support, Advantal PAM is positioned for organizations that need secure, scalable, and compliance-ready privileged access management.

CONTACT FOR SUPPORT

Corporate Office
Unit No. 527 and 528, 5th Floor, Vipul Trade Centre, Sector 48, Sohna Road, Gurugram, Haryana – 122018, India

Development Center
17-A, Electronic Complex, Pardesipura, Indore - 452010, Madhya Pradesh

For Sales Assistance
sales@advantal.net

kartikay.shukla@advantal.net
+91-9971161261

www.advantaltechnologies.com