sectona

DATASHEET

Privileged Access Management

Secure every privileged identity across On-Premises, Cloud, and DevOps environments.

Sectona's Privileged Access Management (PAM) solution enables CISOs and security teams to secure modern enterprise infrastructure and gain complete visibility into privileged usage with a suite that is scalable and faster to deploy than legacy providers, preventing breaches and ensuring compliance.

Legacy Security Architectures Cannot Protect Modern Dynamic Enterprise Environments.

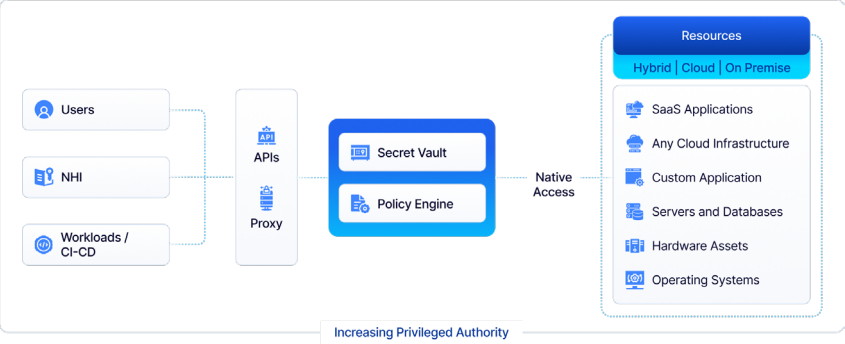
Privileged Access Gaps and Security Blind Spots

- Limited visibility into ephemeral and non-human identities creates persistent blind spots.
- Lack of phased PAM leaves overprivileged human, machine, and workload identities unmanaged.
- Retrofitted PAM stacks are clunky, fragmented, and slow to deploy at scale.
- Rigid APIs and integrations increase overhead, delay deployments, and expose credentials.

Ahead of the Curve. Scalable. Compliant. Simple.

Sectona is Purpose-Built for the Modern Enterprise.

- Scale effortlessly with Sectona's lightweight and integrated console that secures passwords, secrets, and cross-platform access seamlessly across cloud and hybrid environments.
- Get compliant quickly with Sectona's automated compliance reporting, dynamic policy controls, privilege elevation, and continuous resource discovery, all aligned with standards like ISO 27001 and NIST.
- Deploy quicker through Sectona's simplified onboarding, single-console management, and rapid implementation that outpaces other bulky incumbent vendors.



Core Capabilities

Continuous Discovery and Onboarding

- **Discovery Intelligence and Scheduling:** Tailored methods for specific environments/assets; supports periodic/on-demand scanning of assets and privileged accounts.
- **Privileged and Service Account Discovery:** Identifies all privileged users, SSH keys, service accounts, orphaned/unmanaged accounts, and dependencies for policy assignments and password changes.
- **Automated Onboarding and Governance:** Discovery policies auto-onboard accounts into PAM and auto-assimilate passwords into the vault.

Session Management

- **Session Monitoring, Control, and Policy Enforcement:** Live monitoring, playback, keystroke logging, real-time admin termination; granular policies (MFA, file size limits, command/keystroke allow/deny, whitelist/blacklist for high-risk actions); configurable timeouts.
- **Logging, Audit, and Compliance:** Exportable video recordings, vaulted command logs/metadata (admin-inaccessible); tamper-proof, write-once encrypted repositories separate from targets; searchable audits by user, asset, session attributes, timeframe.
- **Threat Analytics, Detection, and Automated Response:** Privileged Threat Analytics engine profiles sessions, assigns risk scores, applies risk-based models for prioritised investigations; detects brute force, out-of-PAM access; automates remediation (kill sessions, lock accounts, SOC alerts); Windows/Unix agents detect out-of-PAM access.

Specifications

Discovery Coverage: Automatically scans OS and assets (AWS, Microsoft Azure, Google Cloud, VMware, Hyper-V, SNMP discovery, VMware ESX/ESXi managed guest OS, network devices*). Discovers accounts across AD, Windows, Unix, Linux, hypervisors, AWS, GCP, databases, and standard devices.

Encryption and Key Management: Unique random salt per entry; AES-256 and RSA-2048 encryption for data at rest/in transit; integrates with HSMs/ external key vaults (e.g., Utimaco, Thales, Gisa*).

Authentication and Access Methods: Vaulted, auto-rotated credentials for primary authentication to assets. Supports protocol-driven, browser/ native access for RDP, SSH, Telnet, FTP, SFTP, SCP, HTTP, PowerShell, and popular SQL databases*.

Application Launcher and Thick-Client Workflows: Launches specialised clients (SQL Server Management Studio, Oracle SQL Developer, MySQL Workbench, VMware vSphere Client*) via custom launchers from the PAM console. Supports thick clients on a dedicated secure Terminal Server.

Primary Authentication Methods: Supports AD, SAML, LDAP/LDAPS, RADIUS, local, PKI/smartcard, Web SSO, username/password, Windows authentication, and RSA SecurID*.

DevOps Integrations: Jenkins, Ansible, Terraform, Kubernetes, GitHub*.

High Availability and Backup: Geo-replication of vaults/session data. Automated failover. Backup/vault encryption.

Credential Vaulting and Management

- **Vault Design and Storage:** Built-in encrypted vault with internal MySQL storage (no external vault required); centralised, auto-hardened repository for access keys, secret keys, privileged passwords, SSH keys, API tokens, certificates.
- **Access Control, Auditing, and Policy Enforcement:** Policy/role-based access with approval workflows for password check-out; configurable duration-based password reconciliation; detailed audit trails for every password, SSH key, access key, or secret checked out/used.
- **Credential Lifecycle and Rotation:** Supports application credential management with reconciliation/rotation of dependencies; discovers/vaults service (machine-to-machine) accounts to keep credentials current/controlled.
- **Resilience, Failover, and Satellite Vault:** Failover, high availability, disaster recovery for vaults; Satellite Vault with offline real-time sync to Primary Vault, activates if Primary is unreachable due to disaster/network failure.

Access Management

- **Identity and Policy-Based Access:** Grants access by role, group, or user attributes, enforcing least-privilege; policy-driven grouping, mapping, exclusive mapping; organises accounts by asset type, name, or attributes for simplified policy application/onboarding.
- **Just-in-Time and Task-Based Privileges:** Custom just-in-time (JIT) methods (Enable/Disable, Provisioning/ De-Provisioning, Elevation) for assets; session checks record/monitor JIT-tied sessions; delegates privileged tasks (e.g., password reset, enable/disable accounts) via automation instead of full login.
- **Requests, Approvals, and Workflow Automation:** Self-service privileged access requests; configurable flows (manager-driven/automated) with multi-level approvals up to 15 levels.
- **Secure Internet-Based Remote Access:** Proxy components (WSSL) enable privileged access over the internet via HTTPS.

Authentication

- **Verification Methods:** OTP, hardware tokens, push notifications, biometrics, FIDO2.
- **Adaptive/Context-Aware Policies:** Based on IP/IP zone, time, launcher, geo-location, and device type; context factors include location, time, and device.

Dashboards and Reports

- **Reporting and Export Features:** Evidence-ready audit summaries (who approved access/when); scheduled exports in PDF, Excel, CSV.
- **Visualisation and Dashboards:** Customisable real-time dashboards with asset/account/activity summaries, stakeholder insights (risk stats, user activity) viewable by roles; detailed reports with risk classification for orphaned/unmanaged accounts.

Unlock Instant Value

Governance Module

- **Access Control Policies:** Defines who/what/when/how access; enforces separation of duties.
- **Access Approval and Management:** Flags/removes "granted in perpetuity" access via justification/manager approval; manager/owner approves/denies via user-friendly interface.

DevOps Module

- **DevOps and CI/CD Secret Management:** Manages CI/CD secrets via on-demand API credential injection; manages API keys, tokens, and secrets for pipelines.
- **Secret Handling Features:** Secures hardcoded secrets; secures passwords/secrets in config files, scripts, code.

Multi-Factor Authentication (MFA): Out-of-the-box MFA with adaptive secondary authentication to the Sectona portal. Integrates with Okta, Duo, OneLogin, Windows Azure MFA, and RADIUS-based 2FA*. Supports unique passwords by email, TOTP, RSA SecurID, and YubiKey*.

Ticketing and Workflow Integration: Automated workflows; automatic ticket linking with ServiceNow and Jira*.

Alerts and Notifications: Configurable for predefined events (e.g., critical commands); parameterised filters (command type/pattern, device, privileged account); email notifications.

Compliance and Auditing: Built-in PCI-DSS and ISO 27001* reports that show organisational compliance with a single click.

SIEM Integration: Supports ArcSight, QRadar, Splunk, AlienVault, and RSA NetWitness*. Generates syslog for any SIEM.

Architecture: Clustered, microservices-based enterprise architecture. Agent-based/agentless/hybrid PAM models. Horizontal/vertical scaling. Lightweight resource usage.

Deployment: On-prem/hybrid/SaaS/multi-cloud (AWS/Azure/GCP)/virtual for remote/dynamic workloads. Centralised management and unified platform with integrated modules. Distributed HA (multi-site/cloud, replication, failover; central/regional auth control).

The tools and technologies marked with an asterisk (*) in the specifications are not an exhaustive list.

sectona

Sectona is an infrastructure security platform that neutralises privileged account risks across hybrid data centers, multicloud environments, endpoints, remote workforces, and machine-to-machine communications. Our unified suite PAM (privileged access management), CAM (cloud access management), and EPM (endpoint privilege management) deliver zero-trust protection for dynamic enterprise access.

For more information, visit www.sectona.com and follow @Sectona on LinkedIn.