HyperSDK

Security & Compliance

Enterprise-grade security built into every layer. PAM authentication, RBAC, audit logging, secrets management, and compliance-ready architecture.

Defense in Depth — Zero Trust — SOC2 & GDPR Ready

Security Architecture

Multi-layered security with defense-in-depth principles at every tier.

PAM Authentication

Native Linux PAM integration for user authentication. Leverages existing enterprise identity infrastructure — LDAP, Active Directory, SSSD, Kerberos.

Bcrypt Password Hashing

All passwords hashed with bcrypt (cost factor 12). No plaintext storage. Constant-time comparison prevents timing attacks on authentication endpoints.

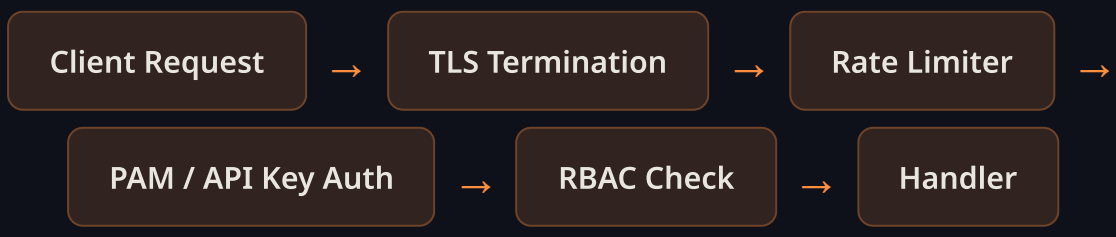
Session Tokens

Cryptographically secure session tokens with configurable TTL. Automatic expiry and renewal. Server-side session store prevents token replay attacks.

API Key Authentication

Per-user API keys for programmatic access. Key rotation support. Scoped permissions tied to RBAC roles. Revocation takes effect immediately.

Authentication Flow



> *"HyperSDK's middleware chain ensures every request passes through logging, authentication, authorization, and rate limiting before reaching any handler."*

RBAC Model

Role-Based Access Control with four predefined roles and granular permissions.

Permission	Admin	Operator	Viewer	Auditor
Browse VMs	Yes	Yes	Yes	Yes
View Job Status	Yes	Yes	Yes	Yes
Export VMs	Yes	Yes	No	No
Cancel Jobs	Yes	Yes	No	No
Configure Providers	Yes	Yes	No	No
Manage Users	Yes	No	No	No
Manage API Keys	Yes	No	No	No
View Audit Logs	Yes	No	No	Yes
Manage Secrets	Yes	No	No	No
System Configuration	Yes	No	No	No

Admin

Full system access. User management, secrets, configuration, and audit log access. Reserved for platform administrators.

Operator

Day-to-day migration operations. Can export VMs, manage providers, and monitor jobs. Cannot manage users or view audit logs.

Viewer

Read-only access. Can browse VMs and view job status. Ideal for stakeholders who need visibility without operational access.

Auditor

Compliance-focused role. Read-only VM and job access plus full audit log visibility. Designed for security and compliance teams.

Network Security

Comprehensive network-level protections against common attack vectors.

Rate Limiting

Configurable per-endpoint rate limiting via middleware. Prevents brute-force attacks on authentication endpoints and API abuse. Returns 429 with Retry-After header.

SSRF Protection

All outbound requests validated against SSRF attack patterns. Private IP ranges (10.x, 172.16-31.x, 192.168.x, 169.254.x) blocked by default for webhook targets.

TLS Encryption

TLS 1.2+ enforced for all API connections. Configurable certificate paths. Supports mTLS for provider-to-daemon communication in high-security environments.

Security Headers

Automatic injection of security headers: X-Content-Type-Options, X-Frame-Options, Strict-Transport-Security, Content-Security-Policy on every response.

Request Size Limiting

All incoming requests are size-limited at the middleware layer to prevent memory exhaustion attacks. Configurable per-endpoint limits with sensible defaults (10 MB for exports, 1 MB for API calls).

CORS Configuration

Cross-Origin Resource Sharing configured with explicit allow-lists. No wildcard origins in production. Preflight caching reduces overhead. Credentials mode

requires explicit origin matching.

> *"Every request passes through 7 middleware layers: logging, request ID, CORS, security headers, authentication, rate limiting, and request size limiting — in that exact order."*

Data Protection

Protecting sensitive data at rest, in transit, and in use.

File Permissions (0600)

All configuration files, credential stores, and exported data written with 0600 permissions (owner read/write only). No group or world access by default.

Secrets Management

Dedicated SecretManager port interface. Provider credentials stored encrypted. Support for external secret backends. Never logged, never exposed in API responses.

Audit Logging

Every authentication attempt, API call, and state change logged via the AuditLogger port. Tamper-evident log format. Configurable retention policies.

Credential Scrubbing

Passwords, API keys, and tokens automatically scrubbed from log output, error messages, and API responses. No credential leakage in stack traces.

Audit Log Entry Structure

Field	Description	Example
Timestamp	ISO 8601 UTC timestamp	2026-04-02T14:30:00Z
User	Authenticated user or API key ID	admin@corp.com
Action	Operation performed	vm.export

Resource	Target resource identifier	vm-web-prod-01
Result	Success or failure with reason	success
Source IP	Client IP address	10.0.1.50
Request ID	Unique correlation identifier	req-a1b2c3d4

Compliance Readiness

Built to meet enterprise compliance requirements across multiple frameworks.

SOC 2 Ready

Comprehensive audit logging, access controls, encryption at rest and in transit, and change management controls map directly to SOC 2 Trust Service Criteria.

GDPR Ready

Data minimization by design. No unnecessary PII collection. Audit trails support right-to-access requests. Data export capabilities for portability requirements.

ESG / Carbon Reporting

Built-in carbon-aware scheduling with quantifiable CO2 savings. Generate reports for ESG disclosures. Integration with ElectricityMap for real-time grid data.

Compliance Control Mapping

Control Area	HyperSDK Feature	SOC 2	GDPR
Access Control	RBAC, PAM, API Keys	CC6.1	Art. 32
Audit Logging	AuditLogger, Request IDs	CC7.2	Art. 30
Encryption	TLS 1.2+, Bcrypt, 0600 perms	CC6.7	Art. 32
Change Management	Job history, Manifests	CC8.1	Art. 25
Monitoring	Metrics, Alerts, Webhooks	CC7.1	Art. 33
Data Portability	Multi-format Export	--	Art. 20

Security-First Architecture

HyperSDK's hexagonal architecture ensures security is not an afterthought but a core design principle. Every port interface enforces authentication and authorization contracts.