prodactive

SMARTHUB - SYSTEM SECURITY FACT SHEET

Security posture and standards

- OWASP-aligned application security incorporating ***OWASP Top 10*** as a part of our SDLC and runtime controls
- Defence in depth and least privilege access by enabling layered controls at the application, database, and platform levels with tightly scoped ***RBAC*** permissions
- Security features are enabled out of the box; *non-optional hardening*
- *QA-focus* with vulnerability assessment planning and third-party penetration testing

Data protection and privacy

- Encryption in transit with all endpoints enforcing ***HTTPS/TLS***
- Encryption at rest with sensitive data (including API keys) using ***AES-256-GCM*** authenticated encryption. Encrypted payloads include a modern encryption approach -- *per-object IV and authentication tag* -- and are safely encoded for storage and transport.
- We only collect information required to perform core operations and functions
- ***GDPR-compliant*** deletion flows are supported
- Encryption keys are segmented per tool/key to constrain blast radius

Authentication and authorization

- RBAC refined multi-layer, plan-scoped role-based access control
  - **Plan Admin** – set up plan, user management, configure tools
  - **Plan User** – use of limited tools, access revoked to configure tools
- Function level RPC validation
- 8-hour user sessions with secure session management; *CSRF tokens generated per session* and validated across form submissions
- Password policy: 12+ characters, mixed case, numbers and symbols with weak pattern and sequence detection pattens blocked.
- **Roadmap**: **Muli-factor authentication (MFA)** via SMS, email and authentication applications

Application Security Controls

- Input validation and output encoding to prevent XSS; with **Content-Security-Policy** (CSP) headers applied.
- SQL injection prevention: All data access uses *parameterized queries* in our managed PostSQL environment.
- ***RFC 5321 aware validation*** with XSS pattern checks

Monitoring, logging, and incident response

- Audit trails provide timestamps, user agents and IPs recorded for security-relevant events such as logins, password resets, rate-limit hits, CSRF failures, invalid input, etc)
- Automated pattern analysis with allow/deny list management for suspicious activity

- Multi-layer rate limits on auth, password resets, API endpoints. Upstream DDoS protections are now in place
- 24/7 monitoring with documented response procedures; continuous security improvements and full-time functional Help Desk

Architecture, reliability and performance

- Containerized microservices isolate services to optimize resource allocation and tool high-availability
- **Load balancing** with horizontal smart scaling concepts applied
- Connection pooling and *adaptive caching* with an eviction policy tuned for predictable performance
- Strictly isolated **sandbox, beta and production** environments

Data governance and compliance

- **GDPR and CCPA** controls support *EU and California privacy requirements*
- *Row level security* enforced on sensitive tables
- Managed backups with **point in time recovery**
- Encrypted connections with service-role authentication with Enterprise-grade management features

Observability and service health

- **Real-time health checks** with execution time tracking and success rates
- Defensive error handling with detailed diagnostics

Security Roadmap

- **MFA** via SMS, email and authenticator applications
- *Machine learning based* anomaly detection
- Enhanced monitoring with **real time security dashboard**
- Additional protections on critical areas of input such as CAPTCHA, device fingerprinting, and IP reputation checks

Support and contact

- **Security contact:** security@prodactivesmarthub.com
- Please utilize Smartsheet form for **Help Desk submission** available via your Smarthub dashboard

Note on disclosure: To preserve the integrity of our defences, we do not publicly disclose infrastructure vendors, network topology, or other operational details. We are happy to provide additional information under NDA to enterprise customers during security reviews via request.