



Platform Security, Resilience & Data Assurance

TECHNICAL SECURITY OVERVIEW

Cloud Architecture · Governance · Layered Controls

For project owners, developers, and digital teams evaluating OmTrak's infrastructure, data protection standards, and security governance posture.

Powered by



ISO 27001
Certified ISMS

AWS Multi-Region
Regional Data Residency

DISP
Defence Security Program

ACSC Essential Eight
Aligned



CLOUD ARCHITECTURE

Built for Resilience. Designed for Continuity.

OmTrak is hosted on Amazon Web Services (AWS), with critical services architected across multiple Availability Zones to maintain service availability during infrastructure disruptions. Resilience, redundancy, and high availability are embedded into the platform architecture by design, rather than applied as an overlay.

For **Australian** clients operating under defence and government data handling requirements, customer data files are stored within Australian AWS regions. Backup environments are maintained in separate AWS accounts, logically and operationally isolated from production systems.

For **GCC** clients operating under government data handling requirements, customer data files are stored within AWS Middle East (UAE) region. Backup environments are maintained in separate AWS accounts, logically and operationally isolated from production systems.

Where other jurisdictions require localised storage, the same residency controls and account-level isolation can be configured within the applicable AWS region.

RESILIENCE

Critical services architected across multiple AWS availability zones within the same region. No single point of failure in platform design. High availability embedded at architecture level.

DATA RESIDENCY

Localised file storage configured per client jurisdiction. Consistent residency controls and account-level isolation applied across all supported markets.

RECOVERY

Backup environments in separate AWS accounts — isolated from production. Regular restoration testing confirms recovery readiness and validates business continuity.

SCALABILITY

AWS infrastructure scales elastically on demand. OmTrak's SaaS model requires no client-side infrastructure investment for additional users, projects, or data volume.

Account-level separation between production and backup environments means recovery infrastructure cannot be reached, degraded, or compromised by a production-side event — by design, not by configuration.

GOVERNANCE & ASSURANCE

Structured Oversight. Independently Validated.

OmTrak's security governance operates within WebFM's ISO 27001 certified Information Security Management System (ISMS), supported by alignment to the ACSC Essential Eight and active participation in the Australian Government's Defence Industry Security Program. Independent validation through penetration testing, regular security reviews, and control assessments provides ongoing assurance that controls remain effective and current.



INTERNATIONAL CERTIFICATION

ISO 27001 — Certified ISMS

WebFM holds an ISO 27001 certified Information Security Management System under which OmTrak operates. The certification is current and independently audited. Certificate details are published at OmTrak.com and available to procurement teams on request.



CYBERSECURITY FRAMEWORK

ACSC Essential Eight — Aligned

Security controls aligned to the Essential Eight — a set of baseline cybersecurity strategies developed by the Australian Cyber Security Centre (ACSC), Australia's national cybersecurity authority. Recognised internationally as a government-validated approach to reducing cyber risk across eight core control domains.



SOVEREIGN DEFENCE ASSURANCE

DISP — Australian Defence Industry Security Program

Active participation in the Australian Government's Defence Industry Security Program, administered by the Department of Defence. For government and sensitive-sector clients, DISP represents a security baseline extending beyond standard commercial compliance — assessed against sovereign defence-grade standards.

Assurance Activity	Approach	Cadence
Penetration testing	Independent third-party	Yearly*
Security control assessments	Documented, ISO-linked	Quarterly
Vulnerability management	Continuous monitoring	Ongoing
Security awareness training	Workforce-wide programme	Monthly
Phishing simulations	Targeted and varied	Regular
Restoration testing	Live recovery validation	Quarterly

* Conducted at least annually and following significant application, infrastructure, or architectural changes.



SECURITY CONTROLS

Prevent. Detect. Respond. Recover.

A four-domain control framework applied across infrastructure, cloud services, applications, and endpoints.



PREVENT

Access Control & Attack Surface Reduction

RBAC, MFA, SSO, and Conditional Access enforce least-privilege and controlled authentication

Automated security testing integrated into CI/CD pipeline at every release

WAF, network segmentation, hardening standards, and encryption reduce attack surface



DETECT

Monitoring, Visibility & Anomaly Detection

SIEM provides centralised visibility across infrastructure, cloud services, and endpoints

Cloud-native monitoring and EDR support early threat identification

Continuous monitoring and anomaly detection across all production environments



RESPOND

Incident Response & Privileged Access Control

Defined incident response, triage, and escalation processes support timely containment

Just-in-Time (JIT) access controls limit privileged exposure during operational activities

Patch management and governance maintain ongoing risk reduction between review cycles



RECOVER

Resilience Architecture & Business Continuity

AWS Regions are composed of multiple Availability Zones — maintains availability during infrastructure disruptions

Backup environments in separate AWS accounts — isolated from production at account level

Regular restoration testing confirms RTO/RPO objectives are met

DATA PROTECTION

Encryption, Identity Controls & Secure Development.

OmTrak's data protection controls span the full delivery and access lifecycle — covering encryption at rest and in transit, security embedded into the software delivery process, layered identity and access governance, and the workforce practices that maintain those controls in operation.



Data Encryption

Customer data is protected through encryption both at rest and in transit. All data stored within regional AWS environments — regardless of the jurisdiction in which it resides — is subject to the same encryption standards applied consistently across the full OmTrak platform.

Secure Development Lifecycle

Security embedded into OmTrak's delivery process — identified and remediated before deployment, not after. The CI/CD pipeline integrates automated testing at every release cycle:

SAST

Static Application Security Testing — source code analysis before build

DAST

Dynamic Application Security Testing — runtime vulnerability scanning against live instances

SCA

Software Composition Analysis — open-source dependency scanning for known vulnerabilities

Identity & Access Management

- RBAC** Role-based permissions scoped to project role and functional responsibility
- MFA** Multi-factor authentication required for access to production and sensitive systems
- SSO** Single sign-on integration supported for enterprise client environments
- Cond. Access** Policies enforced based on device posture, location, and risk signals

Workforce Security

Security awareness training and phishing simulations embedded into workforce practices — continuous maturity improvement through regular training cycles and simulated threat scenarios.

Security testing is integrated into every release cycle. Identified vulnerabilities are assessed, prioritised by risk, and tracked through to remediation as part of an ongoing improvement process.

“The end results for our clients are real time, cost saving and reduced risk. With OmTrak, there are no surprises and no information gaps and gives everyone involved a complete journey of confidence.”

STUART SMITH

Managing Director - WebFM

Supporting Documentation

 **ISO 27001 Certificate of Conformity**
Available at OmTrak.com

 **DISP Participation Confirmation**
Available on request

 **Penetration Test Summary Report**
Available on request under NDA

Global Reach

For technical enquiries, architecture questions, and data residency documentation, contact your regional WebFM representative.

Australia & South East Asia

Toll Free: 1300 135 815
Phone: 02 4655 5044

New Zealand

Phone: 0800 600 070

Middle East

Phone: +971 504 600 714

USA / Canada

Phone: 949-757-4165

UK

Phone: 020 7692 4048

