GeoEvident Security Pack

GeoEvident Security Pack (B2G/B2B)

Document version: 1.0
Last updated: 7 February 2026

Scope: This document provides a comprehensive overview of the security, deployment, and operational controls associated with **GeoEvident**, an AI-driven photo geolocation tool. This product is capable of returning location candidates such as **Hotel**, **Apartment**, or **Street View** with a structured, case-oriented workflow that is fully auditable.

Note: This Security Pack serves as informational support for customer due diligence and procurement reviews. It does not serve as a warranty or certification.

Executive Summary

GeoEvident is tailored for investigative and risk management workflows necessitating:

- **Role-based access control (RBAC)** for regulated usage
- **Auditability** for tracking actions (who did what, when, and with what result)
- **Deployment flexibility** including options for **Cloud** or **On-Premise** setups, accommodating **air-gapped/offline** environments

GeoEvident is highly applicable in public sector and regulated enterprise activities such as investigations, compliance/AML support, corporate security, insurance SIU, and vetted OSINT teams where traceability and repeatability are crucial.

Deployment Models

Cloud Deployment (GeoEvident Cloud)

Ideal for: Quick onboarding, multi-team access, and centralized operation management.

Security features:

- **RBAC** with least-privilege role allocation
- **Comprehensive audit logs** supporting investigative workflows
- **SSO availability** on specific plans using enterprise identity standards such as **SAML 2.0** and/or **OIDC**
- Tenant separation and access controls tailored to customer environment requirements

Operational features:

- Centralized administration for users, roles, and access
- Features for case workflow and evidence reporting
- Retention and export options that are configurable based on contract/deployment specifics

Shared Responsibility: In the cloud setup, GeoEvident secures the application platform, while customers manage user provisioning, access policies, and the sensitivity of submitted content.

On-Premise Deployment (GeoEvident On-Prem)

Ideal for: Environments with high sensitivity, limited connectivity, sovereignty requirements, and controlled networks.

Security features:

- **RBAC** for controlled access
- **Audit logs** for traceability
- **Network isolation**, supporting fully offline/no-internet operations
- **Offline updates** via controlled media and approved update packages
- Designed for environments requiring “air-gapped/offline” operations, common in critical/controlled networks

Customer-controlled controls:

- Physical security of the hosting environment
- Network segmentation/ACLs, endpoint hardening, and SIEM integration (where applicable)
- Backup, retention, and key management policies in alignment with internal governance

---

Identity, Access Control, and Authentication

Role-Based Access Control (RBAC)

GeoEvident employs RBAC to ensure access is restricted to authorized personnel and specific functions:

- **Admin:** Manages user/role, configures tenants
- **Analyst:** Creates cases, uploads media, conducts analyses, and generates reports
- **Viewer/Auditor:** Provides read-only access for oversight and review

RBAC is implemented to maintain least-privilege access and separation of duties.

Single Sign-On (SSO) (Cloud, select plans)

When enabled, GeoEvident supports SSO in line with common enterprise standards such as:

- **SAML 2.0** – prevalent for enterprise web SSO
- **OpenID Connect (OIDC)** – modern SSO for cloud/API-first environments

---

Audit Logs and Case Traceability

Importance of Audit Logs

Audit logging is pivotal for investigations and ensuring compliance. Industry standards emphasize the collection and retention of logs to aid in detecting, understanding, or recovering from incidents.

Content of Audit Logs

GeoEvident's audit logs are crafted to provide ample context for retrospective review. In accordance with established advice, audit records typically document:

- **What** event occurred
- **When** it occurred
- **Where** it occurred (system/component context)
- **Source** of the event
- **Outcome** of the event
- **Identity** associated with the event

Examples of Auditable Events

Common events subject to auditing include:

- Authentication events (login, logout, failed attempts)
- User and role changes (RBAC modifications, access grants/removals)
- Case lifecycle actions (case created, updated, closed)
- Evidence actions (media upload, frame extraction request, report generation)
- Export and sharing actions (case report export, evidence package creation)
- Administrative changes (retention settings, configuration changes)

Principles of Log Protection

GeoEvident adheres to best practices in security logging, which includes:

- Avoiding the logging of sensitive secrets (e.g., passwords, session tokens)
- Preserving log integrity and ensuring logs are available for investigations

---

Data Handling and Privacy

Data Processed (High Level)

Depending on the workflow and deployment, GeoEvident may handle:

- Uploaded **photos** and/or **video frames**
- Case metadata (case title, timestamps, analyst notes)
- Result objects (candidate locations, evidence match references)
- Audit log events

Data Minimization and Handling Guidance

In B2G/B2B environments, GeoEvident is designed to support regulated workflows:

- Customers should avoid submitting sensitive or classified information

unless the deployment and contract specifically support it.
- On-Prem deployments can be used for restricted environments where data must remain isolated.

Retention and Deletion

Retention policies are driven by deployment and policy. Typical capabilities include:

- Case-based retention policies aligned with customer governance
- Deletion workflows for cases and associated artifacts (where enabled)
- Backup/restore handling aligned with customer environment (especially On-Prem)

Security Operations

Vulnerability Management (Overview)

GeoEvident adheres to structured vulnerability management practices aligned with widely accepted operational guidance, including identifying, prioritizing, remediating, and verifying vulnerabilities.

Patch and Update Management (Cloud vs On-Prem)

- **Cloud:** Updates are administered through controlled release processes.
- **On-Prem:** Updates can be delivered offline.

For controlled environments, formal review of patches and assessments of applicability and risk are recommended before deployment—especially for critical networks.

Offline Updates for Air-Gapped/Isolated On-Prem

For fully isolated environments, GeoEvident supports **offline update workflows**, including:

- Customer-approved update packages delivered via controlled media
- Integrity verification of update artifacts (e.g., checksums/signatures where applicable)
- Staged rollout: from test environment to production environment
- Documented change control and update audit trail (recommended in restricted networks)

Incident Response and Support

GeoEvident's incident response strategy aligns with standard incident response lifecycle practices, including preparation, detection/analysis, containment/eradication/recovery, and post-incident improvements. NIST provides widely used guidance for this lifecycle.

Support Model Typically Includes:

- A defined security contact channel for reporting issues
- Coordinated investigation and customer communication, with scope and SLA dependent on the agreement
- Post-incident review and control improvements where applicable

---

Security "Pack" Add-ons (Available on Request)

To facilitate procurement and security review cycles, GeoEvident can provide (under NDA where appropriate):

- **Deployment hardening checklist** (Cloud and On-Prem)
- **Network requirements** (ports, inbound/outbound expectations, proxy handling)
- **Audit event catalogue** (exact event names and schemas)
- **SSO configuration guide** (when enabled)
- **Air-gapped update procedure** (offline rollout steps + integrity checks)
- **Security questionnaire response pack** (standard procurement questions)

Quick Due Diligence Answers (Procurement-Friendly)

Q: Do you support Cloud and On-Prem?
A: Yes. Cloud deployment is available for rapid onboarding, while On-Prem supports isolated and fully offline environments.

Q: Do you support RBAC?
A: Yes, for controlled access and least privilege.

Q: Do you provide audit logs?
A: Yes. Audit logs capture key user and case actions for traceability.

Q: Do you support SSO?
A: Yes, on select Cloud plans, via common enterprise identity standards such as SAML/OIDC.

Q: Can the On-Prem system run without internet?
A: Yes. On-Prem can be deployed in fully isolated networks with offline updates.

Security Contact

For security reviews, questionnaires, or responsible disclosure coordination, please contact:
contact@geoevident.com