GTT PRIVACY DATA SHEET

FOR DEFENSE HALO AI

SERVICE DESCRIPTION

GTT Defense Halo is a network defense platform delivering Services designed to reduce enterprise risk at network speed through unified network intelligence, AI-driven threat insights, and prioritized remediation.

Halo Recon – Configuration provides policy assessment via on demand analysis of Service Asset configurations. Continuous evaluation of Service Asset configuration changes comparing against known security frameworks to uncover compliance gaps. Delivers compliance AI-driven mitigation guidance.

Halo Recon – CVE provides exposure assessment by mapping CVEs to Service Assets at network speed quantifying exposure risk. Prioritizes vulnerabilities with AI recommendations.

Halo Detect provides threat detection by correlating logs and flows across Service Assets to establish behavioral baselines. Uses AI to detect anomalies at network speed and deliver risk-scored alerts before threats escalate.

Clients control alarm thresholds, notification targets, user access, approval requirements for automated response, chat retention, and participation in community threat intelligence.

For the purpose of this Privacy Data Sheet, any terms used herein shall have the same meaning as the one described under the relevant Data Processing Agreement and/or Service Schedule.

TYPES OF (CLIENT) END USER DATA

The following personal data may be included in data ingested and processed by Defense Halo, depending on the data sources the client supplies..

Input Data

Source	Personal data that may be included
Network flow telemetry	Connections, source and destination IP addresses, ports, protocols, timestamps, session duration, byte and packet volumes, location where available
System and security logs	Usernames and account identifiers, authentication events (source, destination, auth method, success or failure), privilege and group changes, admin command usage, account lifecycle events, process execution and file access attributable to a user, API key, token and service principal usage, working hours, geolocation
Asset inventory	IP address, MAC address, host name, domain name, device name, support group. Host names frequently embed employee names
Device configurations and configuration changes	Local administrator and VPN user accounts, ACLs and policy objects mapping individuals to addresses, change author identity and timestamps, secrets embedded in configuration text
Configuration import credentials	Device hostname or IP, username, API key
Identity provider claims	User ID, email address, display name, for client and GTT personnel
Notification and contact data	Email addresses, mobile numbers, webhook endpoints, user list and roles
Free text and unstructured	Any personal data the user chooses to enter. Not enumerable

Output Data

Defense Halo generates the following data from Input Data in the course of providing the service. Input Data and Outputs carry different retention periods and deletion positions.

Category	Type of End User Personal Data
User behavioural baselines	Geolocation, working hours, login pattern, device associations, application and file use, ingress and egress volumes
Risk scores	Scores at user, asset, connection and destination level, plus aggregate tenant score.*
Identity-linked anomalies	Impossible travel, brute force, privilege escalation, dormant account reactivation, geographic deviation
Entity discovery	MAC to IP mapping, host name, OS fingerprinting
Encrypted traffic analysis	TLS fingerprinting, packet length and timing patterns

**Disclaimer: This feature and the associated processing involved are not currently available. Any references to future availability are for informational purposes only and do not constitute a commitment to release the feature. Availability, functionality and timing are subject to change.*

Notes

Special category data. Defense Halo is not designed or intended to process special categories of personal data. Destination telemetry and DNS query patterns present in Input Data may nevertheless support inferences about individuals. Clients control the selection of data sources connected to Defense Halo.

Workforce monitoring. Defense Halo establishes per-user behavioural baselines and user-level risk scores (when available). Where the monitored estate includes the client's workforce, the client is responsible for satisfying applicable employee monitoring requirements, including transparency obligations and any works council or similar consultation requirements in the applicable jurisdictions.

PURPOSE OF PROCESSING (PROCESSOR)

GTT processes Client Data and creates Outputs in accordance with applicable Data Processing Agreement for the following purposes:

- **Service Provision**: Ingesting, storing and analysing telemetry from Client-designated sources; establishing tenant-specific behavioural baselines; detecting, correlating and classifying anomalies; generating risk scores, insights and recommendations; executing response actions in accordance with the Client's approval configuration; providing the Halo Portal, dashboards, reporting and Halo Chat; delivering notifications to Client-designated targets.
- **Service Management**: Tenancy, user access and entitlement administration, administered by the Client; capacity, performance and change management.
- **Technical Monitoring**: Monitoring availability, performance, integrity and security of the Halo Platform, including prevention of misuse.
- **Client Support and Troubleshooting**: Diagnosing and resolving faults, incidents and service requests, including those raised via Halo Chat.
- **Legal Compliance**: Processing strictly required by law which GTT is subject to, with prior notice to the Client unless legally prohibited.
- **Community Threat Intelligence** (opt-in only): Where the Client opts in, deriving aggregated threat indicators from the Client's tenant and contributing them to the community threat intelligence feed, as described in the relevant

Service Schedule.

Model training. GTT shall not use client personal data to train or improve other client instances of Halo Defense. Detection classifiers are trained on GTT's own data. Behavioural baselines and tenant-scoped models are generated and used solely within each client's tenancy and are deleted on termination of the Service. Any product-improvement use of client data is off by default and occurs only under a separately documented client opt-in.

DATA DELETION & RETENTION

The table below lists the applicable retention periods for each category of personal data processed by GTT in connection to the Service.

Categories of Personal Data	Retention Period
End User Client Personal Data (Input and Output data)	- Retained for only as long as necessary to provide the Services and, where applicable, for up to 30 days following termination or expiration of the Services, unless a longer retention period is required by applicable law. -

Note

For avoidance of doubt, the Retention Period specified herein does not apply to Aggregated and Anonymized Data, and to Derived Data, that are used by GTT for any lawful business purpose, including research, analytics, benchmarking, reporting, product development, and for the development, training, evaluation, and improvement of Defense Halo and of models, and GTT may derive, own, retain, and use Derived Data, including to protect GTT and its customers collectively against threats.

DATA AND STORAGE LOCATIONS, AND THIRD-PARTY SERVICE PROVIDERS (SUB-PROCESSORS)

Data and storage locations together with the list of third party service providers used in the provision of Defence Halo can be found on the Privacy Center.

Access Locations
GTT Personnel: Authorized personnel with authenticated access into the appropriate management platform located primarily in EU, UK, USA, and other approved locations. **Client**: Authorized Client employees, contractors, representatives and end-users depending on their country's location.

PERSONAL DATA TRANSFER

To ensure compliant data transfers across jurisdictions, GTT has established an Intra Group Data Transfer Agreement (IGDTA) between GTT's entities. This agreement utilizes the EU Standard Contractual Clauses and other applicable data transfer mechanisms as needed to maintain lawful and secure data processing practices.

ACCESS TO PERSONAL DATA

Users, Client, and GTT can access personal data in connection to the Service as described in the table below.

Parties with Access	Justification	Access Control
GTT personnel	Troubleshoot, support Service and report.	Corporate Credentials and MFA
Client	Through appropriate management platform with access limited to only that Client's End User Personal Data	Client Credentials and MFA (may be available depending on the technology provided)
Sub-processors (if applicable)	Troubleshoot and support Service in terms of hardware (data centers)	Corporate Credentials and MFA

Technical and Organizational Measures for Defense Halo

The technical and organizational measures specified below are specific to Defense Halo. They apply in addition to the GTT Technical and Organisational Measures ("**GTT GENERAL TOMs**") available at GTT Privacy Center. In the event of any conflict or inconsistency, in respect of Defense Halo, the measures specified below shall prevail.

1. Tenant and Model Separation

1.1. Each Instance is a client-dedicated deployment of the GTT Defense Halo software stack distinct from every other environment, including its configurations, settings, integrations, credentials, client personal data, Outputs, logs and Tenant Models.

1.2. Tenant Models are trained or tuned on Client Data (which may include personally identifiable information) solely for deployment within each client's Instance. GTT shall not use client personal data to train, tune or improve any model, behavioural baseline, profile or detection configuration made available to any other GTT customer, unless the client has expressly consented to participate in the Community Threat Intelligence.

1.3. Defense Halo supports deployment of client tenants and collectors in specified regions, including the EU, UK, US, APAC, as applicable to the specific client service configuration.

2. Encryption and Key Management

2.1. Defense Halo is designed to securely transmit client data using TLS version 1.2 or higher encryption.

2.2. All data at rest within an Instance of Defense Hali is encrypted in-line with industry best practices.

3. Pseudonymisation, Minimization and Retention

3.1. When Client opts into the Community Threat Intelligence feature(s) of Defense Halo, identifiers are pseudonymised or tokenized before contributing to the Defence Halo utilizes an autoencoder-based vector database, which stores information as high-dimensional numerical embeddings rather than the original source content. The vectorization process transforms data into a latent mathematical representation that preserves relevant patterns while removing much of the original human-readable structure. As a result, the stored vectors are not directly interpretable and serve as a pseudonymized representation of the underlying data.

4. Access Control and Authentication

4.1. All GTT personnel access to production systems and to client personal data requires multi-factor authentication integrated into GTT's SSO.

4.2. Access is granted on a role-based, least-privilege and need-to-know basis, subject to the approval, review and starters and leavers processes described in Section 3.1 of the GTT TOMs.

4.3. GTT reviews personnel privileges as appropriate to confirm that access remains aligned with assigned duties, and GTT applies starter and leaver processes designed to remove accounts that are no longer required.

5. Availability, Backup and Disaster Recovery

5.1. Defense Halo is deployed with industry best practices for resiliency and availability and operates on infrastructure designed for redundancy.

5.2. Client personal data is backed up in encrypted form. GTT tests backup restoration at least annually.

5.3. GTT maintains disaster recovery and business continuity plans.

6. Logging and Monitoring

6.1. Client access to client personal data and model artifacts is recorded in audit logs.

6.2. Defense Halo is subject to continuous security monitoring by GTT.

7. Vulnerability Management and Security Testing

7.1. GTT performs continuous vulnerability scanning of the GTT-managed infrastructure supporting the Defense Halo Services and applies security patches on a risk-assessed basis within defined timescales.

7.2. GTT applies hardening, patch management, and vulnerability management processes to Defense Halo platform components under GTT's control, including platform services, collectors, virtual firewalls, data stores, portal components, APIs, integrations, operational tooling, and supporting infrastructure.

7.3. An independent penetration test of the Defense Halo platform is performed at least annually. An executive summary of the most recent test is available to Client under confidentiality obligations upon written request.

8. AI and Model Security

8.1. General Model training and tuning are segregated from production inference environments.

8.2. GTT maintains controls designed to verify the source, traceability, and integrity of training data and any third-party models or components incorporated into Defense Halo, including a secure model release pipeline with integrity-verified model artifacts.

8.3. GTT assesses model accuracy, robustness and drift on an ongoing basis, and maintains backups of Tenant Models.

8.4. The Defense Halo chat function is clearly identified to users as an AI-based feature and displays a notice that Outputs generated through it may contain inaccuracies and should be verified before being relied upon. The form and wording of this identification and notice may be updated from time to time, provided that their substance is maintained.

8.5. Defense Halo chat function uses models designed to apply safeguards for agentic response functionality, including semantic controls between agents, strict schema-based worker-agent outputs, red-team testing for new agents, shadow-mode testing for new agents or model changes, ongoing sampled shadow-mode testing, regression testing, no persistent agent permissions, and execution of agent-generated code in ephemeral instances.

9. Secure Development and Change Management

9.1. The Defense Halo Services are securely developed in-line with security best practices.

9.2. Changes to production, including model releases, follow a documented change management process.

10. Incident Detection and Response

10.1. GTT maintains a documented security incident response plan covering Defense Halo, addressing detection, containment, eradication, recovery and post-incident review.

10.2. Personal data breaches are notified to Client in accordance with the DPA and the applicable data protection laws.

11. Data Lifecycle and Deletion

11.1. Upon termination or expiry of the applicable Service Order Form, GTT shall, at Client's election, delete client personal data, Outputs, and logs, except to the extent retention is required by applicable law.

12. Personnel

12.1. GTT personnel with access to client personal data are bound by confidentiality obligations and complete the information security and data privacy training described in Section 3.2 of the GTT GENERAL TOMs.

12.2. Relevant background checks are performed for personnel with access to production systems, to the extent permitted by applicable law.

12.3. GTT maintains a role-based AI literacy programme for GTT personnel involved in the development, operation, and support of Defense Halo. The programme is calibrated to the technical knowledge, experience and role of the relevant personnel and the context in which the AI Services are used.

13. Sub-Processors

13.1. GTT imposes on any sub-processor engaged in the processing of client personal data the same data protection obligations as those set out in the Data Processing Agreement, in accordance with Article 28(4) GDPR.

14. Review and Updates

14.1. GTT may update or modify the technical and organizational measures for Defense Halo from time to time, provided that such updates do not materially decrease the overall level of security of Defense Halo during the applicable subscription term.