NetReach Security Summary for InfoSec Review **5/12/2025**

Executive Summary

NetReach is a secure, containerized web application developed by WTI to enable centralized access and control of remote WTI units. It is hosted within Microsoft Azure and designed to meet modern InfoSec expectations for enterprise networks. NetReach uses HTTPS, supports SSO and MFA via Microsoft Entra ID, and integrates with Azure VNet for secure hybrid deployments. This document provides a comprehensive breakdown of the application's architecture, authentication, data storage, and support practices, along with controls to support security approval.

NetReach is intended for use in secure environments with private or VPN-based access to WTI hardware. It relies on Azure platform services for baseline compliance, logging, and optional integrations with enterprise monitoring and access policies. The software does not currently carry independent security certifications (e.g., SOC2 or ISO 27001), but its design supports policy-aligned deployments.

---

1. Purpose & Overview

NetReach is a containerized web application hosted on Azure App Services. It provides centralized access, control, and management of remote WTI devices over HTTPS. The app supports multiple authentication methods, role-based access, and secure communication with API-driven interactions.

Users are granted access via two roles:

- **Admin:** Full access to Admin Center and Inventory resources
- **User:** Limited to Inventory management based on Admin configuration

NetReach is designed to run within a corporate environment or via a secure Site-to-Site VPN connection, with optional custom domain or static IP.

---

2. Network Architecture & Access

- **Public Endpoint:** Accessible via the internet (Azure default domain or custom domain/static IP)
- **Private Endpoint:** Site-to-Site VPN enables secure access to on-prem WTI units
- **Port Usage:** Default HTTPS (443), configurable to alternate ports if needed by both WTI Units and NetReach
- **Isolation:** Azure VNet integration allows for subnet-level isolation

WTI units should never be exposed directly to the public internet and must be installed behind a firewall or connected via VPN.

---

3. Data Handling & Storage

- **Data Stored:**
  - Usernames and password hashes (bcrypt)
  - Configuration parameters and audit logs
  - Uploaded license required to validate subscription
- **Encryption:** NetReach encrypts user records, OAuth registration, and AppID data using AES encryption for data at rest
- **Storage Location:** Azure App Service's built-in persistent storage
- **Optional External Storage:** Azure Blob Storage or Azure Files (configurable)
- **No PII beyond usernames is stored**
- **Data Retention:** Stored indefinitely or until space constraints apply

---

4. Deployment Architecture

NetReach runs as a Linux container in Azure App Services with the following options:

- Hosted in Azure App Service (Linux container)
- VNet integrated for private access
- Supports public or private endpoints with optional custom domain/static IP
- Requires Azure Site-to-Site VPN for on-prem device access
- No additional Azure resources are required

---

5. Authentication & Access Control

- **SSO Support:** OAuth with Azure, AWS, and Google
- **Local Accounts:** Admins can create/invite local users
- **Password Storage:** bcrypt-hashed; no plaintext
- **MFA Support:** Enforced via Azure Entra ID conditional access policies
- **RBAC:**
  - **Admins:** Full control (Admin Center + Inventory)
  - **Users:** Inventory only, based on Admin-granted access
  - WTI access via token-based API, scoped by user access level

---

6. Logging & Monitoring

- **Logs Captured:**
  - Audit logs (user activity, API usage, configuration changes)
  - Auth logs (login attempts)
  - Debug logs (diagnostics)
- **Storage:** Logs stored in built-in persistent storage
- **Export:** Logs exportable via Azure Portal; can be integrated into SIEM platforms
- **Alerting:** No in-app alerts; external tools (e.g., Sentinel) required for event detection
- **Retention:** Indefinite (until storage limits reached)

---

7. Software Maintenance & Support

- **Release Cadence:** Quarterly + as-needed patches
- **Update Method:** Manual via Azure Portal (admin sets image tag to latest, then restarts app)
- **Patch Evaluation:** WTI assesses severity and deploys immediate or scheduled fixes
- **Bug Management:** Tracked by version; high-priority issues fixed in next image
- **Vulnerability Response:** Patches within 24 hours for severe cases; may take additional time if mitigation is needed

---

Appendix A: Application Roles and Access Matrix

Role	Access Area	Permissions
Admin	Admin Center, Inventory	Full management and configuration
User	Inventory only	Read/control access based on Admin policies

---

Appendix B: Authentication Flow Summary

- **SSO (OAuth)** with Azure, AWS, Google (via Entra ID)
- **Local login** (bcrypt password + optional MFA via conditional policy)
- **API access** to WTI units requires a valid token scoped by user role

---

Appendix C: Software Update Process

1. Admin accesses NetReach App Service via Azure Portal
2. Updates the container image tag under Deployment Center settings
3. Restarts the App to trigger a Docker pull from WTI Azure Registry
4. NetReach loads the new version on restart

Appendix D: WTI Point of Contact

- Andres Vargas AndresV@wti.com +1 949-421-4126

Appendix E: Version History / Change Log

Version	Release Date	Notes
1.0	[4/4/2025]	Initial internal deployment