NetReach® Security Overview

5/28/2025

WESTERN TELEMATIC INC | 5 STERLING IRVINE, CA 92618

Contents

Executive Summary

NetReach® is a secure, containerized web application developed by WTI to enable centralized access and control of remote WTI units. It can be hosted within Microsoft Azure and is 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 the Azure cloud platform that provides users with a centralized, secure interface to manage WTI units. It is API-driven and uses HTTPS for secure communications.

Access Model:
Depending on the deployment:

- **Public Endpoints:** The app, hosted in Azure App Service, is accessible directly over the internet to reach internet-hosted WTI units.
- **Private Endpoints:** For NetReach to reach on-premise WTI units, a Site-to-Site (S2S) VPN gateway connection between the on-premise network and Azure Virtual Network is required.

Data Stored:
NetReach stores limited data within Azure App Service, specifically:

- User audit logs
- Application configuration parameters
  (No sensitive customer or regulated personal data is stored.)

User, OAuth registration, and AppID data are encrypted using AES encryption.

In addition to audit logs and configuration parameters, NetReach stores the uploaded license key required to validate subscription entitlements. This key is stored securely and is required to activate and maintain functionality based on purchased licensing tiers.

User Management:
The customer is responsible for creating and managing user accounts and role-based permissions (Admin and User roles). System functionality (e.g., number of WTI units manageable) is restricted based on the validated license. Admins are responsible for uploading a valid license file issued by WTI.

Update Policy:
NetReach is updated on an "as needed" basis when bug fixes, security patches, or feature enhancements are released.

2. Risk Assessment

Availability Risks:
NetReach is hosted within Azure App Services, supporting multiple instances to improve reliability. In the event of a NetReach outage, users can still access WTI units directly using terminal emulation programs (such as Tera Term) via SSH connections.

Exposure Risks:
WTI units are **not** exposed directly to the internet.
They are expected to be installed and accessed securely behind corporate firewalls or over VPN connections, minimizing attack surface.

Authentication Risks:
NetReach relies on Azure App Services' standard protections against brute force and password attacks. No additional custom account lockout policies are implemented at the application layer.

Audit and Monitoring:
Audit logging is fully enabled for all key user activities, including login attempts, configuration changes, and API access. Logs are retained within Azure.

Backup and Recovery:
NetReach leverages Azure App Service backup features for data protection. Application configurations and logs can also be manually exported if needed.

3. Compliance Check

Regulatory Scope:
NetReach is not explicitly subject to regulatory frameworks such as ISO 27001, SOC 2, HIPAA, or CCPA. However, NetReach is aligned with common security standards to enhance deployment confidence.

Data Classification:
NetReach does **not** handle regulated data such as PII, financial, or health-related information. It only stores basic user information — namely usernames and (encrypted) passwords — along with audit logs and configuration settings.

Authentication Compliance:
NetReach supports OAuth integration with popular identity providers including **Azure AD**, AWS, and Google. This allows for seamless SSO authentication aligned with corporate identity policies.

Access Control Model:
NetReach uses a simple **role-based access control (RBAC)** structure with two roles:

- **Admin**: Full access to the Admin Center and Inventory management
- **User**: Access limited to Inventory management only
  No additional granular or read-only roles are currently implemented.

Data Retention:
NetReach does not enforce specific data retention policies. Audit logs and configuration data are retained indefinitely or until available storage capacity is exhausted. Retention policies can be introduced based on organizational requirements.

4. Deployment Architecture

Hosting Platform:
NetReach is hosted in **Azure App Service (Linux containers)**.
Azure **VNet Integration** can be configured to enable private access to on-premise WTI devices through a Site-to-Site (S2S) VPN.

Storage Backend:
NetReach uses **built-in persistent storage** within the Azure App Service environment. Optionally, it can be configured to use **external Azure storage accounts** such as Azure Blob Storage or Azure Files for expanded capacity or specific use cases.

Network Access:
NetReach can be accessed via:

- A **custom domain** (e.g., `netreach.mycompany.com`)
- A **static public IP**
- Or the **default Azure App Service URL**
  These access methods can be configured based on the deployment scenario.

Ports:
By default, NetReach communicates over **HTTPS (port 443)**.
It may also be configured to use an alternate port, provided both NetReach and the connected WTI units are set to use the same port. All communication remains encrypted.

Supporting Services:
NetReach operates as a **self-contained application**. It does **not require any additional Azure services** (e.g., Azure Key Vault, Application Gateway, Load Balancer, or Log Analytics) for core functionality. While no additional Azure services are required for base functionality, NetReach now includes a license validation mechanism based on encrypted keys issued by WTI. The license must be manually uploaded during or after deployment.

5. Authentication & Access Control

SSO Integration:
NetReach supports **OAuth-based Single Sign-On (SSO)** with Microsoft Entra ID (formerly Azure AD), AWS, and Google.
While NetReach itself does not enforce **group-based access restrictions**, organizations can apply **conditional access policies** in Microsoft Entra ID to control access based on group membership, device compliance, or location.

Local User Management:
Admins within NetReach can create and manage **local user accounts** and send invitations. This enables hybrid environments that use both SSO and local credentials.

Password Security:
Local user passwords are securely **hashed using bcrypt**, following modern cryptographic best practices. Plaintext passwords are never stored or logged.

Multi-Factor Authentication (MFA):
NetReach does not have built-in MFA enforcement but supports MFA indirectly by integrating with Microsoft Entra ID.
Admins can configure **conditional access policies in Azure AD** to enforce MFA for all users accessing NetReach.

Role-Based Access Control (RBAC):

- **Within NetReach App:**
  - **Admin Role:** Full access to Admin Center and Inventory management

  - **User Role:** Limited to Inventory-related functions, as granted by Admin Center configurations
- **Access to WTI Devices:**
  - API access to WTI units is governed by user roles assigned within NetReach (Admin Center Users)
  - These roles determine the ability to configure, manage, or control WTI devices

All access restrictions are enforced at both the **UI** and **API** layers.

6. Logging & Monitoring

Types of Logs Generated:

- **Audit Logs:**
  Capture user activities and system events within NetReach, including:
  - API requests to WTI units
  - Configuration changes
  - Device management actions
  - User login events
- **Auth Logs:**
  Record all login attempts, including successful and failed authentications.
- **Debug Logs:**
  Log application behavior for the purpose of troubleshooting and diagnostics.

Log Storage:
All logs are stored within **built-in persistent storage** inside the Azure App Service hosting NetReach. This allows for localized access and retention.

Export & Integration:
Logs can be **manually exported via the Azure portal**. There is **no built-in integration with external SIEM tools**, but exported logs can be imported into platforms like **Microsoft Sentinel or Splunk** as needed.

Alerts & Notifications:
NetReach does **not generate alerts or notifications** for security-related events such as failed logins or unauthorized access attempts.

Retention:
Logs are stored **indefinitely**, subject only to storage capacity constraints within the hosting environment.

7. Software Maintenance & Support

Release & Patching Schedule:
NetReach follows a **quarterly release cycle**, with **additional patches released as needed**, especially in response to security issues or high-priority bugs.

Update Mechanism:
Updates are applied **manually** via the **Azure Portal**:

1. Admin accesses the App Service hosting NetReach
2. Under **Deployment Center > Registry Settings**, the **Tag** is updated to the latest version
3. The NetReach App is restarted, triggering a Docker pull from **WTI's Azure Registry**
4. Admin users are **notified within the app** when a new version is available

Critical Patch Process:
WTI actively monitors for security vulnerabilities. When an issue is discovered:

- The **exploitability and impact are evaluated**
- **Immediate patches are issued** if necessary
- If an immediate patch is not feasible, **alternative mitigations** are explored

Bug & Lifecycle Management:
WTI maintains an internal **version and bug tracking system**:

- Before each production release, known bugs are reviewed
- Critical issues are prioritized for immediate fix
- Non-critical bugs are deferred to future releases
  There is no published **EOL (End-of-Life) policy** yet, but version tracking is actively managed.

Vulnerability Response Time:

- For high-severity issues, **patches may be issued within hours**
- If mitigations require further evaluation or coordination, **it may take additional time**

8. Licensing & Entitlement Control

License Enforcement:
NetReach now requires a valid subscription license to enable core functionality. WTI (the developer) generates a license key file, encrypted and bound to the subscription tier purchased by the customer. The license key must be uploaded by the customer into the NetReach Admin interface during initial setup or renewal.

License Validation:

- The encrypted license key is verified by NetReach during startup and periodically thereafter.
- If the license is missing, expired, or invalid, NetReach will restrict version updates and changes to inventory until a valid key is uploaded.
- Subscription tiers control the **maximum number of WTI units** that can be added to the inventory.

Data Protection:

- The uploaded license key is encrypted at rest using AES and is never transmitted externally.
- No personal or regulated data is embedded within the key.

Operational Dependencies:

- Manual upload of the license key is required; no online activation is used.
- The application does not contact WTI servers automatically for validation (air-gapped deployments are supported).

Support Implications:

- Customers must retain access to their license files and renew them through WTI when subscriptions expire.
- WTI will provide updated keys for subscription renewals or tier upgrades.

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 (via Entra ID), AWS, Google
- **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 Product Support Contact

- Andres Vargas - Technical Solutions Manager 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