Trojan Technologies Stream Connectivity Platform Security White Paper

Executive Overview

The Stream™ Connectivity Platform™ is Danaher and Trojan Technologies Water Intelligence System that is designed to enable organizations in the water sector to securely transform UV system operational and process data into actionable insights to drive better business outcomes. Trojan Technologies realizes that helping protect our customer's data, ensuring proper security regulations, and mitigating potential risks is essential to building trust and delivering a high level of service. Trojan Technologies takes a risk-based approach to security, and this paper details the many measures and technologies that the Stream Connectivity Platform leverages to protect our customer's data.

This document describes how the Stream Connectivity Platform addresses the fundamental objectives of information security: confidentiality, integrity, and availability, as well as Trojan Technologies approach to security architecture and our customer's responsibilities. Within this security context, we define confidentiality as our set of rules that control access to information, integrity as accuracy and trustworthiness of the information, and availability as the reliable access to information by authorized users.

Please see below for an appendix of the topics contained within:

Trojan Technologies Approach

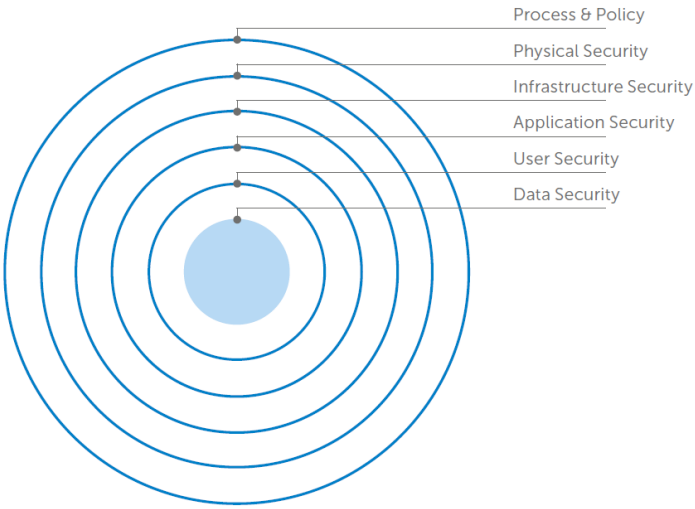
Defense-in-Depth

With the Stream Connectivity Platform, there is no the single layer that protects Customer data, but rather a well-architected solution that considers every layer from the physical security measures at the data center, all the way through the access privileges that determine what data an individual user can access. Trojan Technologies uses this multi-layered security strategy to protect customer data.

Defense-in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.
-TechTarget

Process & Policies

The first layer of defense is having a well-defined and Comprehensive set of security processes and policies to ensure the security of our customers' data and users. Trojan Technologies information security management system (ISMS) employs a number of process and policy measures that ensure security is a key priority at our core with our own people.



Training

Trojan and Danaher employees who are authorized to access the Stream Connectivity Platform undergo periodic training that allows them to be compliant with Danaher corporate security policies. For example, Development, Operations, Research & Development, and Technical Support and Services personnel, who may handle sensitive customer data and information, regularly undergo compliance and security awareness training to maintain awareness of relevant and emerging security threats.

Authorized Access

In addition to restricting personnel from entering the production area, operational access to the Stream Connectivity Platform is limited to only a restricted group of Trojan Technologies Development Operations employees. Access is controlled via the Trojan Technologies corporate network, ensuring that only personnel who are authorized can access the data. All Trojan Technologies personnel with physical or operational access to production environments are subject to training and all activities are logged for auditability.

Change Control

Trojan Technologies formal change-control process minimizes the risk associated with the Stream Connectivity Platform changes and updates. This process enables tracking of changes made to the Stream Connectivity Platform and verifies that risks have been assessed, interdependencies are explored, and necessary policies and procedures have been considered and applied before any change is authorized. Trojan Technologies documents all changes in our Release Notes, which are distributed to customers in advance of any system changes or updates.

Systems Hardening

The Stream Connectivity Platform utilizes many well-coordinated technologies to deliver our service, yet there may be many capabilities that are not required. Consistent with industry best practices, the Stream Connectivity Platform Development Operations closely inspects the entire solution to identify unnecessary services and remove and/or disable these capabilities to reduce vulnerabilities to security threats.

Periodic Vulnerability Scans & Penetration Tests

According to internal policies and international cybersecurity frameworks and standards, Trojan Technologies periodically carries out vulnerability and penetration tests covering critical security flaws, including OWASP Top 10, to stay ahead of security threats.

Security Patches

Trojan Technologies has rigorous policies and procedures in place to update all components of the Stream Connectivity Platform, including operating systems, VM (virtual machines) hypervisors, middleware, databases, mobile applications, etc. with the vendors' security patches. These security patch activities are subject to IEC62443-4-1 Secure Product Development Lifecycle auditing and are subject to rigorous standards.

Confidentiality

Authentication

The Stream Connectivity Platform architecture relies on a centralized authentication and authorization security framework to control access to the service and
the field devices. This security framework enables the enforcement of security policies by requiring password strength algorithms to
set password minimum length and complexity.

Encryption in Transit

All traffic in and out of the Stream Connectivity Platform is encrypted to provide communications security. This encryption uses a TLS/SSL (Transport Layer Security/ Secure Sockets Layer) protocol that leverages either Secure Hash Algorithm 2 (SHA-2) or Advanced Encryption Standard (AES) algorithms. This means that no data leaving or reaching one of the trusted endpoints is unencrypted anytime while traversing the internet.

Encryption at Rest

Trojan Technologies takes no risks with customer data at rest. All Stream Connectivity Platform data is stored on Microsoft Azure Servers and encrypted using AES-256 bit encryption, so even if someone were to gain access to data on the servers, it would be fully scrambled and unrecognizable.

Integrity

Controlled & Role-Based Access

All customer access to the Stream Connectivity Platform is controlled through user interfaces (UI), APIs (Application Programming Interface), and/or dedicated tools. Use of any of these methods of access requires a username and password with privileges appropriate for the requested access. Each Stream Connectivity Platform account administrator can set the permissions of user accounts, which is called Role Based Access Control (RBAC). With RBAC enforced throughout the Stream Connectivity Platform infrastructure, customers do not have root or administrative access to any portion of the Stream Connectivity Platform technology stack and access is permitted only via the Stream Connectivity Platform application layer (UI or API).

Application Access

Customer data may only be accessed through the Stream Connectivity Platform application. Whether this access is through the user interfaces or through available APIs, it enforces RBAC to regulate access to the customer data only by authorized users and personnel. As such, the Stream Connectivity Platform does not provide direct access to any databases. This approach prevents unauthorized services or systems from accidentally or maliciously retrieving or modifying customer data.

Communication

All communication to the Stream Connectivity Platform is initiated by the field devices, so that the customer can track all communication attempts from their own network to the outside world and add extra security measures to their surrounding network. Every communication attempt to and from field devices to the Stream Connectivity Platform data is validated for authenticity.

Firewalls

All network access from and to the field devices is protected by a multi-layered firewall operating in a deny-all mode. Internet access is only permitted on explicitly opened ports for only a subset of specified virtual hosts. For an additional layer of security, all database servers reside behind an additional firewall.

Unnecessary Ports and Services

Any ports, and services on any server and embedded field devices that are not required for the operation of the Stream Connectivity Platform are disabled, thereby eliminating additional opportunities for external intrusion. **When access to the Stream Connectivity Platform is implemented using a cellular mode, (default), no ports or access is made to the customer network.** When access to the Stream Connectivity Platform is implemented using the customer network, the following table provides an overview of the ports and services that the Stream Connectivity Platform utilizes:

PORT	DIRECTION	SERVICE	PURPOSE
1194 (UDP)	Outgoing	VPN	Secure Trojan traffic by way of an encrypted Openssl VPN tunnel. Used for remote device monitoring, OS security updates and configuration updates.
5671 (TCP)	Outgoing	AMQPS	Secure messaging traffic from the edge-gateway device to the Stream Connectivity Platform using AMQPS messaging protocol with TLS. Used to securely push the data collected at the location to the Stream Connectivity Platform.
123 (TCP)	Outgoing	NTP	Allow the edge-gateway the ability to sync it's time against an external time server source.
53 (UDP) *if local dns not available	Outgoing	DNS	Requires an external DNS service unless one can be used from the local network. Such as in the case of a dns host being returned from a local dhcp server IP negotiation request. If the device is setup to be a static IP and a local dns is not available, the edge-gateway would need to have this port open. This is used to resolve the Stream Connectivity Platform service hosts that port 5671 will send the data collected to.
443 (TCP)	Outgoing	HTTPS	Provide the ability to update the agent containers using TLS (transport layer security).and access Stream Connectivity Platform UI if required
44818 (TCP)	Outgoing (on local LAN only)	PLC EtherNet/IP	Explicit messaging to the PLC IP to monitor tag information and settings. (already existing on UV system network)

Availability

Microsoft Azure

The Stream Connectivity Platform leverages Microsoft Azure cloud computing for delivering its services, therefore all Stream Connectivity Platform customers are benefit from the Microsoft Azure Service Level Agreement (SLA), which commits to 99.95% or higher uptime of all major Azure services.

Infrastructure

Between the physical data center layer and the Stream Connectivity Platform application layer is the infrastructure that supports our solution. Throughout the infrastructure, security is implemented in a comprehensive and coordinated fashion to enhance the security of customer data.

Compliance

To help our customers comply with national, regional, and industry-specific requirements governing the collection and use of individual's data, Microsoft Azure offers the most comprehensive set of compliance offerings of any

industry-standard cloud service provider. All Microsoft Azure data centers are certified against leading information security standards, which are listed in the following table:

CDSA	Azure is certified to the Content Delivery and Security Assoc. Content Protection and Security standard.
CSA STAR Attestation	Azure and Intune were awarded Cloud Security Alliance STAR Attestation based on an independent audit.
GxP	Microsoft cloud services adhere to Good Clinical, Laboratory, and Manufacturing Practices (GxP).
ISO 9001	Microsoft is certified for its implementation of these quality management standards.
ISO 20000-1:2011	Microsoft is certified for its implementation of these service management standards.
ISO 22301	Microsoft is certified for its implementation of these business continuity management standards.
ISO 27001	Microsoft is certified for its implementation of these information security management standards.
ISO 27017	Microsoft cloud services have implemented this Code of Practice for Information Security Controls.
ISO 27018	Microsoft was the first cloud provider to adhere to this code of practice for cloud privacy.
MPAA	Azure successfully completed a formal assessment by the Motion Picture Association of America.
Shared Assessments	Microsoft demonstrates alignment of Azure with this program through the CSA CCM version 3.0.1.
SOC 1	Microsoft cloud services comply with Service Organization Controls standards for operational security.
SOC 2	Microsoft cloud services comply with Service Organization Controls standards for operational security.
SOC 3	Microsoft cloud services comply with Service Organization Controls standards for operational security.
WCAG 2.0	Microsoft cloud services comply with the Web Content Accessibility Guidelines 2.0.

Regional Deployments

Microsoft Azure has more global regions than any other cloud provider—offering the scalability needed to bring the Stream Connectivity Platform applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers. To help customers keeping their data sovereignty and comply with regional regulations, Trojan Technologies uses Microsoft Azure data centers for customers in their regions, or as close as possible. Currently Trojan Technologies utilizes Microsoft Azure Data Center regions in Eastern US and Western EU.

All of these data centers also feature N+1 redundant HVAC and uninterruptible power supply (UPS).

The physical security adheres to the best practices in the industry and includes:
• Keycard protocols, biometric scanning protocols, and around-the-clock interior and exterior surveillance
• Access limited to authorized data center personnel – no one can enter the production area without prior clearance and appropriate escort
• Every data center employee undergoes thorough background security checks

Customer Responsibilities

Controlled Access & Setup

In order for Trojan Technologies to keep data secure, we also expect our customers to maintain security standards. Trojan Technologies relies on our customers to ensure that each Stream Connectivity Platform account is set up with the appropriate permissions and access for each user. It is incumbent on each customer to identify who within the plant has administrative access and manage those accounts over time.

Physical Protection

Customers are responsible for the physical protection of their Trojan Technologies system and security infrastructure. Each plant is responsible for its controlled access to the plant, relevant Trojan Technologies devices (e.g. controllers and sensors) and communications networks.

Connectivity

Trojan Technologies system connectivity to the Stream Connectivity Platform at each customer site is the responsibility of the customer. For the Stream Connectivity Platform to work effectively, the instrumentation typically requires a cellular or network connection that the customer must maintain and sufficiently protect