Axonius Cybersecurity

Asset Management Platform v4.0-f

Security Target

Version 1.0

3 February 2022

Prepared for:

AXONIUS

Axonius Federal Systems LLC
330 Madison Ave 39th Floor
New York, NY 10017

Prepared by:

leidos

Accredited Testing and Evaluation Labs
6841 Benjamin Franklin Drive
Columbia, MD 21046

Contents

Tables

1 Security Target Introduction

The Security Target (ST) contains the following additional sections:

- Product and TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)
- TOE Usage of Third-Party Components (Appendix A)
- Axonius Supported Adapter Data Sources (Appendix B)

1.1 Security Target, TOE and CC Identification

ST Title – Axonius Cybersecurity Asset Management Platform v4.0-f Security Target

ST Version – Version 1.0

ST Date – 3 February 2022

TOE Identification – Axonius Cybersecurity Asset Management Platform v4.0-f

The specific tested version was 4.0.11-f. In the evaluated configuration, the product is a containerized application using Docker, which in turn runs on Ubuntu Linux 16.04. Evaluation testing included:

- Docker runtime engine v19.0.3
- VMware ESXi 6.5
- AMD Ryzen Threadripper 1950X (Zen microarchitecture) processor.

TOE Developer – Axonius Federal Systems LLC

Evaluation Sponsor – Axonius Federal Systems LLC

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- *Protection Profile for Application Software, Version 1.3, 01 March 2019* (App PP) with the following optional and selection-based SFRs:
    - FCS_CKM.1(1)
    - FCS_CKM.1(2)
    - FCS_CKM.1(3)
    - FCS_CKM.2
    - FCS_COP.1(1)
    - FCS_COP.1(2)
    - FCS_COP.1(3)
    - FCS_COP.1(4)

  - FCS_HTTPS_EXT.1/Client
  - FCS_HTTPS_EXT.1/Server
  - FCS_RBG_EXT.2
  - FIA_X509_EXT.1
  - FIA_X509_EXT.2
  - FPT_TUD_EXT.2

- *Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019* (TLS Package) with the following optional and selection-based SFRs:

  - FCS_TLSC_EXT.1
  - FCS_TLSC_EXT.5
  - FCS_TLSS_EXT.1

- *Extended Package for Secure Shell (SSH), Version 1.0, February 19, 2016* (SSH Package) with the following optional and selection-based SFRs:

  - FCS_COP.1(1)/SSH
  - FCS_SSHC_EXT.1

- The following NIAP Technical Decisions have been accounted for in the ST development and the conduct of the evaluation and apply to the ST unless otherwise identified as not applicable:

  APP PP

  - TD0601: X.509 SFR Applicability in App PP
    This TD modifies FTP_DIT_EXT.1.1, FCS_HTTPS_EXT.* and FIA_X509_EXT.1
  - TD0600: Conformance claim sections updated to allow for MOD_VPNC_V2.3
    This TD allows for an additional PP-Module to be specified in a PP-Configuration with the App PP. This PP-Module is not specified in this ST and therefore the TD is not applicable.
  - TD0598: Expanded AES Modes in FCS_COP for App PP
  - TD0582: PP-Configuration for Application Software and Virtual Private Network (VPN) Clients now allowed
    This TD allows for a PP-Configuration that includes the VPN Client PP-Moduleand changes the File Encyption EP reference to the PP-Module for File Encryption. These modules are not claimed in the ST and therefore the TD is not applicable.
  - TD0561: Signature verification update
  - TD0554: iOS/iPadOS/Android AppSW Virus Scan
  - TD0548: Integrity for installation tests in AppSW PP 1.3
  - TD0544: Alternative testing methods for FPT_AEX_EXT.1.1
  - TD0543: FMT_MEC_EXT.1 evaluation activity update
    This TD is not applicable because it modifies an evaluation activity for Windows, the TOE runs on a Linux platform
  - TD0519: Linux symbolic links and FMT_CFG_EXT.1
  - TD0515: Use Android APK manifest in test
    This TD is not applicable because the TOE does not run on Android.
  - TD0510: Obtaining random bytes for iOS/macOS
    This TD is not applicable because the TOE does not run on iOA/macOS.

- TD0498: Application Software PP Security Objectives and Requirements Rationale
- TD0495: FIA_X509_EXT.1.2 Test Clarification
- TD0465: Configuration Storage for .NET Apps
  Modifies an Evaluation Activity for Windows apps. The TOE is a linux app and therefore this TD does not apply.
- TD0445: User Modifiable File Definition
- TD0437: Supported Configuration Mechanism
- TD0435: Alternative to SELinux for FPT_AEX_EXT.1.3
- TD0434: Windows Desktop Applications Test
  This TD modifies an Assurance Activity for Windows Desktop Applications. The TOE is a linux application and therefore the TD does not apply.
- TD0427: Reliable Time Source
- TD0416: Correction to FCS_RBG_EXT.1 Test Activity

TLS PKG

- TD0588: Session Resumption Support in TLS package
- TD0513: CA Certificate loading
- TD0499: Testing with pinned certificates
- TD0469: Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1
- TD0442: Updated TLS Ciphersuites for TLS Package

SSH EP

- TD0598: Expanded AES Modes in FCS_COP for App PP
- TD0446: Missing selections for SSH
- TD0420: Conflict in FCS_SSHC_EXT.1.1 and FCS_SSHS_EXT.1.1
- TD0332: Support for RSA SHA2 host keys
- TD0331: SSH Rekey Testing
- TD0240: FCS_COP.1.1(1) Platform provided crypto for encryption/decryption

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
  - Part 3 Extended
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019
  - Package Conformant
- Extended Package for Secure Shell (SSH), Version 1.0, 19 February 2016
  - Package Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. An iterated SFR is indicated by a number in parentheses placed at the end of the component. For example, FCS_COP.1(1) through FCS_COP.1(4) indicate that the ST includes four iterations of the FCS_COP.1 requirement: (1), (2), (3), and (4). Additionally, iterations can be differentiated using a slash ('/') followed by a description. For example, FCS_COP.1(1)/SSH identifies an iteration of FCS_COP.1 specifically for the SSH protocol.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows technical changes to a requirement to make it more restrictive and allows non-technical changes to grammar and formatting. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that minor grammatical changes that do not involve the addition or removal of entire words (e.g., for consistency of quantity such as changing "meets" to "meet") do not have formatting applied.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.
- The ST does not show operations that have been completed by the PP authors, though it does preserve brackets to show where such operations have been made.

1.3.1 Terminology

The following terms and abbreviations are used in this ST:

Table 1: Terms and Definitions

Term	Definition
Adapters	Axonius integration-specific code that allow the TOE to connect to various target data sources to fetch and process data.
Data Correlation	The process of identifying which two bits of data from separate sources but referring to the same property (e.g. a MAC address) is "correct". The process provides an "aggregated" view of metadata about each asset that includes the most accurate version of all reported information known about an asset as reported by multiple third-party systems.
GNU Privacy Guard (GnuPG or GPG)	A free-software replacement for Symantec's PGP cryptographic software suite. GNU Pirvacy Guard is an implementation of the OpenPGP standard (Pretty Good Privacy) and is included in Ubuntu and other Linux distributions.

1.3.2 Acronyms

Table 2: Acronyms

Term	Definition

API	Application Programming Interface
AES	Advanced Encryption Standard
ASLR	Address Space Layout Randomization
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CCECG	Common Criteria Evaluated Configuration Guidance
CEM	Common Evaluation Methodology for Information Technology Security
CN	Common Name
CTR	Counter (cryptographic mode)
CVE	Common Vulnerabilities and Exposures
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman (Ephemeral)
ECDSA	Elliptic Curve Digital Signature Algorithm
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GB	Gigabyte
GCM	Galois/Counter Mode
GPG	GNU Privacy Guard
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
LUKS	Linux Unified Key Setup
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPM	Node Package Manager
OCSP	Online Certificate Status Protocol
OE	Operational Environment
OS	Operating System
PII	Personally Identifiable Information
PP	Protection Profile
RAM	Random Access Memory
RPC	Remote Procedure Call
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAN	Subject Alternative Name

SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

2 Product and TOE Description

2.1 Introduction

The Axonius Cybersecurity Asset Management Platform (Axonius or the TOE) is a containerized software application designed to give the organization a comprehensive inventory of its IT assets, uncover cybersecurity coverage gaps, and enforce security policies. The solution connects to the organization's existing data sources to retrieve information about assets such as devices and users. It stores the relevant details locally, correlating the data across different sources to provide the organization with a comprehensive and accurate inventory and perform security gap analysis and remediation tasks.

2.2 Product Overview

Outside of its core platform functionality, Axonius integration-specific code, referred to as "adapters", connect to various target data sources to fetch and process data. Each adapter encapsulates integration-specific code that Axonius created to fetch and process data corresponding to a specific data source. Adapters use SSH or HTTPS protocols wherever supported to establish a secure channel to the data source and retrieve relevant data. The configuration information for each adapter includes the hostname or IP address of the data source and the relevant access credentials.

Axonius provides a Graphical User Interface (GUI) for monitoring and management of the TOE, which users access over HTTPS. Users can also access the underlying Linux platform through SSH, however this only provides access to the host OS and not to the TOE and is therefore out of the scope of the evaluation. Axonius also provides a RESTful API Client for querying the correlated asset data. This interface does not provide any management functions to manage the TOE and is excluded from the evaluation.

2.3 TOE Overview

The Target of Evaluation (TOE) for the Axonius Cybersecurity Asset Management Platform consists of the mandatory functionality prescribed by the App PP and TLS/SSH Packages, as well as some selection-based functionality where needed.

The logical boundary is summarized in section 2.4.2 below. In general, the following Axonius capabilities are considered to be within the scope of the TOE:

- **Protection of sensitive data at rest:** the TOE uses encryption to protect credentials.
- **Protection of data in transit:** the TOE secures data in transit between itself and its operational environment using HTTPS/TLS and SSH.
- **Trusted updates:** the TOE provides visibility into its current running version and the vendor distributes updates to it that are digitally signed so that administrators can securely maintain up-to-date software.
- **Security Management:** the TOE provides a Web GUI to administer its security functions.
- **Cryptographic services:** the TOE includes an implementation of OpenSSL with NIST-approved algorithm services that it uses to secure data at rest and in transit.
- **Secure interaction with operating system:** the TOE is designed to interact with its underlying host operating system platform in such a way that the TOE cannot be used as an attack vector to compromise an operating system.

The TOE's data collection, analysis, and automated response capabilities are outside the scope of the TOE (aside from the trusted channels used to communicate with the assets), as is any other product behavior that is not described in the App PP or TLS/SSH Packages.

2.4 TOE Architecture

The Axonius Cybersecurity Asset Management Platform v4.0-f TOE is a Linux-based containerized software application written in Python (both versions 2 and 3) and includes the Python Cryptography library that uses CAVP validated OpenSSL FIPS Object Module (FOM) for its cryptographic functionality. JavaScript version ES6 is used for the web app's front end and nginx as its web server. The embedded Python Paramiko module is used for the SSHv2 implementation. The embedded Python Secrets module provides random number generation services. The TOE includes a MongoDB database running within its own Docker container for secure storage of credentials. Both modules and the database use the FOM for cryptographic primitives. The FOM is included with the TOE.

Axonius integrates with numerous security and management solutions or assets on a network that are referred to as adapter data sources. Outbound connections to data sources are secured using HTTPS or SSH. In the evaluated configuration, unsecured connections to data sources should not be used. All management of the TOE is done through the GUI, which is protected by HTTPS/TLS.

The TOE is supported on a Ubuntu Linux-based virtualized appliance platform with Linux Unified Key Setup (LUKS) and uses Docker to run its containerized applications. In the evaluated configuration, the TOE runs on a virtual machine with Ubuntu 16.04 and Docker runtime engine v19.0.3 on ESXi 6.5 on AMD Ryzen Threadripper 1950X (Zen microarchitecture).

2.4.1 Physical Boundary

The TOE consists of the following components:

- Axonius Cybersecurity Asset Management Platform v4.0-f, including:
  - MongoDB database v4.2.8
  - OpenSSL 1.0.2 with the FIPS Object Module 2.0.16
  - Nginx openresty/1.15.8.1rc1.

The TOE consists of exactly one instance of the Axonius Cybersecurity Asset Management Platform provided as either a .deb file or a .deb file packaged as an OVA file.

The TOE has the following minimum system requirements for its VMware ESXi Virtual Machine:

- 8 CPU cores
- 32 GB RAM
- 500 GB Hard Drive (SSD is strongly recommended for better performance)
- Dynamic or static IP address.

These system requirements reflect the lightest usage scenarios for the TOE. Additional factors such as network size and storage retention requirements will affect the system requirements for a particular deployment. Refer to the relevant TOE documentation (as referenced in section 2.5) for the specific system requirements that apply to a given deployment.

The TOE's operational environment includes the following:

- Platform (hardware and software) on which the TOE is hosted.
    - Ubuntu 16.04 OS
    - Docker runtime engine v19.0.3
    - VMware ESXi 6.5
    - AMD Ryzen Threadripper 1950X (Zen microarchitecture)
- Web browser, used to access the GUI interface (Chrome v84 and Firefox v79 are vendor tested).
- One or more adapter data sources as identified in Appendix B.

2.4.2 Logical Boundary

This section summarizes the security functions provided by the TOE:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels.

2.4.2.1 Cryptographic Support

The TOE implements cryptography to protect data at rest and in transit.

For data at rest, the TOE securely stores the credential data used to log in to the TOE, private keys, as well as adapter credentials that the TOE uses to authenticate to adapter data sources. This stored data is encrypted/hashed using either PBKDF2_HMAC with SHA512 and 100,000 rounds in conjunction with LUKS or using MongoDB's Client-Side Field Level Encryption (AES-256-CBC).

For data in transit, the TOE implements HTTPS and TLS as both a client and a server. The TOE implements a HTTPS/TLS server for its administrative interface while it implements either an SSH Client or a HTTPS/TLS client to communicate with any data sources connected to it. The TOE does not support mutual authentication.

The TOE implements all cryptography used for these functions using its own OpenSSL with CAVP validated algorithms. The TOE's DRBG is seeded using entropy from the underlying OS platform.

2.4.2.2 User Data Protection

The TOE protects sensitive data in non-volatile memory using approved cryptographic algorithms and by leveraging LUKS functionality provided by the host platform.

The TOE relies on the network connectivity capabilities of its host OS platform. The TOE supports user-initiated and application-initiated uses of the network.

The TOE does not access any of the sensitive information repositories on the host platform.

2.4.2.3 Identification and Authentication

The TOE supports X.509 certificate validation as part of establishing TLS and HTTPS connections. The TOE supports various certificate validity checks and checks certificate revocation status using OCSP. If the certificate is invalid or the revocation status of a certificate cannot be determined, the certificate will not be accepted.

2.4.2.4 Security Management

The TOE itself and the configuration settings it uses are stored in locations recommended by the Linux platform vendor.

The TOE includes a web GUI. This interface enforces username/password authentication using locally stored credentials that are created using the TOE. The TOE does not include a default user account to access its management interface.

The security-relevant management functions supported by the TOE relate to configuration of adapters and certificates.

2.4.2.5 Privacy

The TOE does not collect or transmit personally identifiable information (PII) of any individuals.

2.4.2.6 Protection of the TSF

The TOE enforces various mechanisms to prevent itself from being used as an attack vector to its host OS platform. The TOE runs on top of the host operating system as a series of Docker containers containing Python and JavaScript code, and does not explicitly require disabling built-in operating system controls for any reason (e.g. those built into Ubuntu 16.04). As such, the TOE relies on the operating system to handle sensitive low-level operations such as memory mapping, and is compatible with Ubuntu 16.04, including when AppArmor is enabled on the host OS. The TOE is interpreted code and not just-in-time compiled and therefore compiler flags to enforce ASLR are not necessary. The TOE also does not use both PROT_WRITE and PROT_EXEC on the same memory regions. There is no situation where the TSF maps memory to an explicit address.

The TOE does not use any undocumented platform APIs and no system calls are directly invoked in Axonius code. The TOE is entirely Dockerized Python/JavaScript, so all calls are indirect.

The TOE has a mechanism to determine its current software version. Software updates to the TOE can be acquired by leveraging its OS platform. All updates are digitally signed to guarantee their authenticity and integrity.

The TOE developer has internal mechanisms for receiving reports of security flaws, tracking product vulnerabilities, and distributing software updates to customers in a timely manner.

2.4.2.7 Trusted Path/Channels

The TOE encrypts sensitive data in transit between itself and its operational environment using TLS, HTTPS, or SSH.

2.5 TOE Documentation

Axonius provides the following product documentation in support of the installation and secure use of the TOE:

- Axonius Cybersecurity Asset Management Platform v4.0-f Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0

3 Security Problem Definition

This ST includes by reference the Security Problem Definition, composed of threats and assumptions, from the App PP, including the inclusion of A.PLATFORM as required by TD0427. The Common Criteria also provides for organizational security policies to be part of a security problem definition, but no such policies are defined in the App PP.

As functional/extended packages, the TLS/SSH Packages do not contain a Security Problem Definition. The TOE's use of TLS/SSH is intended to mitigate the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats defined by the App PP.

The PP's offer additional information about the identified threats, but that has not been reproduced here and the PP's should be consulted if there is interest in that material. In general, the PP's have presented a Security Problem Definition appropriate for application software, and as such is applicable to the Axonius Asset Management Platform TOE.

4 Security Objectives

As with the Security Problem Definition, this ST includes by reference the security objectives defined in the App PP. This includes security objectives for the TOE (used to mitigate threats) and for its operational environment (used to satisfy assumptions).

As functional packages, the TLS/SSH Packages do not contain a Security Problem Definition. The TOE's use of TLS/SSH is intended to satisfy the O.PROTECTED_COMMS objective of the App PP by implementing a specific method by which network communications are protected.

5 IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the following Protection Profiles (PP) and Functional Packages:

- *Protection Profile for Application Software*, Version 1.3, March 1, 2019
- *Functional Packages for Transport Layer Security (TLS),* Version 1.1, February 12, 2019
- *Extended Package for Secure Shell (SSH),* Version 1.0, February 19, 2016.

As a result, any selection, assignment, or refinement operations already performed by that PP on the claimed SFRs are not identified here (i.e., they are not formatted in accordance with the conventions specified in section 1.3 of this ST). Formatting conventions are only applied on SFR text that was chosen at the ST author's discretion.

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the App PP and TLS/SSH Packages. These documents define the following extended SAR and extended SFRs; since they have not been redefined in this ST, the App PP and TLS/SSH Packages should be consulted for more information regarding these extensions to CC Parts 2 and 3.

Defined in App PP:

- ALC_TSU_EXT.1 Timely Security Updates
- FCS_CKM_EXT.1 Cryptographic Key Generation Services
- FCS_HTTPS_EXT.1/Client HTTPS Protocol
- FCS_HTTPS_EXT.1/Server HTTPS Protocol
- FCS_RBG_EXT.1 Random Bit Generation Services
- FCS_RBG_EXT.2 Random Bit Generation from Application
- FCS_STO_EXT.1 Storage of Credentials
- FDP_DAR_EXT.1 Encryption of Sensitive Application Data
- FDP_DEC_EXT.1 Access to Platform Resources
- FDP_NET_EXT.1 Network Communications
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication
- FMT_CFG_EXT.1 Secure by Default Configuration
- FMT_MEC_EXT.1 Supported Configuration Mechanism
- FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information
- FPT_AEX_EXT.1 Anti-Exploitation Capabilities
- FPT_API_EXT.1 Use of Supported Services and APIs
- FPT_IDV_EXT.1 Software Identification and Versions
- FPT_LIB_EXT.1 Use of Third Party Libraries
- FPT_TUD_EXT.1 Integrity for Installation and Update
- FPT_TUD_EXT.2 Integrity for Installation and Update
- FTP_DIT_EXT.1 Protection of Data in Transit

Defined in TLS Package:

- FCS_TLS_EXT.1 TLS Protocol
- FCS_TLSC_EXT.1 TLS Client Protocol
- FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension
- FCS_TLSS_EXT.1 TLS Server Protocol

Defined in SSH Package:

- FCS_SSH_EXT.1 SSH Protocol
- FCS_SSHC_EXT.1 SSH Client Protocol

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

Table 3: TOE Security Functional Components

Requirement Class	Requirement Component
FCS_FCS: Cryptographic Support	FCS_CKM.1(1) Cryptographic Asymmetric Key Generation
	FCS_CKM.1(2) Cryptographic Symmetric Key Generation
	FCS_CKM.1(3) Password Conditioning
	FCS_CKM.2 Cryptographic Key Establishment
	FCS_CKM_EXT.1 Cryptographic Key Generation Services
	FCS_COP.1(1) Cryptographic Operation – Encryption/Decryption
	FCS_COP.1(1)/SSH Cryptographic Operation – Encryption/Decryption (SSH EP)
	FCS_COP.1(2) Cryptographic Operation – Hashing
	FCS_COP.1(3) Cryptographic Operation – Signing
	FCS_COP.1(4) Cryptographic Operation – Keyed-Hash Message Authentication
	FCS_HTTPS_EXT.1/Client HTTPS Protocol
	FCS_HTTPS_EXT.1/Server HTTPS Protocol
	FCS_RBG_EXT.1 Random Bit Generation Services
	FCS_RBG_EXT.2 Random Bit Generation from Application
	FCS_SSH_EXT.1 SSH Protocol
	FCS_SSHC_EXT.1 SSH Protocol - Client
	FCS_STO_EXT.1 Storage of Credentials
	FCS_TLS_EXT.1 TLS Protocol (TLS PackageFunctional Package for TLS)
	FCS_TLSC_EXT.1 TLS Client Protocol (TLS Package)
	FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension (TLS Package)
	FCS_TLSS_EXT.1 TLS Server Protocol (TLS Package)
FDP: User Data Protection	FDP_DAR_EXT.1 Encryption of Sensitive Application Data
	FDP_DEC_EXT.1 Access to Platform Resources
	FDP_NET_EXT.1 Network Communications
	FIA_X509_EXT.1 X.509 Certificate Validation

Requirement Class	Requirement Component
FIA: Identification and authentication	FIA_X509_EXT.2 X.509 Certificate Authentication
FMT: Security Management	FMT_CFG_EXT.1 Secure by Default Configuration
	FMT_MEC_EXT.1 Supported Configuration Mechanism
	FMT_SMF.1 Specification of Management Functions
FPR: Privacy	FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information
FPT: Protection of the TSF	FPT_AEX_EXT.1 Anti-Exploitation Capabilities
	FPT_API_EXT.1 Use of Supported Services and APIs
	FPT_IDV_EXT.1 Software Identification and Versions
	FPT_LIB_EXT.1 Use of Third Party Libraries
	FPT_TUD_EXT.1 Integrity for Installation and Update
	FPT_TUD_EXT.2 Integrity for Installation and Update
FTP: Trusted Path/Channels	FTP_DIT_EXT.1 Protection of Data in Transit

5.2.1 Cryptographic Support (FCS)

5.2.1.1 FCS_CKM.1(1) Cryptographic Asymmetric Key Generation

FCS_CKM.1.1(1) The application shall [***implement functionality***

] to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- ***[ECC schemes] using ["NIST curves" P-256, P-384 and [P-521]] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4],***
- ***[FFC Schemes] using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3***

].

5.2.1.2 FCS_CKM.1(2) Cryptographic Symmetric Key Generation

FCS_CKM.1.1(2) The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [

- ***256 bit***

].

5.2.1.3 FCS_CKM.1(3) Password Conditioning

FCS_CKM.1.1(3) A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm as specified in FCS_COP.1(4), with [**100,000**] iterations, and output cryptographic key sizes [***256***] that meet the following [NIST SP 800-132].

FCS_CKM.1.2(3) The TSF shall generate salts using a RBG that meets FCS_RGB_EXT.1 and with entropy corresponding to the security strength selected for PBKDF in FCS_CKM.1.1(3).

5.2.1.4 FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 The application shall [***implement functionality***] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- ***[Elliptic curve-based key establishment schemes] that meet the following: [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"],***
- ***[Key establishment scheme using Diffie-Hellman group 14] that meets the following: RFC 3526, Section 3***
  ].

].

5.2.1.5 FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1 The application shall [***implement asymmetric key generation***].

5.2.1.6 FCS_COP.1(1) Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1(1)[1] The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm [

- ***AES-CBC (as defined in NIST SP 800-38A) mode,***
- ***AES-GCM (as defined in NIST SP 800-38D) mode,***

] and cryptographic key sizes [***128-bit, 256-bit***].

5.2.1.7 FCS_COP.1(1)/SSH Cryptographic Operation - Encryption/Decryption (SSH FPEP)

FCS_COP.1.1(1)/SSH[1] The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm [

- ***AES-CTR (as defined in NIST SP 800-38A) mode***

] and cryptographic key sizes [***128-bit, 256-bit***].

5.2.1.8 FCS_COP.1(2) Cryptographic Operation – Hashing

FCS_COP.1.1(2) The application shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [

- ***SHA-1,***

[1] Modified by TD0598. Note that TD0240 modified this SFR to allow for platform to provide the crypto but TD0598 subsequently modified this SFR to its current wording. Though there is no indication that TD0240 was superceded by TD0598, the ST author is using the wording from the most recent TD.

- ***SHA-256,***
- ***SHA-384,***
- ***SHA-512***

] and message digest sizes [

- ***160,***
- ***256,***
- ***384,***
- ***512***

] bits that meet the following: FIPS Pub 180-4.

5.2.1.9 FCS_COP.1(3) Cryptographic Operation – Signing

FCS_COP.1.1(3) The application shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- ***RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4***
- ***ECDSA schemes using "NIST curves" P-256, P-384 and [no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.***

].

5.2.1.10 FCS_COP.1(4) Cryptographic Operation – Keyed-Hash Message Authentication

FCS_COP.1.1(4) The application shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm

- HMAC-SHA-256

and [

- ***SHA-1,***
- ***SHA-384***
- ***SHA-512***

] with key sizes [**256 bits, 384 bits, 512 bits**] and message digest sizes 256 and [**160, 384, 512**] bits that meet the following: FIPS Pub 198-1 *The Keyed-Hash Message Authentication Code* and FIPS Pub 180-4 *Secure Hash Standard*.

5.2.1.11 FCS_HTTPS_EXT.1/Client HTTPS Protocol[2]

FCS_HTTPS_EXT.1.1/Client The application shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2/Client The application shall implement HTTPS using TLS as defined in the Functional Package for TLS.

[2] Modified by TD0601

FCS_HTTPS_EXT.1.3/Client The application shall [***not establish the application-initiated connection***] if the peer certificate is deemed invalid.

5.2.1.12 FCS_HTTPS_EXT.1/Server HTTPS Protocol[2]

FCS_HTTPS_EXT.1.1/Server The application shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2/Server The application shall implement HTTPS using TLS as defined in the TLS package.

5.2.1.13 FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [***implement DRBG functionality***] for its cryptographic operations.

5.2.1.14 FCS_RBG_EXT.2 Random Bit Generation from Application

FCS_RBG_EXT.2.1 The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [***CTR_DRBG (AES)***].

FCS_RBG_EXT.2.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [***no other noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

5.2.1.15 FCS_SSH_EXT.1 SSH Protocol

FCS_SSH_EXT.1.1 The SSH software shall implement SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and [***5656, 6668***] as a **[*client*]**.

5.2.1.16 FCS_SSHC_EXT.1 SSH Protocol – Client

FCS_SSHC_EXT.1.1 The SSH client shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, and [***password-based***].

FCS_SSHC_EXT.1.2 The SSH client shall ensure that, as described in RFC 4253, packets greater than [**32000**] bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.3[3] The SSH software shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-ctr, aes256-ctr, [***aes128-cbc, aes256-cbc***].

[3] TD0446 added selections but this ST does not select any of them.

FCS_SSHC_EXT.1.4[4] The SSH client shall ensure that the SSH transport implementation uses [***ecdsa-sha2-nistp256***] and [***ecdsa-sha2-nistp384***] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.5 The SSH client shall ensure that the SSH transport implementation uses [***hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512***] and [***no other MAC algorithms***] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.6 The SSH client shall ensure that [***diffiehellman-group14-sha1, ecdh-sha2-nistp256***] and [***ecdh-sha2-nistp384, ecdh-sha2-nistp521***] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.7 The SSH server shall ensure that the SSH connection be rekeyed after [***no more than 1 Gigabyte of data has been transmitted, no more than 1 hour***] using that key**.**

FCS_SSHC_EXT.1.8 The SSH client shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or [***no other methods***] as described in RFC 4251 section 4.1.

5.2.1.17 FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1 The application shall [

- ***implement functionality to securely store [adapter credentials, keys, Web GUI authentication credentials] according to [FCS_COP.1(1), FCS_CKM.1(3)]***

] to non-volatile memory.

5.2.1.18 FCS_TLS_EXT.1 TLS Protocol (TLS EP)

FCS_TLS_EXT.1.1 The product shall implement [

- ***TLS as a client,***
- ***TLS as a server***

].

5.2.1.19 FCS_TLSC_EXT.1 TLS Client Protocol (TLS EP)

FCS_TLSC_EXT.1.1[5] The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a client that supports the cipher suites [

[4] TD0446 adds a selection but this ST does not select it.

[5] This SFR is modified by TD0442 but this ST does not claim any of the selections that were added by the TD.

- ***TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***

]

and also supports functionality for [

- ***none***

].

FCS_TLSC_EXT.1.2 The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The product shall not establish a trusted channel if the server certificate is invalid [

- ***with no exceptions***

].

5.2.1.20 FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension (TLS EP)

FCS_TLSC_EXT.5.1 The product shall present the Supported Groups Extension in the Client Hello with the supported groups [***secp384r1***].

5.2.1.21 FCS_TLSS_EXT.1 TLS Server Protocol (TLS EP)

FCS_TLSS_EXT.1.1[6] The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a server that supports the cipher suites [

- ***TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289]***

and also supports functionality for [

- ***session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)***[7]

].

FCS_TLSS_EXT.1.2 The product shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [***TLS 1.1***].

FCS_TLSS_EXT.1.3 The product shall perform key establishment for TLS using [

[6] This SFR is modified by TD0442 but this ST does not claim any of the selections that were added by the TD.

[7] Modified by TD0588

- ***ECDHE parameters using elliptic curves [secp384r1, secp521r1] and no other curves ,***
- ***no other key establishment methods***

].

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_DAR_EXT.1 Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [

- ***leverage platform-provided functionality to encrypt sensitive data,***
- ***protect sensitive data in accordance with FCS_STO_EXT.1***

] in non-volatile memory.

5.2.2.2 FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [***network connectivity***].

FDP_DEC_EXT.1.2 The application shall restrict its access to [***no sensitive information repositories***].

5.2.2.3 FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- ***User-initiated communication for [access to Web GUI]***
- ***[application-initiated network communication for***
  - ***Outbound connections (HTTPS and SSH) for connecting to adapter sources,***

  ]

].

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The application shall [***implement functionality***] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field.
- The application shall validate the revocation status of the certificate using [***OCSP as specified in RFC 6960***].
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
- S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the extendedKeyUsage field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
- Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

Application Note: *The TOE does not use certificates for S/MIME, trusted updates, or executable code integrity verification; and client certificates are not presented to the TOE.*

5.2.3.2 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***HTTPS, TLS***].

FIA_X509_EXT.2.2 When the application cannot establish a connection to determine the validity of a certificate, the application shall [***not accept the certificate***].

5.2.4 Security Management (FMT)

5.2.4.1 FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application's binaries and data files from modification by normal unprivileged users.

5.2.4.2 FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1[8] The application shall [***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options***].

[8] Modified by TD0437

5.2.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [

- ***[connect adapters, upload custom certs, set hostname]***

].

5.2.5 Privacy (FPR)

5.2.5.1 FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1 The application shall [

- ***not transmit PII over a network***

].

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for [**no exceptions**].

FPT_AEX_EXT.1.2 The application shall [

- ***not allocate any memory region with both write and execute permissions***

].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

5.2.6.2 FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

5.2.6.3 FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1 The application shall be versioned with [***[semantic versioning (SemVer)]***].

5.2.6.4 FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [**list of third-party libraries in Appendix A1**].

Application Note: *The TOE uses a large number of third-party libraries so this information has been provided in an Appendix for readability purposes.*

5.2.6.5 FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall [***provide the ability***] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall [***provide the ability***] to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace, or update its own binary code.

FPT_TUD_EXT.1.4[9] Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed [***as an additional software package to the platform OS***].

5.2.6.6 FPT_TUD_EXT.2 Integrity for Installation and Update

FPT_TUD_EXT.2.1 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3[10] The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1[11] The application shall [

- ***encrypt all transmitted [data] with [HTTPS as a server in accordance with FCS_HTTPS_EXT.1/Server, HTTPS as a client in accordance with FCS_HTTPS_EXT.1/Client, TLS as defined in the TLS Package, SSH as conforming to the Extended Package for Secure Shell***]

] between itself and another trusted IT product.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference to the App PP.

[9] Modified by TD0561

[10] This element was added by TD0561

[11] Modified by TD0601

Table 4: Assurance Components

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance Documentation	AGD_OPE.1 Operational User Guidance
	AGD_PRE.1 Preparative Procedures
ALC: Life-cycle Support	ALC_CMC.1 Labeling of the TOE
	ALC_CMS.1 TOE CM coverage
	ALC_TSU_EXT.1 Timely Security Updates
ATE: Tests	ATE_IND.1 Independent Testing – Conformance
AVA: Vulnerability Assessment	AVA_VAN.1 Vulnerability Survey

The TLS/SSH Packages do not specify SARs. The expectation is that all SARs required by the App PP will apply to the entire TOE, including the portions addressed by the TLS and SSH Packages. Consequently, the evaluation activities specified in the App PP apply to the entire TOE evaluation, including any changes made to them by subsequent NIAP Technical Decisions as summarized in section 1.2 above.

The TLS/SSH Packages contain evaluation activities for how to evaluate their SFR claims as part of the evaluation of ASE_TSS.1, AGD_OPE.1, AGD_PRE.1, and ATE_IND.1. All Security Functional Requirements specified by the TLS/SSH Packages were evaluated in the manner specified in those packages.

6 TOE Summary Specification

This chapter describes the security functions of the TOE:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels.

It also describes the process put in place by the TOE vendor to provide timely security updates to the TOE as per the ALC_TSU_EXT.1 requirements of the [App PP].

6.1 Timely Security Updates

Axonius regularly releases new versions of its software which are deployed according to the customer's requirements (whether remotely by Axonius over a secure Internet-based connection, or by Axonius scheduling time for an "offline" upgrade procedure as determined by the organization's requirements during which the customer will be provided with a secure download link for an updater file, which can be loaded onto the existing Axonius VM via the customer's preferred side channel). Each update contains both operating system package upgrades and bugfixes within Axonius' code for any known security issues addressed since the prior version. Users are made aware of updates by utilizing the "check for update" feature that lets a customer know whether updates are available.

Axonius welcomes security issue reports from anyone – customer or not – via email sent to security@axonius.com, and offers a public PGP key ID, published at https://www.axonius.com/security and reachable only via HTTPS, for the purpose of encrypting these issue reports. Once a report has been received, it is validated by a member of Axonius' Security Team, and prioritized for remediation by the R&D team according to its technical severity and business impact. If found to be a security issue, the target time for a patch depends on the severity of the issue as follows: Critical – 15 days, High – 30 Days, Medium – 60 days, Low – 90 days. Informational issues have no target time for a patch.

In addition to public reports, Axonius proactively utilizes both manual and automated tooling to attempt to discover issues on their own, and engages with a third-party firm for a penetration test of the TOE on at least an annual basis. Issues discovered via either of these mechanisms are prioritized and remediated according to the same technical severity + business impact system as publicly-reported issues.

Security updates to the TOE are delivered as regular update packages in the same manner as a functional update. This process is described in 6.7.

Timely Security Updates is designed to satisfy:

- ALC_TSU_EXT.1 – The TOE implements procedures to ensure Timely Security Updates.

6.2 Cryptographic Support

The TOE implements cryptography to secure data in transit between itself and its operational environment.

All TOE cryptographic services are implemented by OpenSSL 1.0.2 with the FIPS Object Module 2.0.16 supplied by the TOE and have obtained CAVP certificates. The following table identifies the cryptographic algorithms used by the TSF, the associated standards to which they conform, and the CAVP certificates that demonstrate that the claimed conformance has been met.

Table 5: Cryptographic Functions

Functions	Standards	Certificates
FCS_CKM.1(1) Cryptographic Asymmetric Key Generation **FCS_CKM.1(2) Cryptographic Symmetric Key Generation**		
ECC key pair generation (NIST curves P-256, P-384, P-521)	FIPS PUB 186-4	CAVP cert #C1826
FFC key generation using Diffie-Hellman group 14	RFC 3526, Section 3	N/A
Symmetric cryptographic key generation (256-bit)	Random Bit Generator as specified in FCS_RBG_EXT.1	CAVP cert #C1826
FCS_CKM.2 Cryptographic Key Establishment		
Elliptic curve-based based key establishment	NIST SP 800-56A	CAVP cert #C1826 (KAS-ECC-Component)
FFC based key establishment using Diffie-Hellman Group 14	RFC 3526, Section 3	N/A
FCS_COP.1(1) Cryptographic Operation – Encryption/Decryption **FCS_COP.1(1)/SSH Cryptographic Operation – Encryption/Decryption (SSH EP)**		
AES-CBC, AES-CTR, AES-GCM (128, 256 bits)	CBC as defined in NIST SP 800-38A CTR as defined in NIST SP 800-38A GCM as defined in NIST SP 800-38D	CAVP cert # C1826
FCS_COP.1(2) Cryptographic Operation – Hashing		
SHA-1, SHA-256, SHA-384, SHA-512 (digest sizes 128, 256 384, and 512 bits)	FIPS PUB 180-4	CAVP cert #C1826
FCS_COP.1(3) Cryptographic Operation – Signing		
RSA (2048-bit)	FIPS PUB 186-4, Section 4	CAVP cert #C1826 (PKCS 1.5 gen/ver)
ECDSA schemes (P-256, P-384)	NIST Special Publication 800-56A	CAVP cert #C1826 (KAS-ECC Component)
FCS_COP.1(4) Cryptographic Operation – Keyed Hash Message Authentication		

Functions	Standards	Certificates
HMAC-SHA-1, HMAC-SHA2-384, and HMAC-SHA2-512	FIPS PUB 198-1 FIPS PUB 180-4	CAVP cert #C1826
FCS_RBG_EXT.2 Random Bit Generation from Application		
CTR_DRBG (AES 256 bits)	NIST SP 800-90A	CAVP cert # C1826

The TOE generates asymmetric keys in support of trusted communications. The TSF generates ECC keys using P-384, and P-521 curves. These keys are generated in support of the ECDHE key establishment schemes that are used for TLS/HTTPS communications when the TOE negotiates use of a TLS_ECDHE_* cipher suite and in support of SSH key exchange. The TOE generates asymmetric cryptographic keys in accordance with FFC schemes using Diffie-Hellman group 14 in support of SSH.

The TOE supports 256 bit cryptographic Symmetric Key Generation in support of securing credentials data at rest. To ensure sufficient key strength, the TOE implements DRBG functionality for key generation, using the AES-CTR_DRBG. The TOE uses the Python Requests library (using the “ssl” library), which uses version 2.0.16 of the OpenSSL FIPS Object Module (FOM) wrapped with OpenSSL 1.0.2 as the underlying library for cryptographic primitives.

The proprietary Entropy Analysis Report (EAR) describes how the TSF extracts random data from a software-based source to ensure that an amount of entropy that is at least equal to the strength of the generated keys is present (i.e., at least 256 bits when the largest supported keys are generated) when seeding the DRBG for key generation purposes. OpenSSL requests bits for a seed for the DRBG from /dev/random (the blocking entropy pool).

The TOE also uses OpenSSL to secure credential data at rest. The TOE stores credentials for adapters in the MongoDB using AES-256-CBC symmetric encryption. To protect Web GUI password credentials and private keys, the TOE uses password conditioning (PBKDF2) on user passwords in conjunction with LUKS (provided by the operational environment) to securely store the MongoDB encryption key and the TLS certificate's private key for the web GUI.

On first boot of the Axonius OVA (or after successful installation via the Axonius installer package), the user will be prompted to provide a password for use with PBKDF2_HMAC (SHA512, 100,000 rounds) to derive a key to set up LUKS volume encryption for the volume storing all Axonius application data. This will ensure that upon subsequent reboots, the LUKS volume containing this data, including any randomly-generated private keys or other sensitive data, will be encrypted and inaccessible until the user provides his or her password. This password can be changed from the Axonius GUI after the volume is unlocked and the Axonius application becomes operational.

Once the main storage volume is decrypted, the 256-bit MongoDB symmetric key used for AES-256 symmetric encryption is accessible for MongoDB to use to store sensitive values processed by the application. These values are the adapter credentials, which need to be used by the application, but can be stored in an encrypted format at rest.

Passwords for local users of the TOE GUI and the LUKS volume encryption to protect the MongoDB encryption key and nginx private key are conditioned as follows: The TOE applies a Pseudo Random Function (PRF), HMAC-SHA512, along with a per-user random salt value to the input password to produce a derived key which can then be used as a cryptographic key in subsequent operations. The salt is generated using Python’s secrets.token_hex function, which interacts with the underlying OpenSSL RBG.

The key is derived from the password using Python's hashlib.pbkdf2_hmac function, and the HMAC-SHA512 hash is iterated 100,000 times.

The TOE uses TLS 1.2 for client and server communications. All other TLS and previous SSL versions are rejected. The TLS implementation supports the following TLS cipher suites in the TOE's evaluated configuration:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

All supported ciphersuites use elliptic curves as the method of key establishment. For each ECDHE cipher suite used, the TSF presents secp384r1 in the Supported Groups extension and uses the following NIST curves for key establishment: secp384r1, and secp521r1.

As part of certificate validation in the establishment of TLS connectivity, the TOE will validate the reference identifier of a presented server certificate. This is done through validation of the Common Name (CN) or Subject Alternative Name (SAN) certificate fields, the latter of which is expected to contain the FQDN of the system to which the TOE is attempting to connect (i.e. the adapter source). The reference identifier is established by configuration. IP addresses and Wildcards are supported. Certificate pinning is not supported. Digital signatures used for the establishment of TLS communications use 2048-bit RSA.

The TOE uses HTTP over TLS client functionality for communications between the TOE and adapter sources in the operational environment. The TLS client will not establish a trusted channel if the server certificate is invalid and there is no administrative override. This communication does not use mutually-authenticated TLS.

The TOE uses HTTP over TLS server functionality for communications from remote users to the Web GUI interface. In the evaluated configuration, this communication does not support mutually-authenticated TLS. Session resumption based on session IDs according to RFC 5246 (TLS1.2). The TOE's implementation of HTTPS conforms to RFC 2818 by using a dedicated server port for its HTTP over TLS traffic and providing the server's identity in the server's Certificate message.

The TOE implements the SSH client protocol in accordance with SP 800-38A and that complies with RFCs 4251, 4252, 4253, 4254, 5656, and 6668 in support of SSH communication. The SSH transport implementation uses the aes128-ctr, aes256-ctr, aes128-cbc, and aes256-cbc encryption algorithms using 128-bit and 256-bit keys; ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384 public key algorithms (digital signatures); and hmac-sha1, hmac-sha1-96, hmac-sha2-256, and hmac-sha2-512 are used as its data integrity MAC algorithms. Diffiehellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 are the only allowed key exchange methods used for the SSH protocol. The implementation ensures the uniqueness of counter values by using counter blocks do not repeat within a given message and by ensuring that initial counter blocks are chosen such that counters are unique across all messages that are encrypted under the given key.

The TOE supports public-key and password authentication methods as described in RFC 4252. The SSH client keeps track of SSH packet sizes and ensures that packets greater than 32 kilobytes in an SSH transport connection are dropped as per RFC 4253. The SSH server ensures that the SSH connection is rekeyed after no more than 1 Gigabyte of data has been transmitted or no more than 1 hour has elapsed using that key.

The Cryptographic Support security function is designed to satisfy the following security functional requirements:

- FCS_CKM.1(1)/ FCS_CKM_EXT.1 – The TOE uses a NIST-approved implementation to generate asymmetric keys in support of TLS communications.
- FCS_CKM.1(2) – The TOE performs Cryptographic Symmetric Key Generation in support of securing credentials data at rest.
- FCS_CKM.1(3) – The TOE performs password-conditioning functions on the Web GUI password to protect stored sensitive data.
- FCS_CKM.2 – The TOE performs NIST-approved key establishment in support of TLS and SSH communications.
- FCS_COP.1(1) – The TOE uses a NIST-approved implementation to perform AES encryption and decryption in support of both TLS communications and secure storage of credentials.
- FCS_COP.1/(1)/SSH (SSH EP) – The TOE uses a NIST-approved implementation to perform AES encryption and decryption in support of SSH communication.
- FCS_COP.1(2) – The TOE uses a NIST-approved implementation to perform cryptographic hashing in support of TLS communications. The hash function is also used to support the HMAC functions used in PBKDF2 and SSH data integrity MAC algorithms.
- FCS_COP.1(3) – The TOE uses a NIST-approved implementation to generate and verify digital signatures in support of TLS and SSH communications.
- FCS_COP.1(4) – The TOE uses a NIST-approved implementation to perform HMAC functions in support of TLS and SSH communications, and PBKDF2.
- FCS_HTTPS_EXT.1/Client – The TOE implements HTTPS as a client to secure data in transit.
- FCS_HTTPS_EXT.1/Server – The TOE implements HTTPS as a server to secure data in transit.
- FCS_RBG_EXT.1/ FCS_RBG_EXT.2 – The TOE implements its own random bit generation services. The TOE uses a NIST-approved implementation to generate pseudo-random bits and this implementation is seeded with sufficiently strong entropy collected from the operational environment.
- FCS_SSH_EXT.1/FCS_SSHC_EXT.1– The TOE implements an SSH Client to secure data in transit.
- FCS_STO_EXT.1 – The TOE uses its own cryptographic functions to secure credential data at rest.
- FCS_TLS_EXT.1/FCS_TLSC_EXT.1/ FCS_TLSC_EXT.5 – The TOE implements TLS as a client to secure data in transit. The TOE's TLS client implementation presents supported elliptic curves to the server in the Supported Groups extension when an ECDHE cipher suite is negotiated.
- FCS_TLSS_EXT.1 – The TOE implements TLS as a server.

6.3 User Data Protection

The table below lists the data that is considered to be sensitive data for the Axonius TOE along with how that data is protected:

Table 6: Sensitive Data

Sensitive Data	Exchange	Protection at Rest	Protection in Transit
GUI credentials	Admin's browser to TOE over browser connection	FCS_STO_EXT.1 (PBKDF2) FDP_DAR_EXT.1 (LUKS)	HTTPS/TLS (Server)
TLS Private key	N/A	FCS_STO_EXT.1 (PBKDF2) FDP_DAR_EXT.1 (LUKS)	N/A
MongoDB encryption key	N/A	FCS_STO_EXT.1 (PBKDF2) FDP_DAR_EXT.1 (LUKS)	N/A
Adapter Credentials	TOE to remote system	FCS_STO_EXT.1 (AES-256-CBC)	HTTPS/TLS or SSH (Client)

The TOE uses underlying platform functionality for network connectivity for remote management and connections to assets. The following table highlights the TOE's network usage.

Table 7: TOE Network Usage

Component	User-Initiated	Externally-Initiated	TOE-Initiated
TOE	Access to Web GUI	N/A	N/A
Adapters	N/A	N/A	The TOE adapters connect to adapter sources in the operational environment.

The User Data Protection security function is designed to satisfy the following security functional requirements:

- FDP_DAR_EXT.1 – Sensitive data at rest is protected in accordance with FCS_STO_EXT.1 in conjunction with leveraging platform-provided functionality.
- FDP_DEC_EXT.1 – The TOE's use of platform services is well understood by users prior to authorizing the TOE activity.
- FDP_NET_EXT.1 – The TOE communicates over the network for well-defined purposes. Depending on the function, the use of network resources is remotely initiated by an administrative user or initiated by the TOE itself.

6.4 Identification and Authentication

The TOE uses X.509 certificates when the TOE is providing its own TLS server certificate to a TLS client and for authenticating the asset's TLS server certificate presented to it. Mutual authentication is not supported.

The TOE implements the following functional behavior for all uses of X.509 certificates:

- Certificate validation and certificate path validation is performed in accordance with RFC 5280.
- The certificate path is checked to ensure that it terminates with a trusted CA certificate.

- The certificate path is validated by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The CA certificate is validated to ensure it includes the caSigning purpose in the key usage field
- Revocation status is checked using an OCSP as specified in RFC 6960.
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification[12] shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates[12] presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - S/MIME certificates[12] presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-dp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
    - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

In the event that the revocation status of a certificate cannot be verified because the OCSP responder cannot be reached, the TOE will not accept the certificate.

Because the TOE's use of the certificate validation function is to validate the authenticity of remote adapter sources, the TSF chooses what certificates to use based on what is presented to it as part of establishing the TLS session. The TOE is only assigned one certificate for its own use, so there is only one certificate that it will present in cases where a remote entity may need to validate it.

The Identification and Authentication security function is designed to satisfy the following security functional requirements:

- FIA_X509_EXT.1 – X.509 certificates are validated by the TSF when establishing trusted communications.
- FIA_X509_EXT.2 – The TOE uses X.509 certificates to support authentication of TLS connections. When revocation status of a certificate cannot be determined, the TSF does not accept the certificate.

6.5 Security Management

The TOE provides a web-based graphical user interface (GUI) that requires user authentication to access. As part of initial setup of the TOE, the administrator performing the install must specify an initial username/password that is used to log on to the web GUI; the TOE is not pre-loaded with "default" administrator credentials. These credentials are stored locally and protected by the TSF as per FCS_STO_EXT.1.

The TOE is installed into the following location: /home/ubuntu/cortex, and the app runs as the ubuntu user.

[12] Certificates are not used for S/MIME, trusted updates or executable code integrity verification and client certificates are not presented to the TOE. Therefore these rules are vacuously satisified.

The TOE stores sensitive data encrypted on the file system or in a local mongoDB database that is located in a subdirectory of the installation directory for Linux.

All directories containing TOE software and data are configured by default in such a manner that nothing is world-writable. The adapter connections, custom CA certificates, and hostname configuration settings for the TOE are stored in the Ubuntu user's home directory in a folder called Cortex. The application is configured by default with file permissions to protect the application binaries and data files from modification by untrusted users.

The TOE supports the following security-relevant management functions:

- Configuration of adapter connections,
- Upload custom certs, and
- Set hostname.

The Security Management security function is designed to satisfy the following security functional requirements:

- FMT_CFG_EXT.1 – The TOE requires credentials to be defined before administrative use. The TOE is protected from direct modification by untrusted users via its host OS platform.
- FMT_MEC_EXT.1 – Configuration settings for the TOE are stored in the appropriate location for the supported host OS platform.
- FMT_SMF.1 – Administrators can use the TSF to configure the adapter connections, upload custom certs, and set hostname.

6.6 Privacy

The TOE does not collect or transmit PII. The TOE accepts administrative credentials as part of the GUI login process but user account information is not considered to be PII in the context of the PP.

The Privacy security function is designed to satisfy the following security functional requirements:

- FPR_ANO_EXT.1 – The TOE prevents the unnoticed/unauthorized transmission of PII across a network by not having functionality that is intended for such transmissions.

6.7 Protection of the TSF

The TOE implements several mechanisms to protect against exploitation.

The TOE runs on top of the host operating system as a series of Docker containers containing Python and JavaScript code, and does not explicitly require disabling built-in operating system controls for any reason (e.g. those built into Ubuntu 16.04). As such, the TOE relies on the operating system to handle sensitive low-level operations such as memory mapping, and is compatible with Ubuntu 16.04, including when AppArmor is enabled on the host OS. The TOE is interpreted code and not just-in-time compiled and therefore compiler flags to enforce ASLR are not necessary. The TOE also does not use both PROT_WRITE and PROT_EXEC on the same memory regions. There is no situation where the TSF maps memory to an explicit address.

The TOE runs successfully on a system with AppArmor enabled and in enforce mode. The Ubuntu platform AppArmor security feature is enabled by default during TOE installation, using the default configuration/settings. The TOE does not use any undocumented platform APIs and no system calls are directly invoked in Axonius code. The TOE is entirely Dockerized Python/JavaScript, so all calls are indirect. The TOE makes use of third-party libraries as identified in Appendix A.1. The TOE is versioned using semver (Semantic Versioning) in the format x.y.z-f (x.y.z-fed), where x is major (number), y is minor (number), z is patch (number), and 'f' (or 'fed') is fixed and flags this as a 'federal' version; SWID is not used. Minor versions include new features that are backwards-compatible, and new patch versions are released to address bugs discovered after new features are developed. The TOE is a standalone Ubuntu 16.04 application that is often bundled with Ubuntu 16.04 as a "virtual appliance".

The administrator can identify the TOE's current running version through Settings -> About that provides a version number and build date.

The TOE can check for software updates. The web app itself has a page located at /settings/about-tab. The system regularly checks a service controlled by Axonius to see what the latest version is. When the installed software is ≥1 minor version behind, the user receives a message that says, "Contact us to request an upgrade" with an email link, and the latest available version number. Candidate updates are obtained by the user by downloading them directly from Axonius's website and placing them into the placed in /home/ubuntu directory. At this point, the administrator updates the TOE using standard dpkg package manager instructions for a .deb installation. If the update is successful, an ***Upgrader completed - success*** message is displayed, otherwise a failure message is displayed. The TOE will not download, modify, replace, or update its own binary code.

The TOE is packaged as a digitally signed .deb file, signed using an ECC (NIST P384) based GPG key. Axonius signs the .deb package using its private key, and the Debian Package Manager then uses the published public key to verify the signature. Signature verification of the .deb package is performed automatically before proceeding with the package install. If the signature verification fails, the package is not installed. Removing (uninstalling) the product will remove all executable code from the host system.

The Protection of the TSF security function is designed to satisfy the following security functional requirements:

- FPT_AEX_EXT.1 – The TOE interacts with its host OS platform in a manner that does not expose the system to memory-related exploitation.
- FPT_API_EXT.1 – The TOE does not use any undocumented platform APIs.
- FPT_IDV_EXT. 1 – The TOE is versioned using semver.
- FPT_LIB_EXT.1 – The set of third-party libraries used by the TOE is well-defined.
- FPT_TUD_EXT.1 – There is a well-defined method for checking what version of the TOE is currently installed and whether updates to it are available. Updates are signed by the vendor and validated by the host OS platform prior to installation.
- FPT_TUD_EXT.2 – The TOE can be updated through installation packages.

6.8 Trusted Path/Channels

In the evaluated configuration, the TOE uses its own cryptographic implementation to encrypt sensitive data in transit. Listed below are the various external interfaces to the TOE that requires the use of trusted communications.

- Between users and TOE Web GUI

  - Communications use HTTPS (TOE is server)
  - Port 443
  - Used to secure user interactions with the TOE
- Between TOE and adapter sources
  - Communications use HTTPS or SSH (TOE is client)
  - Port 443 (TLS), Port 22 (SSH)
  - Used to secure communications with adapter data sources

The Trusted Path/Channels security function is designed to satisfy the following security functional requirements:

- FTP_DIT_EXT.1 – The TOE relies on its own mechanisms to secure data in transit between itself and its operational environment.

7 Protection Profile Claims

This ST is conformant to the *Protection Profile for Application Software, Version 1.3, 1 March 2019* (App PP), *Functional Package for Transport Layer Security (TLS), Version 1.1, February 12,* 2019 (TLS Package), and *Extended Package for Secure Shell (SSH), Version 1.0, February 19, 2016* (SSH Package) along with all applicable errata and interpretations from the certificate issuing scheme.

The TOE consists of a software application that runs on a Linux operating system as its platform.

As explained in section 3, Security Problem Definition, the Security Problem Definition of the App PP has been included by reference into this ST.

As explained in section 4, Security Objectives, the Security Objectives of the App PP has been included by reference into this ST.

All claimed SFRs are defined in the App PP and TLS/SSH Packages. All mandatory SFRs are claimed. No optional or objective SFRs are claimed. Selection-based SFR claims are consistent with the selections made in the mandatory SFRs that prompt their inclusion.

8 Rationale

This Security Target includes by reference the App PP Security Problem Definition, Security Objectives, and Security Assurance Requirements. The Security Target does not add, remove, or modify any of these items. Security Functional Requirements have been reproduced with the Protection Profile operations completed. All selections, assignments, and refinements made on the claimed Security Functional Requirements have been performed in a manner that is consistent with what is permitted by the App PP and TLS Package. The proper set of selection-based requirements have been claimed based on the selections made in the mandatory requirements. Consequently, the claims made by this Security Target are sufficient to address the TOE’s security problem.

A TOE Usage of Third-Party Components

This Appendix lists the third-party libraries that are used by the TOE.

A.1 Third-Party Libraries

Listed below are the third-party libraries used by the TOE. Note that these libraries do not necessarily relate to the TOE functionality claimed in the Security Target; however, since they are bundled with the product itself they are disclosed since a vulnerability outside the logical boundary of the product could still present an exploitable vulnerability.

Python Libraries:

```
retry==0.9.2
virtualenv==15.2.0
funcy==1.10
namedlist==1.7
APScheduler==3.4.0
bcrypt==3.1.4
cairocffi==0.5.2
pql==0.4.3
chardet==3.0.4
click==7.1.2
cryptography==2.8
Werkzeug==0.16.0
Flask==1.1.2
Flask_Limiter==1.2.1
idna==2.6
itsdangerous==0.24
JSON-log-formatter==0.2.0
paramiko==2.4.3
pyasn1==0.4.8
ldap3==2.5.1
pycparser==2.18
pymongo==3.11.2
PyNaCl==1.1.2
pytz==2017.3
requests==2.18.4
scp==0.13.2
six==1.13.0
tzlocal==1.4
urllib3==1.22
retrying==1.3.3
pytest==3.2.3
flaky==3.4.0
PyYAML==3.12
```

```
promise==2.3
autopep8==1.3.3
dnspython==1.15.0
pyVmomi==6.5.0.2017.5.post1
pyVim==0.0.21
nexpose==0.1.7
boto3==1.9.22
decorator==4.1.2
netstruct==1.1.2
construct==2.9.25
netmiko==2.4.1
dpkt==1.9.1
mongomock==3.22.0
pyOpenSSL==17.5.0
numpy==1.14.2
username-generator==2.0.0
pypng==0.0.18
netaddr==0.7.19
weasyprint==52.2
jinja2==2.10.1
azure-mgmt-network==1.7.1
azure-mgmt-compute==3.0.1
uritools==2.1.0
google-auth==1.11.0
ipython==6.2.1
jedi==0.17.2
ipython-genutils==0.2.0
google-api-python-client==1.7.3
google-auth==1.11.0
google-auth-httplib2==0.0.3
orionsdk==0.0.6
flasgger==0.9.0
python-dateutil==2.7.3
duo-client==4.2.1
ncclient==0.6.4
junos-eznc==2.1.8
aiohttp==3.3.2
apache-libcloud==2.4.0
passlib==1.7.1
pylint==2.6.2
pylint_quotes==0.1.9
isort==4.3.4
docker==4.1.0
mypy==0.620
```

```
selenium==3.141.0
bandit==1.4.0
aliyun-python-sdk-core-v3==2.9.0
aliyun-python-sdk-ecs==4.9.5
func_timeout==4.3.0
dsp3==0.1rc34
kubernetes==7.0.0
awscli==1.16.40
cachetools==2.1.0
tls-syslog==0.1.3
teamcity-messages==1.21
pefile==2018.8.8
psutil==5.4.8
dataclasses==0.6
dataclasses-json==0.2.2
proxmoxer==1.0.3
pip-licenses==1.10.0
deepdiff==3.3.0
jira==2.0.0
pysnmp==4.4.4
PyPDF2==1.26.0
daemonocle==1.0.1
netifaces==0.10.9
plumbum==1.6.7
aiodns==2.0.0
xmltodict==0.12.0
astor==0.8.0
frozendict==1.2
python-redis-lock==3.7.0
redis==3.5.3
distro==1.4.0
pyparsing==2.4.5
ucsmsdk==0.9.8
python-crontab==2.4.0
pip==19.3.1
pymongocrypt==0.1b1
pem==19.3.0
uptime==3.0.1
matplotlib==3.2.1
segfault==0.0.1
tabulate==0.8.7
cpe==1.2.1
aiodnsresolver==0.0.140
celery==5.0.5
```

```
celery-redbeat==2.0.0
pysmb==1.1.27
requests-ntlm2==6.2.7
pyjwt==1.7.1
flask-jwt-extended[asymmetric_crypto]==3.24.1
filemagic==1.6
google-cloud-bigquery==1.23.0
inotify-simple==1.3.5
python-dotenv==0.15.0
marshmallow==3.9.0
PySocks==1.5.7
attrs==20.3.0
phonenumbers==8.12.12
ocspbuilder==0.10.2
defusedxml==0.6.0
pyinstrument==3.0.0
pyinstaller==4.1
marshmallow-jsonapi==0.23.2
webargs==5.5.1
querystring-parser==1.2.4
jsonschema==3.2.0
apispec==4.0.0
apispec-webframeworks==0.5.2
pydantic==1.7.3
pika==1.2.0
setuptools==49.6.0
retry==0.9.2
uWSGI==2.0.18
uwsgitop==0.11
Werkzeug==0.16.0
Flask==1.1.2
Flask_Limiter==1.2.1
APScheduler==3.4.0
retrying==1.3.3
pymongo==3.11.2
cairocffi==0.5.2
pql==0.4.3
JSON-log-formatter==0.2.0
pyasn1==0.4.8
ldap3==2.5.1
dnspython==1.15.0
boto3==1.16.17
namedlist==1.7
paramiko==2.4.3
```

```
pyVmomi==6.5.0.2017.5.post1
pyVim==0.0.21
nexpose==0.1.7
scp==0.13.2
funcy==1.10
uritools==2.1.0
passlib==1.7.1
bcrypt==3.1.4
netstruct==1.1.2
construct==2.9.25
netmiko==2.4.1
pyodbc==4.0.27
dpkt==1.9.1
ipython==6.2.1
jedi==0.17.2
pyjwt==1.7.1
pychef==0.3.0
openstacksdk==0.12.0
pycrypto==2.6.1
pyOpenSSL==17.5.0
pysnmp==4.4.4
pycryptodomex==3.6.0
ply==3.11
pysmi==0.2.2
weasyprint==52.2
jinja2==2.10.1
cairosvg==2.1.3
python-jose==3.0.0
azure-mgmt-network==11.0.0
azure-mgmt-compute==13.0.0
azure-mgmt-resource==10.1.0
SoftLayer==5.4.4
aiohttp==3.3.2
cchardet==2.1.1
ipython-genutils==0.2.0
google-api-python-client==1.12.8
google-auth==1.24.0
google-auth-httplib2==0.0.3
orionsdk==0.3.0
flasgger==0.9.0
python-dateutil==2.7.3
duo-client==4.2.1
ncclient==0.6.4
junos-eznc==2.1.8
```

```
apache-libcloud==2.8.1
faker==0.8.17
aliyun-python-sdk-core-v3==2.13.11
aliyun-python-sdk-ecs==4.17.8
func_timeout==4.3.0
cbapi==1.3.6
dsp3==0.1rc34
kubernetes==7.0.0
oci==2.21.6
python3-saml==1.4.1
cachetools==4.1.1
tls-syslog==0.1.3
beautifulsoup4==4.6.3
psutil==5.4.8
dataclasses==0.6
dataclasses-json==0.2.2
pymemfd==0.1
names==0.3.0
proxmoxer==1.0.3
deepdiff==3.3.0
jira==2.0.0
pysmb==1.1.27
pancloud==1.5.0
pan_cortex_data_lake==2.0.0a14
zeep==3.3.1
docker==4.1.0
netifaces==0.10.9
aiodns==2.0.0
xmltodict==0.12.0
astor==0.8.0
psycopg2==2.8.3
frozendict==1.2
python-redis-lock==3.7.0
redis==3.5.3
mysql-connector-python==8.0.17
pymongocrypt==0.1b1
cx_Oracle==7.2.3
distro==1.4.0
certifi==2019.9.11
chardet==3.0.4
gql==0.1.0
graphql-core==2.2.1
idna==2.8
promise==2.3
```

```
pytz==2019.3
requests==2.24.0
Rx==1.6.1
six==1.13.0
urllib3==1.25.6
pytenable==1.1.3
google-cloud-bigquery==1.23.0
wrapt==1.11.2
pyparsing==2.4.5
ucsmsdk==0.9.8
pem==19.3.0
requests_ntlm==1.1.0
dicttoxml==1.7.4
vectra-api-tools==1.1rc0
python-gvm==1.2.0
python-ilorest-library==3.0.0
python-keycloak==0.19.0
boxsdk==2.7.1
cryptography==2.8
azure-core==1.7.0
azure-storage-blob==12.3.2
azure-storage-common==1.4.2
azure-storage-file==1.4.0
azure-storage-queue==1.4.0
msrestazure==0.6.4
google-cloud-storage==1.27.0
infoblox-netmri==0.1.5
tabulate==0.8.7
pyotp==2.3.0
msrest==0.6.17
cpe==1.2.1
aiodnsresolver==0.0.140
flask-jwt-extended[asymmetric_crypto]==3.24.1
requests-ntlm2==6.2.7
celery==5.0.5
celery-redbeat==2.0.0
filemagic==1.6
marshmallow==3.9.0
phonenumbers==8.12.12
pyinstaller==4.1
threatstack==1.2.0
Office365-REST-Python-Client==2.3.0.1
pandas==1.1.5
git+https://github.com/Axonius/impacket@axonius_release#egg=impacket
```

```
PySocks==1.7.1
oscrypto==1.2.1
ocspbuilder==0.10.2
marshmallow-jsonapi==0.23.2
webargs==5.5.1
querystring-parser==1.2.4
pyzbar==0.1.8
jsonschema==3.2.0
pg8000==1.16.6
pyinstrument==3.0.0
boxsdk[jwt]==2.10.0
pyjwt==1.7.1
py-spy==0.3.3
defusedxml==0.6.0
sqlserverport==1.0.1
daemonocle==1.0.1
uptime==3.0.1
inotify-simple==1.3.5
netifaces==0.10.9
apispec==4.0.0
apispec-webframeworks==0.5.2
pydantic==1.7.3
apispec==4.0.0
click==7.1.2c
```

Java Libraries:

```
"@babel/polyfill": "7.12.1",
"@mdi/js": "4.6.95",
"@okta/okta-auth-js": "2.3.1",
"ant-design-vue": "1.6.5",
"async-mutex": "0.2.4",
"axios": "0.19.0",
"copy-to-clipboard": "3.3.1",
"core-js": "3.7.0",
"dayjs": "1.9.8",
"filepond": "4.11.0",
"ifvisible": "1.1.0",
"ip": "1.1.5",
"jwt-decode": "3.0.0",
"lodash": "4.17.19",
"lottie-web": "5.7.4",
"promise": "8.0.2",
"qs": "6.9.4",
"regenerator-runtime": "0.13.7",
"shortid": "2.2.14",
"vue": "2.6.10",
"vue-color": "2.7.1",
"vue-cookies": "1.5.13",
"vue-filepond": "6.0.2",
"vue-google-charts": "0.3.2",
"vue-json-component": "0.3.0",
"vue-material": "1.0.0-beta-10.2",
"vue-router": "3.0.2",
"vue-router-multiguard": "1.0.3",
"vuedraggable": "2.23.0",
"vuelidate": "0.7.4",
"vuetify": "2.1.1",
"vuex": "3.1.0"
"@babel/core": "7.12.3",
"@babel/eslint-parser": "7.12.1",
"@babel/plugin-syntax-dynamic-import": "7.8.3",
"@babel/preset-env": "7.12.1",
"@storybook/addon-actions": "5.2.8",
"@storybook/addon-knobs": "5.2.8",
"@storybook/addon-links": "5.2.8",
"@storybook/addons": "5.2.8",
"@storybook/vue": "5.2.8",
"@vue/babel-helper-vue-jsx-merge-props": "1.2.1",
"@vue/babel-preset-jsx": "1.2.4",
"antd-dayjs-webpack-plugin": "0.0.9",
"autoprefixer": "9.4.8",
"babel-loader": "8.1.0",
"babel-plugin-import": "1.13.1",
"clean-webpack-plugin": "1.0.1",
"css-loader": "3.2.0",
"eslint": "6.8.0",
"eslint-config-airbnb-base": "14.0.0",
"eslint-import-resolver-webpack": "0.12.1",
"eslint-plugin-import": "2.19.1",
"eslint-plugin-vue": "6.1.2",
"file-loader": "3.0.1",
"html-webpack-plugin": "3.2.0",
"husky": "4.3.0",
"less": "3.11.1",
"less-loader": "5.0.0",
"lint-staged": "10.4.0",
"mini-css-extract-plugin": "0.9.0",
"node-sass": "4.14.1",
"optimize-css-assets-webpack-plugin": "5.0.3",
"postcss-loader": "3.0.0",
"sass-loader": "8.0.0",
"sass-resources-loader": "2.0.0",
"storybook-vue-router": "1.0.7",
"terser": "3.14.1",
"terser-webpack-plugin": "2.2.1",
"vue-loader": "15.7.0",
"vue-style-loader": "4.1.2",
"vue-template-compiler": "2.6.10",
"webpack": "4.36.0",
"webpack-cli": "3.3.12",
"webpack-dev-server": "3.11.0",
"webpack-merge": "4.2.1",
"worker-loader": "3.0.5"
```

B Axonius Supported Adapter Data Sources

This section identifies the TOE supported adapters and the secure communication methods supported for each: SSH or HTTPS. The use of unsecured connections to assets (such as HTTP) is outside the scope of evaluation.

Adapter_name	Description	Connection_protocols
Absolute	Absolute specializes in software to manage and secure Windows computers and Android smartphones.	HTTP/HTTPS
Alcide	Alcide provides cloud and Kubernetes discovery, K8s audit and compliance scanner, microservices anomaly detection and security policies management and enforcement.	HTTP/HTTPS
Alert Logic	Alert Logic provides vulnerability and asset visibility, endpoint protection, threat detection, incident management, and a web application firewall.	HTTP/HTTPS
Alibaba Cloud	Alibaba Cloud provides cloud computing services and cloud Infrastructure as a service.	HTTP/HTTPS
Amazon Web Services (AWS)	Amazon Web Services (AWS) includes a broad set of global cloud based products. It supports EC2, ECS, EKS, IAM, EBS, ELB, RDS, S3, VPC and Workspaces.	HTTP/HTTPS
Aqua Security	Aqua Security provides container and cloud native cybersecurity for teams using Docker, Kubernetes, serverless, and other cloud native technologies.	HTTP/HTTPS
Arista Extensible Operating System (EOS)	Arista Extensible Operating System (EOS) is the core of Arista cloud networking solutions for next-generation data centers and cloud networks.	HTTP/HTTPS
Armis	Armis is an agentless device security platform to see and protect unmanaged and IoT devices.	HTTP/HTTPS
Aruba	Aruba connects to Aruba switches and routers.	HTTP/HTTPS
Aruba AirWave	Aruba AirWave is a network management system for wired and wireless infrastructure and provides granular visibility into devices, users, and applications on the network.	HTTP/HTTPS
Aruba ClearPass	Aruba ClearPass is a network access control (NAC) solution that allows enterprises to identify devices, enforce policies, and remediate threats.	HTTP/HTTPS
Atlassian Jira Asset Platform	Atlassian Jira Asset Platform links software with Jira to populate an asset inventory, letting users query for assets and link them to issues.	HTTP/HTTPS
Automox	Automox is a cloud-based patch and configuration management solution for Windows, Linux, Mac, and third-party software.	HTTP/HTTPS

Auvik	Auvik is an IT asset and network monitoring solution for managing entire network infrastructures, including physical servers, data centers, workstations and more.	HTTP/HTTPS
Axonius Users	The Axonius Users adapter fetches users with Axonius credentials and their permissions using our API client.	HTTP/HTTPS
BambooHR	BambooHR is HR software used to collect, maintain, and analyze data for hiring, onboarding employees, and managing company culture.	HTTP/HTTPS
BeyondTrust Privileged Identity (Lieberman RED Identity Management)	BeyondTrust Privileged Identity (formerly Lieberman RED Identity Management) is a password management solution that helps companies secure, manage, and administer credentials for privileged users and IT vendors.	HTTP/HTTPS
BeyondTrust Remote Support (Bomgar)	BeyondTrust Remote Support (formerly Bomgar) allows support technicians to remotely connect to end-user systems through firewalls from their computer or mobile devices.	HTTP/HTTPS
BigID	BigID is data security solution that provides enterprise protection and privacy of personal data.	HTTP/HTTPS
Bitdefender GravityZone Business Security	Bitdefender GravityZone Business Security uses machine learning and heuristics to protect against malware, phishing, ransomware, exploits and zero-days.	HTTP/HTTPS
BitSight Security Ratings	BitSight Security Ratings are a data-driven and dynamic measurement of an organizationâ€™s cybersecurity performance.	HTTP/HTTPS
BlackBerry Unified Endpoint Management (UEM)	BlackBerry Unified Endpoint Management (UEM) delivers endpoint management and policy control for devices and apps on-premise or in the cloud.	HTTP/HTTPS
BlueCat Enterprise DNS	BlueCat Enterprise DNS connects all disparate DNS and DHCP with centralized management of all clients and critical assets.	HTTP/HTTPS, ODBC
Box Platform	Box Platform provides data security, file sharing, collaborating, and content management tools. Box Platform provides access to Box APIs.	HTTP/HTTPS
CA Service Management	CA Service Management is an IT service management (ITSM) solution that offers incident management and IT asset management.	HTTP/HTTPS
CA Spectrum	CA Spectrum is a services and network infrastructure management system that enables the modeling of LAN, WAN, wired, wireless, physical, and virtual networks.	HTTP/HTTPS

Carbon Black CB Defense	Carbon Black CB Defense includes antivirus and EDR in a cloud-delivered platform to stop malware, non-malware attacks, and ransomware. (Note: This adapter is also compatible with CB ThreatHunter and CB LiveOps)	HTTP/HTTPS
Carbon Black CB Protection	Carbon Black CB Protection includes application control and critical infrastructure protection for critical systems and fixed-function devices in highly regulated environments.	HTTP/HTTPS
Carbon Black CB Response	Carbon Black CB Response includes EDR and threat hunting for security operations centers and incident response teams.	HTTP/HTTPS
Censys	Censys monitors infrastructure and discovers unknown assets across the Internet.	HTTP/HTTPS
Centrify Identity Services	Centrify Identity Services manages application access, endpoints, and network infrastructure.	HTTP/HTTPS
Check Point Infinity	Check Point Infinity protects against cyber threats across networks, endpoint, cloud and mobile devices. This adapter supports the entire Infinity platform, including Check Point firewalls.	HTTP/HTTPS
Chef	Chef provides continuous automation for building, deploying, and managing infrastructure, compliance, and applications in legacy and hybrid environments.	HTTP/HTTPS
Cherwell IT Service Management	Cherwell IT Service Management is a service desk platform enabling automation for process workflows, supporting tasks, and related approvals.	HTTP/HTTPS
Cisco	Cisco connects to Cisco switches and routers.	SNMP, SSH
Cisco Advanced Malware Protection (AMP)	Cisco Advanced Malware Protection (AMP) includes threat intelligence, sandboxing, and malware blocking to detect, contain, and remove malware.	HTTP/HTTPS
Cisco Firepower Management Center	Cisco Firepower Management Center provides management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.	HTTP/HTTPS
Cisco Identity Services Engine (ISE)	Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the companyâ€™s routers and switches.	HTTP/HTTPS
Cisco Meraki	Cisco Meraki solutions include wireless, switching, security, EMM, communications, and security cameras, all centrally managed from the web.	HTTP/HTTPS
Cisco Prime	Cisco Prime offers a suite of tools to automate the management of wired and wireless Cisco networks.	SNMP, SSH

Cisco Stealthwatch	Cisco Stealthwatch is an agentless malware detection solution that provides visibility and network traffic security analytics across the extended network, including endpoints, branch, data center, and cloud.	HTTP/HTTPS
Cisco UCS Manager	Cisco UCS Manager supports the entire Cisco UCS server and Cisco HyperFlex Series hyperconverged infrastructure portfolios. It enables server, fabric, and storage provisioning as well as, device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection.	HTTP/HTTPS
Cisco Umbrella	Cisco Umbrella is a secure internet gateway in the cloud, including DNS and IP layer enforcement and command and control callback blocking.	HTTP/HTTPS
Cisco Unified Communications Manager 12.5	Cisco Unified Communications Manager provides secure and manageable call control and session management.	HTTP/HTTPS
Citrix Endpoint Management (XenMobile)	Citrix Endpoint Management (formerly XenMobile) is a solution for managing endpoints, offering mobile device management (MDM) and mobile application management (MAM) capabilities.	HTTP/HTTPS
Claroty	Claroty discovers assets and monitors communication patterns for ICS networks.	HTTP/HTTPS
Cloud Health	Cloud Health is a cloud management platform to analyze and manage cloud cost, usage, security, and governance.	HTTP/HTTPS
Cloudflare DNS	Cloudflare DNS runs one of the largest DNS networks in the world.	HTTP/HTTPS
CloudPassage Halo	CloudPassage Halo is a security automation platform providing visibility, protection, and continuous compliance monitoring for AWS and Azure deployments.	HTTP/HTTPS
Code42	Code42 is a next-gen DLP solution used to detect insider threats, satisfy regulatory compliance, and accelerate incident response investigations.	HTTP/HTTPS
Contrast Security	Contrast Security protects software applications against cyberattacks.	HTTP/HTTPS
CrowdStrike Falcon	CrowdStrike Falcon delivers next-generation antivirus, endpoint detection and response (EDR), managed threat hunting, and threat intelligence.	HTTP/HTTPS
CSCDomainManager	CSCDomainManager is a web-based portfolio management platform consolidating domains alongside social media usernames, SSL digital certificates, and DNS.	HTTP/HTTPS

CSV	The CSV adapter imports .csv files with inventory information including: devices and serial numbers, users, and installed software data.	HTTP/HTTPS, SMB
CyberArk Privileged Account Security	CyberArk Privileged Account Security provides privileged password management, session recording, least privilege enforcement, and privileged data analytics.	HTTP/HTTPS
Cybereason Deep Detect & Respond	Cybereason Deep Detect & Respond (EDR) defends against advanced attacks by collecting and analyzing behavioral data to identify suspicious activities.	HTTP/HTTPS
CyCognito CyCAST Platform	CyCognito CyCAST Platform is an automated, cloud-based security testing service that simulates attackers' reconnaissance techniques to find organizations' security blind spots.	HTTP/HTTPS
CylancePROTECT	CylancePROTECT uses artificial intelligence to detect and protect against ransomware, advanced threats, fileless malware, and malicious documents.	HTTP/HTTPS
Cynet 360	Cynet 360 is a detection and response security platform for finding, ranking, and remediating unknown, camouflaged threats.	HTTP/HTTPS
Datadog	Datadog is a monitoring service for cloud-scale applications, providing monitoring of servers, databases, tools, and services.	HTTP/HTTPS
Datto RMM (Autotask Endpoint Management)	Datto RMM (formerly Autotask Endpoint Management) is a cloud-based Remote Monitoring and Management (RMM) platform that provides device auditing, real-time monitoring, and automatic patching.	HTTP/HTTPS
Dell EMC Avamar	Dell EMC Avamar is a backup and recovery solution that enables daily backups of physical and virtual environments, NAS servers, enterprise applications, remote offices and desktops/laptops.	HTTP/HTTPS
Device42	Device42 is a cloud-based CMDB for physical, virtual, and cloud servers and containers, network components, software, services, applications, and their relationships and dependencies.	HTTP/HTTPS
DigiCert CertCentral	DigiCert CertCentral consolidates tasks for issuing, installing, inspecting, remediating, and renewing certificates.	HTTP/HTTPS
DigiCert PKI Platform (Symantec Managed PKI)	DigiCert PKI Platform (formerly Symantec Managed PKI) provides a cloud-based enterprise solution for issuing and managing digital certificates used to enable strong authentication and encryption.	HTTP/HTTPS

Digital Shadows SearchLight	Digital Shadows SearchLight is a digital risk protection solution that protects organizations against external risk exposure.	HTTP/HTTPS
DivvyCloud	DivvyCloud offers security, compliance, and governance guardrails for public and private cloud infrastructures.	HTTP/HTTPS
Dropbox	Dropbox is a file hosting service that offers cloud storage, file synchronization, personal cloud, and client software.	HTTP/HTTPS
Druva Cloud Platform	Druva Cloud Platform is a data protection as-a-service that provides management across all customer data sources that are scalable, predictable and on-demand.	HTTP/HTTPS
Duo Beyond	Duo Beyond identifies corporate vs. personal devices, blocks untrusted devices, and give users secure access to internal applications.	HTTP/HTTPS
Dynatrace	Dynatrace is a software intelligence platform providing application performance management and cloud infrastructure monitoring.	HTTP/HTTPS
Eclypsium	Eclypsium protects the foundation of the computing infrastructure, controlling risks and stopping threats to enterprise firmware and hardware devices.	HTTP/HTTPS
edgescan Fullstack Vulnerability Management	edgescan Fullstack Vulnerability Management is a cloud-based continuous vulnerability management and penetration testing solution that discovers, validates and rates vulnerabilities by running continuous asset profiling to detect rogue/exposed ports, hosts or even hidden APIâ€™s.	HTTP/HTTPS
Endgame	Endgame is an endpoint protection platform that combines on-line and off-line protection against exploits, phishing, malware, ransomware, and fileless attacks.	HTTP/HTTPS
enSilo	enSilo automates and orchestrates detection, prevention, and response against advanced malware and ransomware.	HTTP/HTTPS
ESET Endpoint Security	ESET Endpoint Security is an anti-malware suite for Windows including web filtering, firewall, USB drive and botnet protection.	HTTP/HTTPS
ExtraHop Reveal(x)	ExtraHop Reveal(x) is a network detection and response (NDR) solution that provides visibility, real-time threat detection, and response.	HTTP/HTTPS
F5 BIG-IP iControl	F5 iControl is a Web services-enabled open API providing granular control over the configuration and management of F5's application delivery platform, BIG-IP.	HTTP/HTTPS

FireEye Endpoint Security (formerly HX)	FireEye Endpoint Security (formerly HX) detects and protects against unknown endpoint threats and exploits with integrated threat intelligence.	HTTP/HTTPS
FireMon Security Manager	FireMon Security Manager is a network security solution that provides real-time visibility, control, and management for network security devices across hybrid cloud environments.	HTTP/HTTPS
Flexera IT Asset Management	Flexera lets enterprises gain visibility and control of IT assets, reduce ongoing software costs, and maintain continuous license compliance.	ODBC
Forcepoint Web Security Endpoint	Forcepoint Web Security Endpoint enables end-users to authenticate and receive policy enforcement via the Forcepoint Web Security Cloud infrastructure.	ODBC
Forcepoint Web Security Endpoint CSV File	Forcepoint Web Security Endpoint CSV File imports CSV files with device information.	HTTP/HTTPS, SMB
Foreman	Foreman is a free open source project that automates repetitive tasks, quickly deploys applications, and proactively manages server lifecyle, on-premises or in the cloud.	HTTP/HTTPS
ForeScout CounterACT	ForeScout CounterACT platform provides insight into network-connected devices.	HTTP/HTTPS
Fortinet FortiGate	Fortinet FortiGate is a next-generation firewall providing security and visibility for end-to-end protection across the entire enterprise network.	HTTP/HTTPS
FreeIPA	FreeIPA is a free and open-source identity management system for Linux environments.	HTTP/HTTPS
Freshservice	Freshservice is a cloud-based IT help desk and service management solution that enables organizations to simplify their IT operations.	HTTP/HTTPS
G Suite by Google	G Suite is a set of cloud computing, productivity, collaboration, device, user, and data management tools developed by Google.	HTTP/HTTPS
GitHub	GitHub provides hosting for software development version control using Git, including distributed version control and source code management (SCM) functionality.	HTTP/HTTPS
GitLab	GitLab is an open-source DevOps lifecycle tool that provides a wiki, issue-tracking, and continuous integration and deployment pipeline features.	HTTP/HTTPS
Google Cloud Platform (GCP)	Google Cloud Platform (GCP) is a suite of cloud computing services. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning.	HTTP/HTTPS

Guardicore	Guardicore is a data center and cloud security company that protects the organizationâ€™s core assets.	HTTP/HTTPS
HashiCorp Consul	HashiCorp Consul is a multi-cloud service networking platform to connect and secure services across any runtime platform and public or private cloud.	HTTP/HTTPS
Have I Been Pwned	Have I Been Pwned is a website to check if email accounts have been compromised in a data breach.	HTTP/HTTPS
HP Integrated Lights-Out (iLO)	HP Integrated Lights-Out (iLO) is server management software that enables the configuration, monitoring, and updating of HPE servers.	HTTP/HTTPS
HP Network Node Manager i (NNMi)	HP Network Node Manager i (NNMi) is a network health and performance monitoring software with scalability and device support.	HTTP/HTTPS, SMB
HPE Intelligent Management Center (IMC)	HPE Intelligent Management Center (IMC) is a networking solution that delivers management across campus core and data center networks.	HTTP/HTTPS
HyperSQL	The HyperSQL adapter imports device information from an HyperSQL database.	ODBC
IBM BigFix	IBM BigFix provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory functionality.	HTTP/HTTPS
IBM BigFix Inventory	IBM BigFix Inventory gathers information about installed software and hardware in your IT infrastructure.	HTTP/HTTPS
IBM Cloud	IBM's cloud computing platform combines platform as a service (PaaS) with infrastructure as a service (IaaS) and cloud services.	HTTP/HTTPS
IBM Guardium	IBM Guardium prevents leaks from databases, data warehouses, and Big Data environments. It ensures the integrity of information and automates compliance controls across heterogeneous environments.	HTTP/HTTPS
IBM MaaS360 with Watson	IBM MaaS360 with Watson is a Unified Endpoint Management (UEM) platform covering endpoints, end-users, apps, content, and data. It also gives visibility and control to manage mobile devices running iOS, macOS, Android, and Windows.	HTTP/HTTPS
IBM Tivoli Application Dependency Discovery Manager (TADDM)	IBM Tivoli Application Dependency Discovery Manager (TADDM) is a configuration management tool that helps IT operations personnel ensure and improve application availability in application environments.	HTTP/HTTPS

iboss cloud	iboss cloud is a cloud-based platform that secures user internet access in the cloud.	HTTP/HTTPS
Icinga	Icinga is an open-source computer system and network monitoring application. It monitors data centers and clouds availability and performance, gives access to data and raises alerts.	HTTP/HTTPS
Illusive Networks	Illusive Networks deceives cyber attackers by planting false information about a given network's resources.	HTTP/HTTPS
Imperva Data Activity Monitoring (DAM)	Imperva Data Activity Monitoring (DAM) defines and enforces data security and compliance policies across the cloud and on-premises including relational databases, mainframes, big data platforms, data warehouses, and enterprise file stores.	HTTP/HTTPS
Indegy Industrial Cybersecurity Suite	Indegy Industrial Cybersecurity Suite protects industrial networks from cyber threats, malicious insiders, and human error, including threat detection and mitigation, asset tracking, vulnerability management, configuration control, and device integrity checks.	HTTP/HTTPS
Infinipoint	Infinipoint is a cloud-based automated cyber hygiene platform that enables continuous detection and remediation of risks across the organizationâ€™s IT assets.	HTTP/HTTPS
Infoblox DDI	Infoblox DDI consolidates DNS, DHCP, IP address management, and other core network services into a single platform, managed from a common console.	HTTP/HTTPS
Infoblox NetMRI	Infoblox NetMRI provides network change and configuration management (NCCM), enabling users to automate network change, understand network health, manage network configurations, and meet a variety of compliance requirements.	HTTP/HTTPS
IP Fabric	IP Fabric is a network management system used to discover, verify, visualize and document large scale networks.	HTTP/HTTPS
Ivanti Service Manager	Ivanti Service Manager, is a cloud based ITSM solution that provides workflows automation, IT help desk and support ticket features, and ITIL service management processes.	HTTP/HTTPS
Ivanti Unified Endpoint Manager (Landesk)	Ivanti Unified Endpoint Manager (formerly Landesk) helps IT administrators gather detailed device data, automate software and OS deployments, personalize workspace environments, and fix user issues.	HTTP/HTTPS

Jamf Pro	Jamf Pro is an enterprise mobility management (EMM) tool that provides unified endpoint management for Apple devices.	HTTP/HTTPS
JSON	The JSON adapter is able to import .json files with information about devices, users, or installed software.	HTTP/HTTPS, SMB
JumpCloud	JumpCloud is a Directory-as-a-Service (DaaS) solution to authenticate, authorize, and manage users, devices, and applications via a common directory in the cloud.	HTTP/HTTPS
Juniper Junos	The Juniper Junos Adapter connects to Juniper switches and routers.	SSH
Juniper Junos Space Network Management Platform	Juniper Junos Space Network Management Platform automates management of Juniper's switching, routing, and security devices.	HTTP/HTTPS
Kaseya VSA	Kaseya VSA is a remote monitoring and management solution for remote control, discovery, patch management, and monitoring.	HTTP/HTTPS
Kaspersky Security Center	Kaspersky Security Center is an administration console for Kaspersky Labs security solutions and systems management tools.	HTTP/HTTPS
Kenna Security Platform	Kenna Security Platform is a vulnerability assessment solution that provides risk scoring, prioritization, and benchmarking.	HTTP/HTTPS
Keycloak	Keycloak is an open source identity and access management solution.	HTTP/HTTPS
KnowBe4	KnowBe4 provides Security Awareness Training for anti-phising behavior, social engineering and ransomware attacks, and general security awareness.	HTTP/HTTPS
Lansweeper	Lansweeper is an agentless IT asset management and Network Inventory software tool for Microsoft Windows OS.	ODBC
LibreNMS	LibreNMS is a network monitoring solution that provides auto-discovery for network hardware and operating systems including Cisco, Linux, Juniper, Foundry, and more.	HTTP/HTTPS
Linux SSH	Linux Secure Shell (SSH) uses remote command execution over the SSH protocol to gather information about the endpoint Linux machine.	SSH
LogicMonitor	LogicMonitor is an automated infrastructure monitoring platform for enterprise IT and managed service providers.	HTTP/HTTPS
LogRhythm	LogRhythm combines SIEM, user and entity behavior analytics, network traffic and behavior analytics, and security automation and orchestration.	HTTP/HTTPS

Malwarebytes Endpoint Protection (Cloud Platform)	Malwarebytes Endpoint Protection is a cloud-based security platform that combines detection and remediation technologies into a single cloud-managed agent.	HTTP/HTTPS
Malwarebytes Endpoint Security (On-Prem Platform)	Malwarebytes Endpoint Security protects endpoints from ransomware, automates endpoint remediation, and provides continuous visibility and monitoring.	ODBC
ManageEngine Desktop Central	ManageEngine Desktop Central is a desktop management and mobile device management software for managing desktops in LAN and across WAN and mobile devices from a central location.	HTTP/HTTPS
Masscan	Masscan is a free internet port scanner utility.	HTTP/HTTPS, SMB
McAfee ePolicy Orchestrator (ePO)	McAfee ePolicy Orchestrator (ePO) is a security management platform that provides real-time monitoring of security solutions.	HTTP/HTTPS
Medigate	Medigate is a medical device security platform that protects connected medical devices on health care provider networks, allowing inventory management and facilitating detection and prevention capabilities.	HTTP/HTTPS
Men&Mice DNS Management	Men&Mice DNS Management is a Network Management platform providing secure, centralized, and resilient control of DNS across diverse platforms.	HTTP/HTTPS
Micro Focus Server Automation (HP Server Automation, Opsware)	Micro Focus Server Automation (formerly known as HP Server Automation or Opsware) provides operating system provisioning, automated patch management, and compliance control.	HTTP/HTTPS
Microsoft Active Directory (AD)	Microsoft Active Directory (AD) is a directory service for Windows domain networks that authenticates and authorizes all users and computers.	LDAP/LDAPS
Microsoft Azure	Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers.	HTTP/HTTPS
Microsoft Azure Active Directory (Azure AD) and Microsoft Intune	Microsoft Azure Active Directory (Azure AD) is Microsoft's multi-tenant, cloud-based directory, and identity management service. Microsoft Intune is a cloud-based service in the enterprise mobility management (EMM) space that integrates closely with Azure Active Directory (Azure AD) for identity and access control and Azure Information Protection for data protection.	HTTP/HTTPS

Microsoft BitLocker Administration and Monitoring (MBAM)	Microsoft BitLocker Administration and Monitoring (MBAM) provides a simplified administrative interface for BitLocker Drive Encryption. BitLocker offers protection against data theft or data exposure for computers that are lost or stolen, encrypting all data that is stored on the Windows operating system volumes and drives and configured data drives.	ODBC
Microsoft Defender ATP	Microsoft Defender Advanced Threat Protection (ATP) helps enterprise networks prevent, detect, investigate, and respond to advanced threats.	HTTP/HTTPS
Microsoft Hyper-V	Microsoft Hyper-V is a native hypervisor; it can create virtual machines on x86-64 systems running Windows.	WMI
Microsoft Key Management Service (KMS)	Microsoft Key Management Service (KMS) enables organizations to activate systems within their own network, eliminating the need for individual computers to connect to Microsoft for product activation.	ODBC
Microsoft System Center Configuration Manager (SCCM)	Microsoft System Center Configuration Manager (SCCM) is a systems management software product for managing large groups of computers running Windows NT, Windows Embedded, macOS (OS X), Linux or UNIX, as well as Windows Phone, Symbian, iOS and Android mobile operating systems	ODBC
Minerva Labs Endpoint Malware Vaccination	Minerva Labs Endpoint Malware Vaccination simulates infection markers, rather than creating them, to contain outbreaks that bypass AV tools.	HTTP/HTTPS
MobileIron EMM	MobileIron EMM enables enterprises to secure and manage modern operating systems on mobile devices and desktops.	HTTP/HTTPS
NetBox	NetBox is an open source web application to help manage and document computer networks.	HTTP/HTTPS
NetBrain Integrated Edition	NetBrain Integrated Edition is an adaptive automation integrated with existing NMS tools and IT workflows to automate documentation, troubleshooting, network change, and defense.	HTTP/HTTPS
Netskope	Netskope Security Cloud provides threat protection for cloud services, websites, and private applications.	HTTP/HTTPS
Nexthink	Nexthink is an IT solution that provides insights into activity across devices, operating systems, and workplace locations to improve IT experiences for employees.	HTTP/HTTPS
Nmap Security Scanner	Nmap Security Scanner is a free and open source utility for network discovery and security auditing.	HTTP/HTTPS, SMB

Nozomi Networks Guardian	Nozomi Networks Guardian monitors network communications and device behavior for physical and virtual appliances.	HTTP/HTTPS
Nutanix AHV	Nutanix AHV is a hypervisor included with the Enterprise Cloud OS. AHV delivers flexible migrations, security hardening, automated data protection and disaster recovery, and analytics.	HTTP/HTTPS
ObserveIT	ObserveIT provides insider threat security solutions, including employee monitoring, user activity monitoring, behavioral analytics, policy enforcement, and digital forensics.	ODBC
Observium	Observium is an auto-discovering network monitoring platform supporting a wide range of device types, platforms and operating systems.	HTTP/HTTPS
Okta	Okta provides cloud software that helps companies manage their employees' passwords, by providing a â€œsingle sign-onâ€⍰ experience.	HTTP/HTTPS
OmniVista 2500 NMS	The Alcatel-Lucent OmniVista 2500 Network Management System (NMS) provides management tools and network-wide visibility, enabling operators to provision, manage and maintain a mobile infrastructure.	HTTP/HTTPS
OpenStack	OpenStack is an open source software solution for creating private and public clouds.	HTTP/HTTPS
OpenVAS	OpenVAS is a software framework including several services and tools for vulnerability scanning and vulnerability management.	HTTP/HTTPS, SSH
OPSWAT MetaAccess	OPSWAT MetaAccess prevents risky devices from accessing local networks and cloud applications.	HTTP/HTTPS
Oracle Cloud	Oracle Cloud is a computing service providing servers, storage, network, applications and services.	HTTP/HTTPS
Oracle VM	Oracle VM's server virtualization products support x86 and SPARC architectures and a variety of workloads such as Linux, Windows and Oracle Solaris.	HTTP/HTTPS
Orca Cloud Visibility Platform	Orca Cloud Visibility Platform delivers visibility to cloud security posture, including prioritized alerts on vulnerabilities, compromises, misconfigurations, and more.	HTTP/HTTPS

PacketFence	PacketFence is a free open source network access control (NAC) solution which provides the following features: registration, detection of abnormal network activities, proactive vulnerability scans, isolation of problematic devices, remediation through a captive portal, 802.1X, wireless integration and User-Agent / DHCP fingerprinting.	HTTP/HTTPS
Palo Alto Networks Cortex	Palo Alto Networks Cortex is an open and integrated, AI-based continuous security platform, allowing security operations teams to speed the analysis of massive data sets.	HTTP/HTTPS
Palo Alto Networks Cortex XDR	Palo Alto Networks Cortex XDR is a detection and response app that natively integrates network, endpoint, and cloud data to detect threats and stop sophisticated attacks.	HTTP/HTTPS
Palo Alto Networks Panorama	The Palo Alto Panorama management server provides centralized monitoring and management of multiple next-generation firewalls and appliance clusters.	HTTP/HTTPS
Panorays	Panorays is a SaaS-based platform that enables companies to view, manage and engage on the security posture of their third-parties, vendors, suppliers, and business partners.	HTTP/HTTPS
phpIPAM	phpIPAM is an open-source web IP address management application (IPAM).	HTTP/HTTPS
Pivotal Cloud Foundry	Pivotal Cloud Foundry is an app development and deployment platform for public and private clouds.	HTTP/HTTPS
PKWARE	PKWAREâ€™s data protection platform finds, classifies, and protects sensitive data, allowing security managers to define data protection policies and monitor activity across the organization.	HTTP/HTTPS
Preempt	Preempt lets organizations reduce user risk on their attack surface and preempt threats in real-time with conditional access. It continuously analyzes, adapts and responds to threats based on identity, behavior, and risk to resolve insider threats and targeted attacks.	HTTP/HTTPS
Prisma Cloud	Prisma Cloud is a native cloud security platform that provides visibility, threat prevention, compliance assurance, and data protection across multi-cloud environments.	HTTP/HTTPS
PrivX	PrivX provides privileged access to on-prem and cloud environments, including control access to servers, network devices and other critical infrastructure according to user roles and privileges.	HTTP/HTTPS

Promisec Endpoint Manager	Promisec Endpoint Manager is an agentless endpoint detection and remediation solution that detects, analyzes, and remediates abnormalities.	ODBC
Proxmox Virtual Environment (VE)	Proxmox Virtual Environment (VE) is an open source server virtualization management solution based on QEMU/KVM and LXC.	HTTP/HTTPS
Puppet	Puppet is an open-source software configuration management tool.	ODBC
Pure Storage Pure1	Pure Storage Pure1 is a cloud-based storage management solution that provides self-driving storage, data-storage management, and monitoring.	HTTP/HTTPS
Qualys Cloud Platform	Qualys Cloud Platform monitors customers' global security and compliance posture using sensors.	HTTP/HTTPS
Quest KACE Endpoint Systems Management Appliances	Quest KACE Endpoint Systems Management Appliances provision, manage, secure, and service network-connected devices.	HTTP/HTTPS
Rancher	Rancher is an open-source multi-cluster orchestration platform that enables operations teams to deploy, manage and secure enterprise Kubernetes.	HTTP/HTTPS
Randori	Randori is an attack platform which combines continuous reconnaissance, real-time target analysis, and the ability to safely execute attacks on-demand to provide an attackerâ€™s perspective.	HTTP/HTTPS
Rapid7 Nexpose and InsightVM	Rapid7 Nexpose is an on-premise vulnerability management solution, providing discovery, detection, verification, risk classification, impact analysis, reporting and mitigation. Rapid7 InsightVM is a cloud-based vulnerability management solution that combines Rapid7â€™s Insight platform along with Nexpose core capabilities.	HTTP/HTTPS
Rapid7 Nexpose Warehouse	Rapid7 Nexpose Warehouse fetches device information directly from an external data warehouse.	ODBC
Red Canary	The Red Canary suite includes products that record telemetry, detect and investigate threats, and automate remediation.	HTTP/HTTPS
Red Hat Ansible Tower	Red Hat Ansible Tower is a web console and REST API for operationalizing Ansible across teams, organizations, and the enterprise.	HTTP/HTTPS
Red Hat Satellite	Red Hat Satellite is a system management solution used to deploy, configure, and maintain systems across physical, virtual, and cloud environments.	HTTP/HTTPS
RedSeal	RedSealâ€™s network modeling and risk scoring platform models customers' entire hybrid data center of public cloud, private cloud and physical network.	HTTP/HTTPS

Remediant SecureONE (JITA)	Remediant SecureONE is a Just-In-Time Privileged Access Management (JITA) solution that enables control and insight over the distribution, usage, and protection of privileged access across enterprise environments.	ODBC
RescueAssist (GoToAssist)	RescueAssist (formerly GoToAssist) is a cloud-based toolset for IT and customer support teams including remote support, IT monitoring, and service desk management.	HTTP/HTTPS
RiskIQ Digital Footprint	RiskIQ Digital Footprint software provides an active, comprehensive inventory of all of the organizationâ€™s IPs, domains, and hosts.	HTTP/HTTPS
Riverbed SteelCentral Controller (SCC)	Riverbed SteelCentral Controller SCC facilitates administration tasks for groups of SteelHeads, Interceptors, Mobile Controller, Cores, and Edges.	HTTP/HTTPS
Rumble Network Discovery	Rumble Network Discovery is a cloud-based network discovery platform that identifies and monitors network-connected IT assets.	HTTP/HTTPS
Sal	Sal is an open-source reporting solution for managed endpoints.	HTTP/HTTPS
SaltStack Enterprise	SaltStack Enterprise intelligent automation delivers event-driven security, cloud, and configuration management.	HTTP/HTTPS
SaltStack Open Source	SaltStack Open Source is open-source software for event-driven security, cloud and configuration management.	HTTP/HTTPS
Samanage	Samanage is a unified, cloud-based IT service desk and asset management platform.	HTTP/HTTPS
Secdo Endpoint Protection	Secdo Endpoint Protection automates endpoint forensic analysis and cyber investigations for security teams.	HTTP/HTTPS
Secureworks Red Cloak	Secureworks Red Cloak is an endpoint detection and response technology that continuously monitors endpoints for signs of adversary activity.	HTTP/HTTPS
Sensu	Sensu is a cloud monitoring solution that provides monitoring workflow automation and visibility into multi-cloud environments.	HTTP/HTTPS
SentinelOne	SentinelOne is an endpoint protection solution including prevention, detection, and response.	HTTP/HTTPS
ServiceNow	ServiceNow provides service management software as a service, including IT services management (ITSM), IT operations management (ITOM) and IT business management (ITBM).	HTTP/HTTPS

SevOne Data Platform	SevOne Data Platform is a network and infrastructure management platform that provides monitoring and analytics.	HTTP/HTTPS
Shodan	Shodan is a search engine for Internet-connected devices.	HTTP/HTTPS
Signal Sciences	Signal Sciences is a web protection platform that protects on-premise, multi-cloud and hybrid-cloud apps, within containers and serverless functions.	HTTP/HTTPS
Skybox Firewall Assurance	Skybox Firewall Assurance provides automation of firewall management tasks across different firewall vendors and complex rulesets.	HTTP/HTTPS
Slack	Slack is a chat and collaboration hub used to connect people, information, tools, and services.	HTTP/HTTPS
Snipe-IT	Snipe-IT is a free, open source IT asset management system written in PHP.	HTTP/HTTPS
Snow Software Asset Management	Snow Software provides Software Asset Management (SAM) products and services to reduce the risk, cost, and complexity associated with software assets and licensing.	HTTP/HTTPS
SolarWinds Network Performance Monitor	SolarWinds Network Performance Monitor is a unified IT systems management system that tracks the performance of networks, applications, systems, and databases on-premises, in a hybrid environment, or in the cloud.	HTTP/HTTPS
SonicWall	SonicWall next-generation firewalls (NGFW) provide security, control, and visibility to maintain an effective cybersecurity posture.	HTTP/HTTPS
Sophos Cloud Optix	Sophos Cloud Optix is a public cloud visibility and threat response solution that detects, responds, and prevents cloud security and compliance gaps.	HTTP/HTTPS
Sophos Endpoint Protection	Sophos Endpoint Protection helps secure workstations by adding prevention, detection, and response technology on top of the operating system.	HTTP/HTTPS
SOTI MobiControl	SOTI MobiControl is a software system for managing mobile devices in the enterprise.	HTTP/HTTPS
Spacewalk	Spacewalk is an open-source systems management solution for system provisioning, patching and configuration.	HTTP/HTTPS
Specops Inventory	Specops Inventory collects and reports information on hardware, software, registry, user settings, operating system, security data, and Active Directory data.	ODBC
Spiceworks	Spiceworks provides network monitoring to capture, analyze, and monitor network traffic.	HTTP/HTTPS

Splunk	Splunk captures, indexes, and correlates real-time data in a searchable repository.	HTTP/HTTPS
SQL Server	The SQL Server adapter imports device information from arbitrary SQL servers: Microsoft SQL Server, MySQL, Oracle and PostgreSQL.	ODBC
SQLite	The SQLite adapter imports device information from an SQLite database.	ODBC
Sumo Logic	Sumo Logic is a cloud-based service for logs & metrics management for modern apps.	HTTP/HTTPS
Symantec Cloud Workload Protection (CWP)	Symantec Cloud Workload Protection (CWP) automates security policy enforcement to protect public cloud workloads.	HTTP/HTTPS
Symantec Control Compliance Suite (CCS)	Symantec Control Compliance Suite (CCS) is a solution to help identify security gaps and vulnerabilities and automate compliance assessments for over 100 regulations, mandates, and best practice frameworks including GDPR, HIPAA, NIST, PCI and SWIFT. Symantec CCS discovers and inventories all networks and assets including managed and unmanaged devices allowing for assets to be profiled and ranked for risk potential.	HTTP/HTTPS
Symantec DLP	Symantec DLP is a data loss protection and prevention solution. Its management console, the DLP Enforce Platform, and its reporting tool, IT Analytics for DLP, allows writing and enforce policies to reduce information risks.	ODBC
Symantec Endpoint Encryption	Symantec Endpoint Encryption combines full-disk and removable media encryption with centralized management to protect sensitive information and ensure regulatory compliance.	ODBC
Symantec Endpoint Management Suite (Altiris)	Symantec Endpoint Management Suite (formerly Altiris) manages, patches, and remediates application and OS configurations on desktops, laptops and servers to strengthen endpoint security and maximize user productivity.	ODBC
Symantec Endpoint Protection 12.x	Symantec Endpoint Protection manages events, policies, and registration for the client computers that connect to customer networks.	ODBC
Symantec Endpoint Protection 14.x	Symantec Endpoint Protection manages events, policies, and registration for the client computers that connect to customer networks.	HTTP/HTTPS

Symantec Endpoint Protection Cloud	Symantec Endpoint Protection Cloud unifies threat protection and device management for PC, Mac, mobile devices, and servers to protect endpoints from ransomware, zero-day threats, and other sophisticated attacks.	HTTP/HTTPS
SysAid	SysAid is an integrated ITSM, Service Desk and Help Desk software solution.	HTTP/HTTPS
Tanium Asset	Tanium Asset provides an inventory of hardware and software assets including servers, laptops, and desktops for thorough insight.	HTTP/HTTPS
Tanium Discover	Tanium Discover scans for unmanaged assets with almost no impact on the network.	HTTP/HTTPS
Tanium Interact	Tanium Interact lets you ask questions to gather live endpoint data in order to create an up-to-date inventory of hardware and software assets.	HTTP/HTTPS
Tanium System Status	Tanium System Status provides an inventory of all clients that have registered with the Tanium platform.	HTTP/HTTPS
Tenable Nessus	Tenable Nessus is a vulnerability scanning platform for auditors and security analysts.	HTTP/HTTPS
Tenable Nessus CSV File	Tenable Nessus CSV File Adapter imports device information from vulnerability scan data.	HTTP/HTTPS, SMB
Tenable.io	Tenable.io automatically discovers and assesses a customer's environment for vulnerabilities, misconfigurations, and other cybersecurity issues.	HTTP/HTTPS
Tenable.sc (SecurityCenter)	Tenable.sc (formerly SecurityCenter) consolidates and evaluates vulnerability data, prioritizing security risks.	HTTP/HTTPS
Torii	Torii is a SaaS Management Platform letting IT professionals discover, optimize, and control SaaS usage and costs.	HTTP/HTTPS
Trend Micro Apex One (OfficeScan)	Trend Micro Apex One (formerly OfficeScan) is an endpoint security solution protecting against malware, scripts, injection, ransomware, memory and browser attacks, and exploits.	HTTP/HTTPS
Trend Micro Deep Security	Trend Micro Deep Security can automatically virtually patch server, cloud, VDI and application vulnerabilities.	HTTP/HTTPS
Tripwire Enterprise	Tripwire Enterprise is a security configuration management (SCM) suite that provides fully integrated solutions for policy, file integrity and remediation management.	HTTP/HTTPS
TrueFort	TrueFort offers application behavior analytics, control, and protection.	HTTP/HTTPS

Twistlock	Twistlock provides container and cloud native cybersecurity for teams using Docker, Kubernetes, serverless, and other cloud native technologies.	HTTP/HTTPS
Ubiquiti Networks UniFi Controller	The UniFi Controller is a wireless network management software solution for managing multiple wireless networks using a web browser.	HTTP/HTTPS
UpGuard CyberRisk	UpGuard CyberRisk provides third-party vendor risk and external cyber risk monitoring. The platform has two main modules: UpGuard BreachSight which monitors company external risk posture and Vendor Risk monitors and helps manages the risk posture of third party vendors.	HTTP/HTTPS
Vectra AI	Vectra AI is a cybersecurity platform that uses AI to detect and respond to cyberattacks.	HTTP/HTTPS
VMWare ESXi	VMware ESXi is an enterprise-class, type-1 hypervisor for deploying and serving virtual computers.	HTTP/HTTPS
VMware vCloud Director	VMware vCloud Director is a cloud service-delivery platform.	HTTP/HTTPS
VMWare Workspace ONE (AirWatch)	VMWare Workspace ONE (formerly AirWatch) provides enterprise mobility management (EMM) software and standalone management systems for content, applications, and email.	HTTP/HTTPS
Wazuh	Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.	HTTP/HTTPS
Web Server Information	Web Server Information provides information about the web server for a given website domain, including the server type, its version and operating system, the content management system (CMS) name and its version, the installed CMS plugins, versions and more.	HTTP/HTTPS
Webroot Endpoint Protection	Webroot Endpoint Protection protects against threats across email, browsers, files, URLs, ads, apps, and more.	HTTP/HTTPS
Windows Management Instrumentation (WMI)	Windows Management Instrumentation (WMI) is a set of specifications from Microsoft for consolidating the management of devices and applications in a Windows network. WMI provides users with information about the status of local or remote computer systems.	WMI, SMB
Windows Server Update Services (WSUS)	Windows Server Update Services (WSUS), previously Software Update Services (SUS), enables administrators to manage the distribution of updates and hotfixes released for Microsoft products.	WMI, SMB

Workday	Workday offers software solutions for financial management, human resources, and planning.	HTTP/HTTPS
Zabbix	Zabbix is an open source monitoring software tool for networks, servers, virtual machines and cloud services.	HTTP/HTTPS
Zoom	Zoom is a remote conferencing service that provides video conferencing, online meetings, chat, and mobile collaboration.	HTTP/HTTPS
Zscaler Web Security	Zscaler Web Security is a secure Internet and web gateway service that stops malware, advanced threats, phishing, browser exploits, malicious URLs, botnets, and more.	HTTP/HTTPS