National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Forescout eyeInspect v5.2

Report Number: CCEVS-VR-VID11499-2024
Version: 1.0
Date: December 27, 2024

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers, Senior Validator - Aerospace Corporation
Farid Ahmed, Lead Validator - Johns Hopkins University Applied Physics Lab
Robert Wojcik, Lead Validator (Trainee) - Johns Hopkins University Applied Physics Lab
Michael Smeltzer, ECR Team (Trainee) - Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Rachel Kovach
Evan Seiz
Kelvert Ballantyne

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Forescout eyeInspect v5.2 provided by Forescout Technologies, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in December 2024. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *collaborative Protection Profile for Network Devices Version 2.2e* (NDcPP).

The Forescout eyeInspect v5.2 product is a distributed TOE network device that include hardware and software. Forescout eyeInspect v5.2 consists of a Command Center and one or more Sensors. The TOE contains the following models for each TOE component:

- Command Center: Forescout FS-HS-5160-OT
- Sensors: Forescout FS-HW-5120, Forescout FS-HW-5160, Forescout FS-HW-4130, and Forescout FS-HW-2130

The minimum configuration for a deployment of Forescout eyeInspect is one Command Center and one Sensor. Only one Command Center can be deployed as part of the operational configuration. Including additional Sensors within a deployment of Forescout eyeInspect as part of the operational configuration will not affect the validity of the functional claims made within this document and the Common Criteria certification.

Forescout eyeInspect's primary purpose is to help reduce risk, automate compliance, and optimize threat analysis for industrial operations management technology within a network. The Command Center provides the main interface for management of eyeInspect, including the ability to manage eyeInspect configuration, manage Sensors, and perform analytics on collected device and threat data. Meanwhile, eyeInspect Sensor(s) receive device information gathered from within the network and send it to the Command Center for analysis. A Forescout eyeInspect deployment consists of one Command Center and at least one Sensor. The Command Center and the Sensor(s) work together to provide visibility and an understanding of security posture for Industrial Control System and Supervisory Control and Data Acquisition (ICS/SCADA) networks.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Forescout eyeInspect v5.2 Security Target v1.0*, dated November 29, 2024, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Forescout eyeInspect v5.2 Refer to Tables 2 and 3 for TOE Component and their model specifications
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Forescout eyeInspect v5.2 Security Target v1.0, dated November 29, 2024
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Forescout eyeInspect v5.2" Evaluation Technical Report v1.0 dated December 6, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Forescout Technologies, Inc.
Developer	Forescout Technologies, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Jerome Myers, Senior Validator - Aerospace Corporation Farid Ahmed, Lead Validator - Johns Hopkins University APL Robert Wojcik, Lead Validator (Trainee) - Johns Hopkins University APL Michael Smeltzer, ECR Team (Trainee) - Johns Hopkins University APL

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.
- It is assumed that availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components, and that the TOE components audit functionality is running.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
- **T.WEAK_CRYPTOGRAPHY –** Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
- **T.WEAK_AUTHENTICATION_ENDPOINTS –** Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the

Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

- **T.UPDATE_COMPROMISE –** Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
- **T.UNDETECTED_ACTIVITY** – Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE –** Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
- **T.PASSWORD_CRACKING –** Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *collaborative Protection Profile for Network Devices, Version 2.2e* 27 March 2020, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the Forescout eyeInspect v5.2 product's purpose of reducing

risk, automating compliance, and optimizing threat analysis for industrial operations management technology within network capabilities described in Section 1.3 of the Security Target were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The TOE is a network device as defined in the NDcPP which states: "a device that is connected to a network and has an infrastructure role within that network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfil the requirements of this cPP…". The Forescout eyeInspect v5.2 product is a distributed TOE network device that include hardware and software. Forescout eyeInspect v5.2 consists of a Command Center and one or more Sensors. The TOE contains the following models for each TOE component:

- Command Center: Forescout FS-HS-5160-OT
- Sensors: Forescout FS-HW-5120, Forescout FS-HW-5160, Forescout FS-HW-4130, and Forescout FS-HW-2130

The minimum configuration for a deployment of Forescout eyeInspect is one Command Center and one Sensor. Only one Command Center can be deployed as part of the operational configuration. Including additional Sensors within a deployment of Forescout eyeInspect as part of the operational configuration will not affect the validity of the functional claims made within this document and the Common Criteria certification. Thus, the TOE is a network device, comprised of multiple TOE components that are composed of hardware and software.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following TOE components and their respective models:

TOE Component Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout eyeInspect: Command Center	Forescout eyeInspect v5.2 operating on Linux Ubuntu 20.04.6 LTS OS	Forescout FS-HS-5160-OT	1U Desktop, 19" rack server
			CPU Xeon Gold 6132 2x 14C/28T
			1/10 GB Network card
			8 Copper, 2 Fiber, 2 unused SFP Ports

Table 2: Forescout eyeInspect Command Center

TOE Component Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout eyeInspect: Sensors	Forescout eyeInspect v5.2 operating on Linux Ubuntu 20.04.6 LTS OS	Forescout FS-HW-5120	1U rackmount
			CPU Intel Xeon Silver 4114 2x 10C/20T
			1GB out of band management port
			4x 10/100/1000 Mbps Ethernet
			4x 1G/10G dual rate SR 2x Fiber SFPs included in base configuration
		Forescout FS-HW-5160	1U rackmount
			CPU Xeon Gold 6132 2x 14C/28T
			1GB out of band management port

			4x 10/100/1000 Mbps Ethernet
			4x 1G/10G dual rate SR 2x Fiber SFPs included in base configuration
		Forescout FS-HW-4130	1U rackmount
			Gen 8 Intel Core i5-8500T 6C/6T CPU 64bit
			2 x 10/100/1000 Mbps Ethernet (i210-IT & i219-LM)
			4 x 10/100/1000 Mbps Ethernet (i210-IT)
		Forescout FS-HW-2130	Shelf/desktop (31 x 100 x 125 mm.)
			Intel Celeron J3455 1.50 GHz 4C/4T CPU 64bit
			2-4 x Intel 10/100/1000 Mbps Ethernet (i210AT)

Table 3: Forescout eyeInspect Sensors

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Component	Definition
Terminal	A terminal is a device that handles the input and display of data when connected to an appliance's serial port. A terminal client, such as *Hyper Terminal* (Windows) or *minicom* (Linux) can be used on a general purpose computer. The TOE's CLI can be accessed locally with a physical connection to the TOE using the designated management port and must use a terminal emulator that is compatible or use the keyboard and display ports. The terminal client (emulator) must support the following parameters: • Baud: 19200 • Parity: None • Data Bit: 8 • Stop Bits: 1 • Flow Control: None (*minicom* enables flow control by default-edit its configuration to disable this) • Emulation: ANSI (at least for *minicom*)
Remote Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. For the TOE to be managed remotely the Remote Management Workstation is required to have: • SSHv2 client installed to access the TOE's CLI on both TOE components • Web browser installed to access the Web GUI on the Command Center TCP communications from the Remote Management Workstation to the TOE is secured using: • SSH for remote access to the CLI • HTTPS for remote access to the Web GUI The TOE acts as a server for both protocols.
Audit Server	The TOE connects to an audit server to send the audit records for remote storage via SSH connection where the TOE is the SSH client. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.

Monitored Network	The monitored network contains operational technology components, Industrial Control Systems, Supervisory Control and Data Acquisition systems, etc. Figure 1 identifies these as a single interface. The interface to the manage the Forescout eyeInspect product is a separate connection from that of the monitored network that the Forescout eyeInspect product is managing. The Forescout eyeInspect's management of the monitored network is out of scope for the NDcPP.

Table 4 – IT Environment Components

5 Security Policy

5.1.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events for all components of the TOE. Both the Command Center and the Sensor store audit logs locally. The TOE supports forwarding audit records to an external audit server at a predefined frequency. There is no direct connection between the Sensors and the remote audit server. Therefore, audit events from the Sensors are first forwarded to the Command Center, and then forwarded to the remote audit server by the Command Center. The Command Center also forwards its audit records directly to the external audit server. In the evaluated configuration, the audit data is securely transmitted to the audit server using a SSHv2 communication channel.

5.1.2 Cryptographic Support

The TOE provides cryptography in support of TLS (v1.2), HTTPS, and SSH trusted communications. The Command Center utilizes Bouncy Castle for TLS and HTTPS communications, and OpenSSL for SSH communications. The Sensor utilizes OpenSSL for TLS and SSH communication. The TOE destroys keys when no longer needed. The following table identifies the cryptographic services per cryptographic library.

SFR		Command Center		Sensors
		Bouncy Castle	**OpenSSL**	**OpenSSL**
FCS_CKM.1	ECC using NIST curves P-256, per FIPS PUB 186-4	#A6120	#A6128	#A6128
	FFC using safe-prime groups NIST Special Publication 800-56A Revision 3 and RFC 3526.	N/A – Bouncy Castle does not provide FFC services	#A6128	#A6128
FCS_CKM.2	Elliptic curve-based key establishment NIST Special Publication 800-56A Revision 3	#A6120	#A6128	#A6128
	FFC using safe-prime NIST Special Publication 800-56A Revision 3 and groups listed in RFC 3526.	N/A – Bouncy Castle does not provide FFC services	#A6128	#A6128
FCS_COP.1/ DataEncryption	AES GCM 256 bits	#A6120	N/A	#A6128
	AES CTR 256 bits	N/A	#A6128	#A6128
FCS_COP.1/ SigGen	RSA FIPS 186-4 Signature Services 2048 bits	#A6120	N/A	#A6128
	ECDSA FIPS 186-4 Signature Services 256 bits	N/A	#A6128	#A6128
FCS_COP.1/ Hash	SHA-256	#A6120	#A6128	#A6128
	SHA-384	#A6120	N/A	#A6128
	SHA-512	#A6120	#A6128	#A6128
FCS_COP.1/ KeyedHash	HMAC-SHA-256	N/A	#A6128	#A6128
	HMAC-SHA-384	#A6120	N/A	#A6128
	HMAC-SHA-512	N/A	#A6128	#A6128
FCS_RBG_EXT.1	Hash DRBG	#A6120	N/A	N/A

	CTR_DRBG	N/A	#A6128	#A6128

Table 5 – Cryptographic Algorithm Table

5.1.3 Communication

Initial TLS communications between TOE components does not occur until the Sensor is configured and enabled by the Security Administrator. Once enabled the Sensor application will send a request for enrollment, via TLS, to the configured Command Center, where the Security Administer must approve before full communications are established.

5.1.4 Identification and Authentication

The TSF provides a configurable number of maximum consecutive authentication failures that are permitted by a user. Once this number has been met, the account is locked for a configurable time interval or until a Security Administrator manually unlocks the account. Additionally, a Security Administrator can define the minimum password length. The displaying of a pre-authentication warning banner is the only function available prior to user authenticating.

The TOE provides a native password authentication mechanism for Web GUI and CLI users. The inter-TOE TLS client functionality on the Sensor performs the validation, without revocation checking, of the presented X.509v3 certificates from the Command Center server.

5.1.5 Security Management

The TOE uses role-based access control to prevent unauthorized management of and access to TSF data. The TOE provides a Security Administrator role that can be assigned to a user which provides the ability to administer the TOE locally and remotely.

5.1.6 Protection of the TSF

The TOE ensures the security and integrity of all data that is stored locally and accessed locally or remotely. User authentication passwords are not stored in plaintext. The Security Administrator is required to manually initiate the update process on the Command Center and the Sensors; as the TOE does not support automatic updates. The TOE automatically verifies the digital signature of the software update prior to installation and if the digital signature is found to be invalid, the update is not installed. The current executing version of the TOE software is displayed upon login. The TOE implements a self-testing mechanism that is automatically executed upon startup. The TOE provides its own time via the underlying OS's internal clock and a Security Administrator has the ability to manually set the time.

5.1.7 TOE Access

The TOE displays a configurable warning banner prior to user authentication. Remote and local sessions are terminated after an administrator-configurable time period of inactivity. Users are allowed to terminate their own interactive session. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session.

5.1.8 Trusted Path/Channels

Security Administrators can remotely manage the Command Center through an SSH channel to access the CLI or HTTPS to access the Web GUI. The Command Center uses a SSH connection to the audit server for remote audit storage.

Security administrators can remotely manage the Sensor through an SSH channel to access the CLI. The Sensor communicates with the Command Center via secure TLS channels.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

[1] Forescout eyeInspect v5.2 Supplemental Administrative Guidance for Common Criteria- v1.0, 03 Dec 2024
[2] Forescout eyeInspect Installation Guide, v5.2 – Revision 2, 26 Oct 2023
[3] Forescout eyeInspect Configuration Guide, v5.2 , 10 Jul 2023

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the Forescout eyeInspect v5.2 which consists of a Command Center and one or more Sensors. The TOE contains the following models for each TOE component:

- Command Center: Forescout FS-HS-5160-OT
- Sensors: Forescout FS-HW-5120, Forescout FS-HW-5160, Forescout FS-HW-4130, and Forescout FS-HW-2130

The minimum configuration for a deployment of Forescout eyeInspect is one Command Center and one Sensor. Only one Command Center can be deployed as part of the operational configuration. Including additional Sensors within a deployment of Forescout eyeInspect as part of the operational configuration will not affect the validity of the functional claims made within this document and the Common Criteria certification.

Section 4.2 of this document describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- Terminal
- Remote Management Workstation
- Audit Server
- Monitored Network

To use the product in the evaluated configuration, the product must be configured as specified in the *Forescout eyeInspect v5.2 Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "Forescout eyeInspect v5.2" Assurance Activities Report v1.0,* dated December 6, 2024.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *Forescout eyeInspect v5.2 Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network. Testing was performed against all two management interfaces defined in the ST (local CLI, remote CLI).

The TOE was configured to communicate with the following environment components:

- Function: Audit Server
  - Linux forescout-2023-syslog 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64 GNU/Linux
  - Protocols: SSH
  - Tools:
    - tcpdump version 4.99.0
    - rsyslogd 8.2102.0 (aka 2021.02)

- Function: Switch
  - Model: Cisco Catalyst WS-C Switch, WS-C3560X-24P
  - OS: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 12.2(55)SE3
  - Protocols: N/A

- Function: Switch
  - Model: Cisco Catalyst WS-C Switch, WS-C2960-24TT-L
  - OS: Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(50)SE4
  - Protocols: N/A

The following machines were used as the Management Workstations ("Test Workstation") for local and remote administration:

- Function: 3 x Administrator Test Workstation
  - Platform: Dell Precision M4800 Laptop/
  - OS: Windows 10 Version 21H2
  - Protocols: TLS, SSH
  - Tools:
    - Wireshark: version 3.6.7
    - PuTTY .73
    - nmap

- Function: CATL Test Workstation
  - Platform: VMware ESXi based Virtual Machine
  - OS: (Kali GNU/Linux Rolling 2018.3 Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64 GNU/Linux
  - Protocols: TLS, SSH

- Tools:
  - Wireshark: version 3.6.7
  - PuTTY .73
  - Ettercap - Man-in-the-Middle (MITM) Packet Modification Tool
  - Modified SSH client for sending large packets for Test Case 010
  - Nmap 7.93
  - Ncat 7.19
  - OpenSSL 1.1.1k

- Function: Test Machine for Configuration 2 and 3
  - Linux forescout-2023-syslog 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64 GNU/Linux
  - Protocols: SSH
  - Tools:
  - tcpdump version 4.99.0
  - rsyslogd 8.2102.0 (aka 2021.02)
  - Nmap 7.93
  - Ncat 7.19
  - OpenSSL 1.1.1k

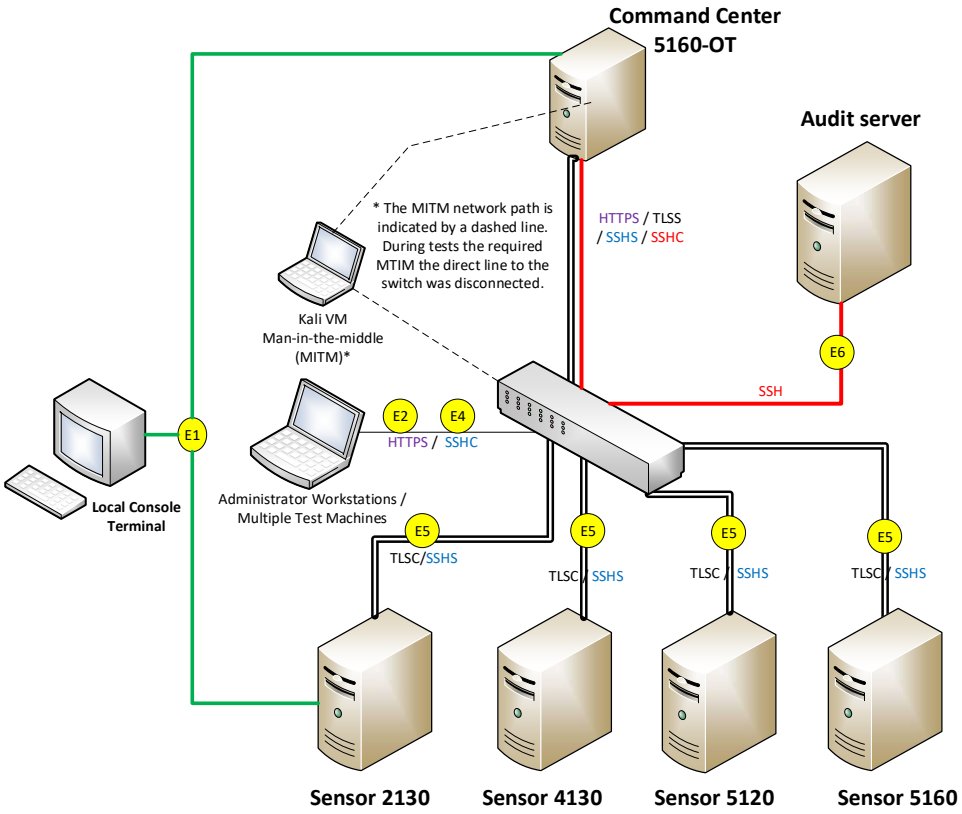

Figure 1 - Test Configuration

- **E1: Terminal to Command Center** – The Terminal utilizes a direct local connection to the Command Center through a designated management port. The Terminal provides a Command Line Interface (CLI) for local management of Command Center.

- **E2: Remote Management Workstation to Command Center** – The Remote Management Workstation allows a Security Administrator to access either the Web GUI or remote CLI for remote administration of the Command Center. These connections are bundled together in Figure 1 as connection E2.
    - The Command Center can be accessed via the Web GUI using a HTTPS connection over a standard browser. In this case, the Command Center acts as an HTTPS server to the standard browser used on the Remote Management Workstation.
    - The Command Center can be accessed via a remote CLI using a SSH connection. The Command Center acts as an SSH server to the SSH Client used on the Remote Management Workstation.
- **E3: Terminal to Sensor** – The Terminal provides a CLI for local management of a Sensor. The Terminal utilizes a direct local connection to the Sensor through monitoring ports.
- **E4: Remote Management Workstation to Sensor** – The Remote Management Workstation provides a remote management interface for a Sensor deployed in an operational configuration of the TOE. The Sensor acts as an SSH server to the SSH Client used on the Remote Management Workstation. There is no Web GUI available for remote administration of a Sensor.
- **E5: Sensor to Command Center** – A Sensor communicates with the Command Center via two secure TLS channel. These connections are used for the Command Center to manage a Sensor installed in a deployment of the TOE, send audit data from the Sensors to the Command Center, and to send collected network data from the Sensors to the Command Center.
- **E6: Command Center to Audit Server** – The Command Center communicates with an external Audit server via a secure SSH channel for external audit record storage.

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that

interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords (version information used for refining results) were identified:

Keyword	Description
Forescout	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
eyeInspect	This is a generic term for searching for known vulnerabilities for the specific product.
Forescout FS-HS-5160-OT	Specific models search / nomenclature search
Forescout FS-HW-5120,	Specific models search / nomenclature search
Forescout FS-HW-5160,	Specific models search / nomenclature search
Forescout FS-HW-4130,	Specific models search / nomenclature search
Forescout FS-HW-2130	Specific models search / nomenclature search
Linux Ubuntu 20.04.2 LTS	This is a term for searching for known vulnerabilities for the underlying OS. A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately. Bearing in mind that this is a locked operating system that has been enhanced by the vendor who is not using the full functionality of the OS.
Generic Terminology	
Network Monitor	Generic term
Command Center	Generic term
Passive Sensor	Generic term
Libraries	See separately provided library documents. The list of libraries are proprietary/supplemental and not provided in the VR report.
Hardware	
Xeon Silver and Gold (Skylake) BIOS upgraded 2.13.3 Xeon Silver 4114 Xeon Gold 6132	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Gen 8 Intel® Core™ i5-8500T (Coffee Lake)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Celeron J3455	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on November 15, 2024. The following public vulnerability sources were searched:

- NIST National Vulnerabilities: https://web.nvd.nist.gov/view/vuln/search

- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning / Nessus scanner
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration. Any unknown ports will be further explored using a Nessus scanner.
- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by exploiting a vulnerability in OpenSSH as described in CVE-2018-15473.
- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Forescout eyeInspect v5.2 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Forescout eyeInspect v5.2 Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, routers, switches, and other network infrastructure, need to be assessed separately and no further conclusions can be drawn about their effectiveness. The Forescout eyeInspect product's capabilities to reduce risk, automate compliance, and optimize threat analysis for industrial operations management technology within a network, and to provide visibility and an understanding of security posture for Industrial Control System and Supervisory Control and Data Acquisition (ICS/SCADA) networks, described in Section 1.3 of the Security Target, were not assessed as part of this evaluation.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Forescout eyeInspect v5.2 Security Target v1.0, dated November 29, 2024*.

13 List of Acronyms

Acronym	Definition
CA	Certificate Authority
CC	Common Criteria
CLI	Command-line Interface
CPU	Central Processing Unit
DB	Database
DRBG	Deterministic Random Bit Generator
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ICS	Industrial Control System
IT	Information Technology
NDcPP	Collaborative Protection Profile for Network Devices
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OE	Operation Environment
OS	Operating System
OT	Operational Technology
PP	Protection Profile
RAM	Random Access Memory
RBAC	Role-Based Access Control
RU	Rack Unit
SAR	Security Assurance Requirement
SCADA	Supervisory Control and Data Acquisition
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSL	Secure Sockets Layer
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

14 Terminology

Term	Definition
Target of Evaluation (TOE)	A set of software, firmware and/or hardware possibly accompanied by guidance. For this document, the TOE is the evaluated Forescout eyeInspect product configured to meet its security claims.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.

Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
TOE Security Function (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.
TSF Data	Data for the operation of the TSF upon which the enforcement of the requirements relies.
Security Administrator	The class of TOE administrators that are tasked with managing the TOE's functional and security configuration. Embodies those administrators that have access to the local and remote administrative interfaces. For the local and remote CLI, the Security Administrator is the *silentdefense* user. For the Web GUI, the Security Administrator is the Admin user.
Command Center	A component of Forescout eyeInspect used for collecting and processing data reported by the Sensors in a deployment of Forescout eyeInspect. The Command Center also supports a web interface for management of the TOE.
Local Command Line Interface (CLI)	The local CLI is utilized to perform administrative management functions on the Command Center or Sensor at the base operating system level. This interface is accessible through a terminal that is connected directly to the product's Command Center or Sensor component.
Remote CLI	The remote CLI is utilized to perform administrative management functions on the Command Center or Sensor at the base operating system level. This interface is accessible over a secure SSH trusted channel from a management workstation to the product's Command Center or Sensor component.
Remote Management Workstation	A standard PC used for remote access to the TOE via either the Web GUI (HTTPS) or remote CLI (SSH).
Sensor	A component of Forescout eyeInspect used for monitoring Industrial Control System and Supervisory Control and Data Acquisition (ICS/SCADA) networks that it is deployed in. The Sensor is a managed component of the Command Center.
Terminal	The device that is connected directly to the appliance through the keyboard/video ports or a serial port. The device will act as a terminal emulator that is compatible with serial communications used for access to the local CLI.
Web Graphical User Interface (GUI)	The Web GUI is utilized to perform administrative management functions on the Command Center. This interface is accessible over a secure HTTPS trusted channel from a management workstation to the product's Command Center.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-001
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-002
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-003
4. Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-004
5. collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020
6. Forescout eyeInspect v5.2 Security Target v1.0, dated November 29, 2024
7. Forescout eyeInspect v5.2 Supplemental Administrative Guidance for Common Criteria-v1.0
8. Forescout eyeInspect Installation Guide, v5.2 – Revision 2, 26 Oct 2023
9. Forescout eyeInspect Configuration Guide, v5.2 , 10 Jul 2023
10. Assurance Activity Report for a Target of Evaluation "Forescout eyeInspect v5.2" Assurance Activities Report v1.0, dated December 2, 2024