National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report for

Forescout eyeSight v9.1

Report Number: CCEVS-VR-VID11591-2025
Version: 1.0
Date: October 1, 2025

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
The Aerospace Corporation

Farid Ahmed, Lead Validator
Robert Wojcik, Lead Validator (Trainee)
Michael Smeltzer, ECR Team
Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Herbert Markle
David Cornwell
Kelvert Ballantyne
Rachel Kovach
Evan Seiz

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 EXECUTIVE SUMMARY 4
2 IDENTIFICATION 5
3 ASSUMPTIONS AND CLARIFICATION OF SCOPE 6
4 ARCHITECTURAL INFORMATION 9
5 SECURITY POLICY **12**
6 DOCUMENTATION **14**
7 EVALUATED CONFIGURATION **15**
8 IT PRODUCT TESTING **16**
9 RESULTS OF THE EVALUATION **20**
10 VALIDATOR COMMENTS AND RECOMMENDATIONS **22**
11 ANNEXES **23**
12 SECURITY TARGET **24**
13 LIST OF ACRONYMS **25**
14 TERMINOLOGY **26**
15 BIBLIOGRAPHY **27**

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Forescout eyeSight v9.1 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 September 2025. 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 3.0e, (NDcPP), December 6, 2023 and *Functional Package for Secure Shell (SSH),* Version 1.0, (SSH FP), May 13, 2021.

The Target of Evaluation (TOE) is the Forescout hardware that runs the Forescout eyeSight software version 9.1. Forescout's primary purpose is to dynamically identify and evaluate network infrastructure, devices and applications connected to the network, and provide enforcement of Network Access Policy (NAC) and Enterprise Conformance Policies. The TOE type is justified because the TOE provides an infrastructure role in internetworking of different network environments across an enterprise. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP and SSH FP.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the *Common Methodology for Information Technology Security Evaluation* (Version 3.1, Rev 5) for conformance to the *Common Criteria for Information Technology Security Evaluation* (Version 3.1, Rev 5), as interpreted by the Evaluation Activities contained in the NDcPP and SSH FP. 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 and SSH FP Evaluation Activities. The validation team found that the evaluation showed that the product satisfies all 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 eyeSight v9.1 Security Target*, v2.0, dated September 09, 2025 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 a Protection Profile containing Evaluation Activities, which are interpretations of CEM v3.1 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 eyeSight hardware that runs the Forescout eyeSight software version 9.1. Refer to Table 2 for Model Specifications
Protection Profile	*collaborative Protection Profile for Network Devices*, Version 3.0e, December 6, 2023 *Functional Package for Secure Shell (SSH),*Version 1.0, May 13, 2021 Including all applicable NIAP Technical Decisions and Policy Letters
Security Target	*Forescout eyeSight v9.1 Security Target*, v2.0, dated September 9, 2025
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation "Forescout eyeSight v9.1" Evaluation Technical Report (ETR)*, v1.0 dated September 10, 2025
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 - The Aerospace Corporation Farid Ahmed, Lead Validator - JHU Applied Physics Laboratory Robert Wojcik, Lead Validator (Trainee) - JHU Applied Physics Laboratory Michael Smeltzer, ECR Team - JHU Applied Physics Laboratory

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.
- 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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
- **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 3.0e, December 6, 2023 and *Functional Package for Secure Shell (SSH)*, Version 1.0, May 13, 2021, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP and SSH FP are claimed by the TOE and documented in the ST.

- Consistent with the expectations of the Protection Profiles, 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 v3.1 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. The product's capabilities to dynamically identify and evaluate network infrastructure, devices and applications connected to the network, and provide enforcement of Network Access Policy (NAC) and Enterprise Conformance Policies–as described in Section 1.4 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.

The evaluated configuration of the TOE is the Forescout eyeSight described in Table 2, running the Forescout eyeSight software version 9.1. In the evaluated configuration, the TOE uses TLS to secure remote GUI-based administration, SSH to secure remote command-line administration, and TLS to secure transmissions of security-relevant data from the TOE to external entities such as Active Directory and Audit Server. The TOE includes administrative guidance to instruct Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

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 the Forescout eyeSight 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…" Additionally, the NDcPP says that example devices that fit this definition include "physical and virtualised routers, firewalls, VPN gateways, IDSs, and switches".

The TOE is a standalone network device, composed of hardware and software, that is connected to the network and enables network access control, threat protection, and compliance of the entire enterprise based on network security policies. Therefore, the TOE provides an infrastructure role in internetworking of different network environments across an enterprise.

The Forescout eyeSight products are devices used to dynamically identify and evaluate network infrastructure, devices and applications connected to the network, and to provide enforcement of Network Access Policy (NAC) and Enterprise Conformance Policies. Based on the TOE being a network device that provides an infrastructure role within a network, the TOE product type classification is justified and the NDcPP conformance claim is appropriate.

4.2 Physical Boundary

The following figure depicts the TOE boundary and operational environment:

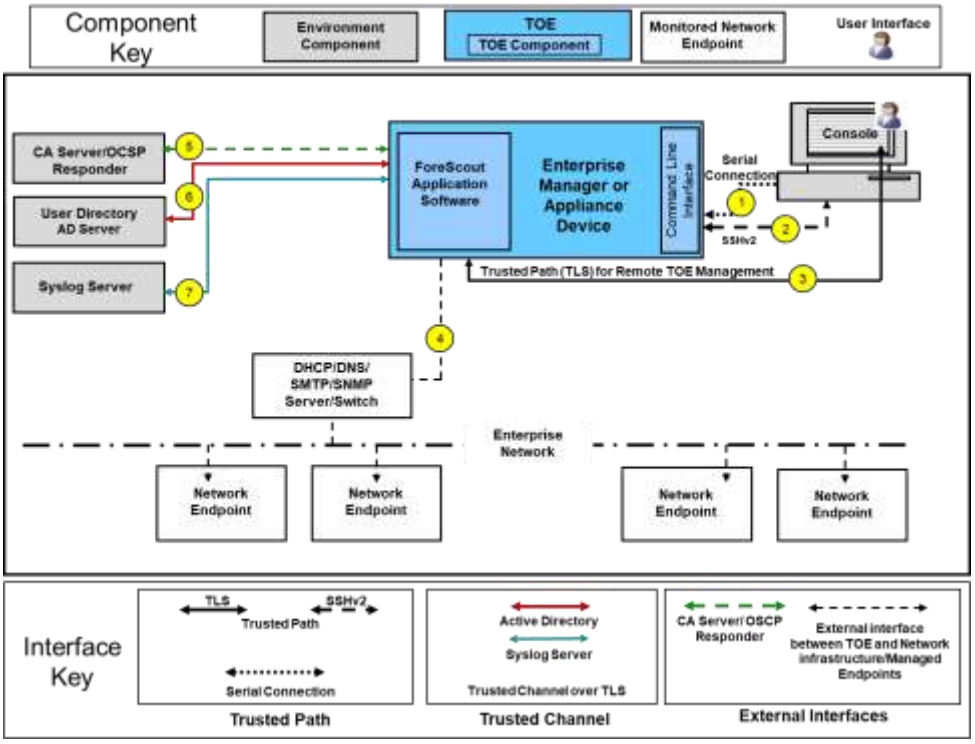

Figure 1: TOE Boundary

As illustrated in Figure 1, the Forescout eyeSight device is responsible for all the security functions of the TOE, as scoped by the Protection Profiles. The TOE is comprised of both software and hardware. The hardware is comprised of the following:

The following table outlines the models and their key differentiators that are part of the evaluation.

Equipment			
Software/Firmware	**Hardware Model**	**Supported Software License**	**Component/Configuration**
Forescout eyeSight v9.1	4130	CT	1U Rack-mount
			1 HDD
			1 x Gen 8 Intel® Core™ i5-8500T (Coffee Lake)
			6 x Intel-based NIC Ethernet Ports
	5120-01	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			1 x Xeon Silver 4110 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
	5120-02	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			1 x Xeon Silver 4208 (Cascade Lake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
	5140-01	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			2 x Xeon Silver 4114 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
	5140-02	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			2 x Xeon Silver 4210 (Cascade Lake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
	5160-01	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			2 x Xeon Gold 6132 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
	5160-02	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			2 x Xeon Gold 6226R (Cascade Lake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
	6120	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			1 x Xeon Silver 4410Y (Saphire Rapids)
			1 Intel-based NIC Ethernet Port
	6140	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			2 x Xeon Silver 4410Y (Saphire Rapids)
			1 Intel-based NIC Ethernet Port
	6160	CT & CEM	1U Rack-mount
			3 HDD (RAID1+HS)
			2 x Xeon Gold 5418Y (Saphire Rapids)
			1 Intel-based NIC Ethernet Port

Table 2: TOE Models

The TOE resides on a network and supports the following hardware, software, and firmware in its environment:

Component	Definition

Management Workstation	Any general-purpose computer that is used by the administrator to manage the TOE. For the TOE to be managed remotely the management workstation is required to have:
	• Non-dedicated machine:
	  o 2GB memory
	  o 1GB disk space
	• OS running:
	  o Windows 7/8/8.1/10/11
	  o Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019
	  o Linux RHEL/CentOS 7.9 / 8
	  o macOS 10.12 / 10.13 / 10.14 / 10.15 / 11
	  o SSHv2 client installed to access the TOE's CLI
	• Forescout Console application (Console) installed
	
	TCP communications from the Management Workstation to the TOE is secured using:
	• SSH for remote access to the remote CLI
	• TLS for remote access from the Console
	
	The TOE's CLI can also be accessed locally with a physical connection to the TOE using the keyboard/video or the serial port and must use a terminal emulator that is compatible with serial communications (local CLI).
	
	The TOE acts as a server for both protocols. This OE component is required to support interfaces E1, E2, & E3 as defined in Figure 1 above.

Active Directory Server	A system that is capable of receiving authentication requests over TLS and validating these requests against identity and credential data that is defined in the directory (Microsoft version of an LDAP Server). The TOE is the TLS client for this communication. Required to support interface E6 as defined in Figure 1 above.
Audit Server	The TOE connects to an audit server to send the audit records for remote storage via TLS connection where the TOE is the TLS client. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes. This OE component is required to support interface E7 as defined in Figure 1 above.
Certificate Authority (CA) Server/Online Certificate Status Protocol (OCSP) Responder	Certificate authority servers issue and revoke digital certificates. The OCSP responder (a server typically run by the certificate issuer) will, when queried for revocation status of a certificate chain, returns a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'. This OE component is required to support interface E5 as defined in Figure 1 above.
Network Infrastructure	The network infrastructure contains components such as routers, switches, DNS server, etc. Figure 1 identifies these interfaces as a single interface. The interface to the managed network infrastructure is a separate connection to the enterprise operational environment the product is managing. The TOEs management of the enterprise operational environment is out of scope for the NDcPP. Therefore, interface E4 to these components is out of scope of the evaluation.

Table 3 – Operational Environment Components

5 Security Policy

5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. The TOE generates application layer audit events and OS log files. Both are stored in the TOE's local hard drive. An administrator has the ability to configure the TOE to forward events to an audit server. In the evaluated configuration, the audit data is also securely transmitted to the audit server using a TLS v1.2 communication channel.

5.2 Cryptographic Support

The TOE provides cryptography in support of SSH and TLS (v1.2) trusted communications. Two different cryptography software packages are included with the TOE: Bouncy Castle and OpenSSL. Bouncy Castle is used specifically for communications with the management workstation running the Console. OpenSSL is used for all other TLS and SSH communications. The TOE immediately destroys keys when no longer used. The following table identifies the cryptographic services per cryptographic library.

SFR	OpenSSL Implementation CAVP #A7369	Bouncy Castle Implementation CAVP #A7362
FCS_CKM.1	RSA per FIPS 186-4 Key Generation	N/A
	ECC schemes using 'NIST curves' P-256, P-384, P-521, per FIPS PUB 186-4	N/A
FCS_CKM.2	RSA Key Establishment per RSAES-PKCS-v1_5	RSA Key Establishment per RSAES-PKCS-v1_5
	Elliptic curve-based Key Establishment NIST Special Publication 800-56A Revision 3	N/A
FCS_COP.1/DataEncryption	AES CTR 128 and 256 bits AES GCM 128 and 256 bits	AES CBC: 128 and 256 bits AES GCM: 256 bits
FCS_COP.1/SigGen	RSA FIPS 186-4 Signature Services 2048 bits	RSA FIPS 186-4 Signature Services 2048 bits
FCS_COP.1/Hash	SHA-256 SHA-384 SHA-512	SHA-1 SHA-256 SHA-384 SHA-512
FCS_COP.1/KeyedHash	HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384
FCS_RBG_EXT.1	CTR DRBG (AES-256)	Hash DRBG [SHA-256, SHA-384, SHA-512]

Table 4: Cryptographic Algorithm Table for OpenSSL and Bouncy Castle

5.3 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.

The TOE provides local password authentication for CLI and Console users as well as providing the ability to securely connect to an Active Directory server for the authentication of Console

users. Communications over this interface is secured using TLS in which the TOE is acting as a client. The TOE enforces the use of X.509 certificates to support authentication for TLS connections. The only function available to an unauthenticated user is the ability to acknowledge a warning banner. Passwords that are maintained by the TSF can be composed of upper case, lower case, numbers and special characters. A Security Administrator can define the minimum password length between 6 and 100 characters.

5.4 Security Management

The TOE can be administered either locally or remotely. Role-based access control is used to prevent unauthorized management and access to TSF data.

5.5 Protection of the TSF

The TOE ensures the security and integrity of all data that is stored locally and accessed remotely. Passwords are not stored in plaintext. An administrator has the ability to query the TOE for the currently executing version the TOE software and is required to manually initiate the update process from the Console as automatic updates are not supported. The TOE automatically verifies the digital signature of the software update prior to installation. If the digital signature is found to be invalid, the administrator is provided with an error and the update is not installed. There is no means for an administrative override to continue the installation if the signature is completely missing. The TOE implements a self-testing mechanism that is automatically executed during the initial start-up and can be manually initiated by an administrator after authentication. The TOE's self-tests verify the correct operation of product and cryptographic modules. The TOE provides its own time via its internal clock.

5.6 TOE Access

The TOE displays a configurable warning banner prior to its use. Inactive sessions will be terminated after an administratively-configurable time period. Users are allowed to terminate their own interactive session. Once a remote session has been terminated, the TOE requires the user to re-authenticate to establish a new session. Local and remote sessions are terminated after the administratively-configured inactivity time limit is reached.

5.7 Trusted Path/Channels

Users can access a CLI for administration functions remotely via SSH (remote CLI) or a local physical connection (local CLI) to the TOE. The TOE operates as an SSH server for the remote CLI. The Console is the main administrator interface, which is running on a separate Windows PC and requires the use of TLS to communicate with the TOE. The TOE operates as a TLS server for requests from the Console.

The TOE acts as a TLS client to initiate the following secure paths for the following functions to their associated operational environment entities:

- User authentication (Active Directory)
- Auditing (audit server)

6 Documentation

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

- *Forescout eyeSight v9.1 Supplemental Administrative Guidance for Common Criteria*, version 1.0, September 09, 2025
- *Forescout eyeSight Installation Guide v9.1.3,* August 20, 2025
- *Forescout eyeSight Administration Guide v9.1.3,* August 20, 2025

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 Forescout that runs the Forescout eyeSight software version 9.1. Section 4 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 directly communicate with the following environment components:

- Management Workstation for local and remote administration
- Active Directory Server for remote authentication
- Audit Server for recording of syslog data
- Certificate Authority/Online Certificate Status Protocol (OCSP) Responder

To use the product in the evaluated configuration, the product must be configured as specified in the *Forescout eyeSight v9.1 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 proprietary *Evaluation Technical Report for a Target of Evaluation "Forescout eyeSight v9.1" Evaluation Technical Report (ETR)*, v1.0 dated September 10, 2025, as summarized in the publicly available *Assurance Activities Report for a Target of Evaluation "Forescout eyeSight v9.1" Assurance Activities Report (AAR)*, version 1.0 dated September 10, 2025.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *Forescout eyeSight v9.1 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 Evaluation 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 three management interfaces defined in the ST (local CLI, remote CLI, and remote GUI).

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

- Management Workstation for local and remote administration
- Syslog Server for recording of syslog data
- Active Directory Server for remote authentication
- Certificate Authority/Online Certificate Status Protocol (OCSP) Responder

Figure 2 shows the network topology of the Test configuration which identifies all of the components of the Test Environment:

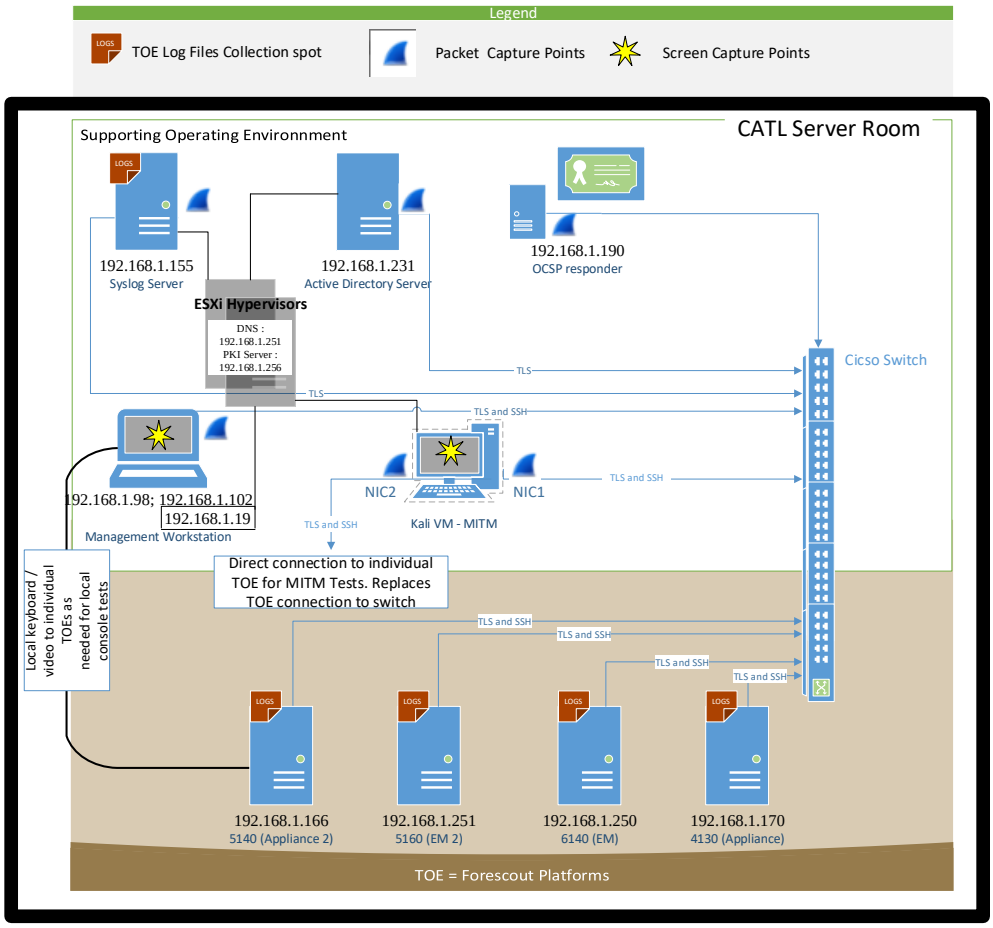

Figure 2: Testbed Network Diagram for Forescout eyeSight Testing

The following test tools were installed in the operational environment on multiple test workstations and servers for testing purposes:

- Bitvise SSH Client 9.38
- Ettercap - Man-in-the-Middle (MITM) Packet Modification Tool 0.8.2
- Forescout Console 9.1
- Metasploit 5.0.20-dev
- Nmap version 7.94
- OpenSSL 1.1.1k for OCSP, OpenSSL 1.0.1T Contains modified SSH client for sending large packets
- PuTTY version 0.73, 8.1
- rsyslogd 8.2310.0-4.el9
- stunnel 5.56
- tcpdump version 4.9.3
- Wireshark version 4.2.2, 4.9.3

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 Forescout by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface was described in the relevant design documentation (e.g., ST and AGD) in terms of the relevant claims on the TOE that can be tested through the external interface. The *Forescout eyeSight v9.1 Security Target* (ST), *Forescout eyeSight v9.1 Supplemental Administrative Guidance for Common Criteria* (AGD), and the *Forescout eyeSight v9.1 Test Procedures* (Test Plan) were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP v3.0e 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 conducted searches for public vulnerabilities related to the TOE including terms for the libraries and processors the TOE is operating with. The following NDcPP defined sources of public vulnerabilities are sources for the evaluators to perform key-word searches during the evaluation of a specific TOE.

a) NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search

b) Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php

c) US-CERT: http://www.kb.cert.org/vuls/html/search

f) Tenable Network Security http://nessus.org/plugins/index.php?view=search

g) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories

h) Offensive Security Exploit Database: https://www.exploit-db.com/

i) Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

NOTE: The additional websites: Exploit / Vulnerability Search Engine: www.exploitsearch.net and SecurITeam Exploit Search: www.securiteam.com listed in the PP are no longer available.

Section 5 of the Assurance Activity Report (AAR) includes a list of keywords, which were used individually and as part of various permutations and combinations to search for vulnerabilities identified in the public domain databases. The evaluation team then created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research.

Upon the completion of the vulnerability analysis research, the team had identified 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 but not duplicate tests already conducted as part of the prescribed assurance test activities defined in the PP.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.
- Force SSHv1
  This attack determines if the SSH server on the TOE will accept an SSHv1 connection when the TOE claims to only support SSHv2

The TOE successfully prevented any attempts of subverting its security.

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 v3.1 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 and SSH FP.

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 v3.1 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 eyeSight v9.1 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 and SSH FP 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 CEM v3.1, 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 v3.1 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 and SSH FP 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 Evaluation 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 v3.1 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 and SSH FP 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 Evaluation 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 v3.1 work unit. 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 CEM v3.1, 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 v3.1 work unit. The evaluation team ran the set of tests specified by the Evaluation Activities in the NDcPP and SSH FP 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 and SSH FP 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 v3.1 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 and SSH FP 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 and SSH FP 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 and SSH FP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments and Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Forescout eyeSight v9.1 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.

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 routers and switches network infrastructure, need to be assessed separately and no further conclusions can be drawn about their effectiveness. Section 2.3 “Excluded from the TOE” of the ST provides the details of features that are part of the purchased product but were not included in the evaluation.

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 eyeSight v9.1 Security Target*, v2.0, dated September 09, 2025

13 List of Acronyms

Acronym	Definition
AD	Active Directory
CC	Common Criteria
CEM	Centralized Enterprise Manager
CEM v3.1	Common Methodology for Information Technology Security Evaluation
CLI	Command-line Interface
CPU	Central Processing Unit
CT	CounterACT
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
RU	Rack Unit
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
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
UI	User Interface

14 Terminology

Term	Definition
Appliance	A Forescout eyeSight with the CounterACT (CT) license applied. The CT license is for basic device visibility features.
Centralized Enterprise Manager (CEM)	A Forescout eyeSight with the CEM license applied. The CEM license unlocks centralized management functionality for managing multiple eyeSight Appliances.
Console or Console application	The Forescout Console is a separate GUI application, installed on an administrative workstation, used for creating NAC, firewall and IPS policies, generating reports, viewing and managing detection information, and managing Forescout eyeSight.
Endpoint	A Network Host discovered by the Forescout eyeSight, for example desktop, laptop, server, etc.
Local CLI	When the TOE's command line interface (CLI) is accessed locally with a physical connection to the TOE via the keyboard/video ports or a serial port and a terminal emulator that is compatible with serial communications is referred to as the local CLI. Note: The NDcPP utilizes the term Local Console in its terminology and this is the same as the Local CLI.
Plugins	Functionality enhancement modules that can be incorporated into the Forescout eyeSight. Plugins enable deeper inspection as well as broader control over network endpoints. Bundled plugins are pre-packaged with the Forescout eyeSight. Other plugins may be available from Forescout or from a third party. Only the syslog and Active Directory plugins are included in the scope of the evaluation as they provide functional support for the NDcPP defined SFRs.

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-2017-04-001.
2. *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components*, dated April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.
3. *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components*, dated April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.
4. *Common Methodology for Information Technology Security Evaluation – Evaluation Methodology*, dated April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.
5. *collaborative Protection Profile for Network Devices,* Version 3.0e, December 6, 2023
6. *Functional Package for Secure Shell (SSH),* Version 1.0, May 13, 2021
7. *Forescout eyeSight v9.1 Security Target*, Version 2.0, September 09, 2025
8. *Forescout eyeSight v9.1 Supplemental Administrative Guidance for Common Criteria*, version 1.0, September 09, 2025
9. *Forescout eyeSight Installation Guide v9.1.3,* August 20, 2025
10. *Forescout eyeSight Administration Guide v9.1.3,* August 20, 2025
11. *Assurance Activities Report for a Target of Evaluation Forescout eyeSight v9.1 Assurance Activities Report (AAR),* Version 1.0, September 10, 2025
12. Evaluation Technical Report for a Target of Evaluation Forescout eyeSight v9.1 Evaluation Technical Report (ETR), Version 1.0, September 10, 2025