National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Berryville Holdings, LLC Warden v1.2

Report Number:	**CCEVS-VR-VID11522-2025**
Dated:	**July 7, 2025**
Version:	**0.5**

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

Swapna Katikaneni

Daniel Faigin

Marybeth Panock

The Aerospace Corporation

Russ Fink

Farid Ahmed

Robert Wojcik

John Hopkins University Applied Physics Laboratory (JHUAPL)

Common Criteria Testing Laboratory
Dip Pudasaini
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Description 3
3.2 TOE Evaluated Platforms 4
3.3 TOE Architecture 4
3.4 Physical Boundaries 5
4 Security Policy 6
4.1 Security audit 6
4.2 Cryptographic support 6
4.3 User data protection 6
4.4 Firewall 6
4.5 Identification and authentication 7
4.6 Security management 7
4.7 Packet filtering 7
4.8 Protection of the TSF 8
4.9 TOE access 8
4.10 Trusted path/channels 8
4.11 Intrusion prevention 8
5 Assumptions & Clarification of Scope 9
5.1 Assumptions 9
5.2 Clarification of scope 9
6 Documentation 10
7 IT Product Testing 10
7.1 Developer Testing 10
7.2 Evaluation Team Independent Testing 10
8 Evaluated Configuration 10
9 Results of the Evaluation 11
9.1 Evaluation of the Security Target (ASE) 11
9.2 Evaluation of the Development (ADV) 11
9.3 Evaluation of the Guidance Documents (AGD) 11
9.4 Evaluation of the Life Cycle Support Activities (ALC) 12
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 12
9.6 Vulnerability Assessment Activity (VAN) 12
9.7 Summary of Evaluation Results 12
10 Validator Comments/Recommendations 13
11 Annexes 13
12 Security Target 13
13 Glossary 13
14 Bibliography 14

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) validation team's assessment of the evaluation of the **Warden** version 1.2 product and Target of Evaluation (TOE), provided by **Berryville Holdings, LLC**. It presents the evaluation results, their justifications, and the conformance results. The VR is intended to assist the end user of the evaluated product and any security certification Agent for that end user in determining the suitability of this product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. This VR is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in June 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the *PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways*, Version 1.2, 18 August 2023 (CFG_NDcPP-IPS-FW-VPNGW_v1.2) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Intrusion Prevention Systems (IPS),* Version 1.0, 11 May 2021 (IPS10), the *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e), and the *PP-Module for VPN Gateways*, Version 1.3, 16 August 2023 (VPNGW13).

The Berryville Warden 1.2 TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL 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). This VR 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. 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). 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 *Berryville Holdings, LLC Warden v1.2 Security Target*, version 0.6, July 3, 2025, *Assurance Activity Report for Berryville Holdings, LLC Warden v1.2* (AAR), *Berryville Holdings LLC, Warden v1.2 CC Administrator Guide* (AGD), *Evaluation Technical Report for Berryville Warden 1.2* (ETR) and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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) against Protection Profiles (PPs) containing Assurance Activities using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 (PCL).

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	Berryville Warden 1.2 (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways*, Version 1.2, 18 August 2023 (CFG_NDcPP-IPS-FW-VPNGW_v1.2) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Intrusion Prevention Systems (IPS)*, 1.0, 11 May 2021 (IPS10), the *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e), and the *PP-Module for VPN Gateways*, Version 1.3, 16 August 2023 (VPNGW13)
ST	*Berryville Holdings, LLC Warden v1.2 Security Target*, version 0.6, July 3, 2025
Evaluation Technical Report	*Evaluation Technical Report for Berryville Warden 1.2*, version 0.4, July 3, 2025
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Berryville Holdings, LLC
Developer	Berryville Holdings, LLC

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Swapna Katikaneni, Daniel Faigin, Marybeth Panock, Russ Fink, Farid Ahmed, and Robert Wojcik

3 Architectural Information

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

The Target of Evaluation (TOE) is the Berryville Warden v1.2. The TOE is a virtual networking device that provides secure remote administration (through SSH), VPN gateway functionality (using IKE/IPSec), stateful firewalling, and an Intrusion Prevention System (IPS).

3.1 TOE Description

The TOE consists of a single instance of virtual Berryville device running the Warden software v1.2 on a physical device running Ubuntu 22.04's KVM hypervisor. It is assumed to be installed and operated within a physically protected environment, administered by trusted and trained administrators. The TOE can be remotely administered via SSH or via a local console.

The TOE is a virtual networking device that provides a centralized management command line interface for secure remote administration through SSH, encrypting all data exchanged between the client and the server, and protecting sensitive information like login credentials, command sequences, and system data from interception or man-in-the-middle attacks. The Warden employs RSA and ECDSA as cryptographic algorithms to secure data in transit, which are utilized for SSH protocol and Rsyslog service. Integration with IPS prevents unauthorized access or brute-force attacks. Restricted access can be further expanded upon with firewall rules to permit access to a specific IP address or a CIDR block.

Suricata, an open-source threat detection engine, inspects and controls network traffic, examining both inbound and outbound data for potential security risks and breaches. Every data packet within the monitored network is scanned, decoded, and preprocessed, then assessed against defined access control and intrusion prevention criteria to identify and address unauthorized or harmful traffic, such as attempted attacks. If suspicious activity is detected, whether due to unexpected network behavior or a known threat signature, the system alerts a designated administrator and may also block the malicious traffic.

Additionally, command restrictions are limited to the capabilities of the Warden Shell (WSH). Session timeout and idle disconnect have been integrated to help protect against unauthorized access if an active session is left unattended. The Warden provides a valuable audit trail, detailing session logging and logging of all access attempts, including successful and failed logins, and any executed commands.

Stateful firewalling, an advanced networking security technique, allows the Warden to track and evaluate the state of active connections to make informed decisions about whether to permit or deny data packets. Any and all packets that are not accepted by the firewall are logged and reported. User-specific custom firewall rules can be configured through the WSH.

The TOE provides VPN gateway capabilities, allowing the Engine to use IKE/IPsec to protect traffic exchanged with remote peer gateways (for a site-to-site VPN configuration) and with VPN clients. Site-to-site configuration can be used to protect data between the TOE and a remote syslog server or NTP server.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

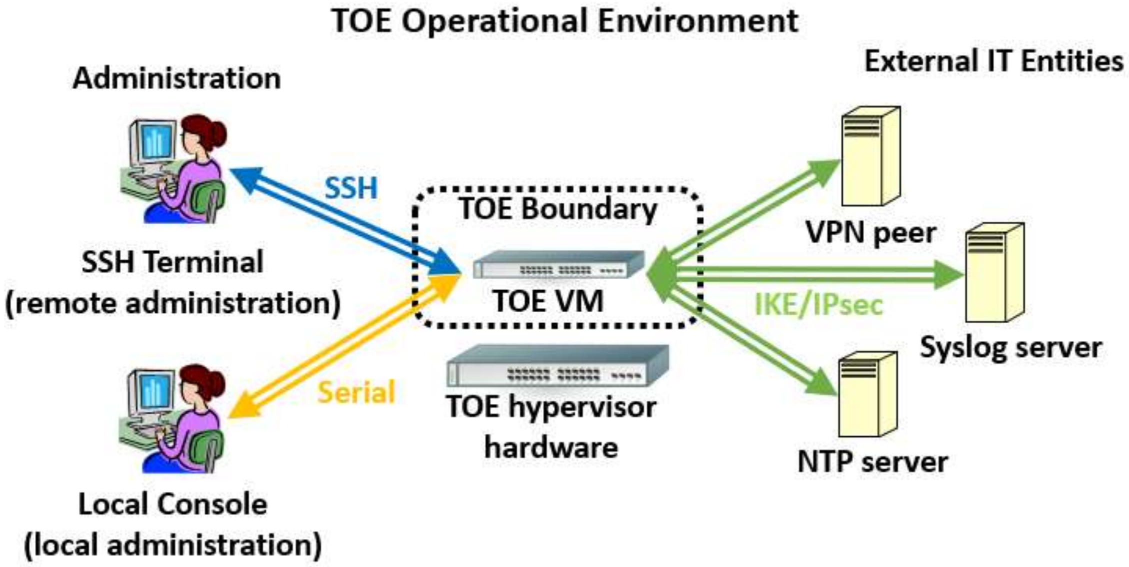
The TOE is a single virtual network device running the Berryville Warden v1.2 software that operates independently (i.e., it is not a distributed TOE) and communicates with entities in its operational environment including remote administrators (who securely connect to the TOE's administrative CLI through SSH), NTP servers (tunneled within IPsec for security), syslog/audit servers, and with IPsec peers (gateways).

The physical characteristics of the TOE platform are the following:

- Ubuntu 22.04 (Linux 5.15) KVM Hypervisor running on 11th Gen Intel(R) Core (TM) i7-1165G7 (Tiger Lake)

The TOE is deployed in an environment that includes the IT components illustrated in the following figure. The TOE itself is delivered as a virtual image to be installed on the KVM hypervisor. The administrator of the TOE may verify the TOE software and, if necessary, download and install the correct version.

The physical boundary of the TOE is illustrated below. Non-TOE components are summarized in the **IT Environment Components** table that follows. The TOE implements IPsec as a VPN Gateway and SSH Server for secure connectivity to the components of the environment.



TOE and TOE Operational Environment

The environmental components described in the following table are required to operate the TOE in the evaluated configuration.

Component	Description
VPN Peer	A peer server that supports IPsec to communicate with the TOE so the TOE can provide VPN Gateway functionality,
Audit (syslog) server	The audit server supports syslog messages over IPsec via a site-to-site connection to receive the audit logs from the TOE. The audit data is stored in the remote audit server for redundancy purposes.
NTP Server	The NTP server supports NTP messages over IPsec via a site-to-site connection. The TOE syncs its clock with the NTP server in order to provide proper timestamps.
SSH Terminal	A remote SSH client, allows an administrator to manage the TOE remotely on a secure management network.
Local Console	A local serial connection allows an administrator to manage the TOE locally in a secure physical environment.

IT Environment Components

3.4 Physical Boundaries

The physical boundary of the TOE is the firmware as well as the hardware the firmware is installed on. The TOE is a single instance of virtual Berryville device running the Warden software v1.2 on a physical device running Ubuntu 22.04’s KVM hypervisor. The physical hardware has an 11th Gen Intel(R) Core (TM) i7-1165G7 (Tiger Lake) CPU. All Ubuntu 22.04 functionality beyond the virtual device running on the KVM hypervisor is outside the scope of the evaluation. Ubuntu 22.04 should be configured that only the relevant services to the virtual device are open.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Firewall
4. User data protection
5. Identification and authentication
6. Security management
7. Packet filtering
8. Protection of the TSF
9. TOE access
10. Trusted path/channels
11. Intrusion Prevention

4.1 Security audit

The TOE provides auditing capabilities to provide a secure and reliable record of all security relevant events, including administrative changes to the TOE. Any security relevant event is audited internally and then transmitted externally over a secure communication channel to an audit server via IPsec in real-time. All audited events have the necessary details like timestamp, event log, event code, and identity of the party involved to provide a comprehensive audit trail. Depending on the context of the audit, the identity may be the relevant user id, or remote IT entity involved in the event. All audits are protected from unauthorized deletion. The TOE’s logd will rotate logs and once out of space, delete the oldest logs in order to make room for newer logs.

4.2 Cryptographic support

The TOE leverages OpenSSL library (version 3.0.10) executing on the TOE’s Intel Core i7-1165G7 Processor library to provide cryptographic functions supporting secure administration access (via SSH), secure network traffic with VPN peers (via IKE/IPsec), and for secure communication to external systems such as audit log servers and NTP servers (also via IPsec). Functions include Key generation, key establishment, key distribution, key destruction, and cryptographic operations.

4.3 User data protection

The TOE prevents leakage of residual information into subsequent packets by clearing packet buffers upon allocation.

4.4 Firewall

The VM bridges the physical hardware’s ethernet interface or additional USB interfaces to create virtual interfaces. Using these virtual interfaces, the TOE supports many protocols for packet filtering including icmpv4, icmpv6, ipv4, ipv6, tcp and udp. The firewall rules implement the SPD rules (permit, deny, bypass). Each rule can be configured to log status of packets pertaining to the rule. All codes under each protocol are implemented. The TOE supports FTP for stateful filtering.

Routed packets are forwarded to a TOE interface with the interface's MAC address as the layer-2 destination address. The TOE routes the packets using the presumed destination address in the IP header, in accordance with route tables maintained by the TOE.

IP packets are processed by the software, which associates them with application-level connections, using the IP packet header fields: source and destination IP address and port, as well as IP protocol. Fragmented packets are reassembled before they are processed.

The TOE mediates the information flows according to an administrator-defined policy. Some of the traffic may be either silently dropped or rejected (with notification to the presumed source).

The TOE's firewall and packet filtering capabilities are controlled by defining an ordered set of iptables rules. The rule specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, and whether to log the connection.

4.5 Identification and authentication

The TOE maintains a single security administrator role. While the TOE allows unique users, each created user has the security administrator role. The TOE provides secure password-based authentication for local administrators and password or public key based authentication for remote SSH administrators. The only functionality available to an administrator prior to authentication is viewing the warning banner. The TOE, supports passwords of varying lengths and allows an administrator to specify a minimum password length between 15 and 32 characters long. The password composition can contain all special characters as required by FIA_PMG_EXT.1.1.

Consecutive unsuccessful authentication attempts beyond a configurable limit will result in locking of the user account for a specified duration of time.

The TOE provides secure connectivity between itself and a remote VPN peer, syslog server, or NTP server using IPsec with X.509 certificate-based authentication.

4.6 Security management

The TOE maintains a single security administrator role that allows both local and remote administration for management of the TOE's security functions. TOE administrators manage the security functions of the TOE through a local console or SSH CLI. The security administrator is able to perform all management functions, including, but not limited to, modifying audit behavior, performing updates, managing crypto keys, managing firewall, IPS, and packet filtering rules.

4.7 Packet filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established with trusted VPN peers. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets. The TOE supports many protocols for packet filtering including ICMPv4, ICMPv6, IPv4, IPv6, TCP and UDP.

4.8 Protection of the TSF

The TOE includes capabilities to protect itself from unwanted modification as well as protecting its persistent data.

The TOE does not store passwords in plaintext; they are obfuscated. The TOE does not support any command line capability to view any cryptographic keys generated or used by the TOE.

The TOE provides image integrity verification using a digital signature to validate the authenticity of the images before loading them. Upon every boot up, power on self-tests is conducted to validate the integrity of the software components as well as perform cryptographic known answer tests for the supported cryptographic algorithms. If power-up self-tests fail, the TOE halts the boot process. The TOE also allows administrator to manually configure the TOE’s clock or to configure an NTP server, with which the TOE will synchronize its time. The TOE provides a timestamp for use with audit records, timing elements of cryptographic functions, and inactivity timeouts.

4.9 TOE access

On user logins, the TOE presents a login banner; the administrator has the ability to customize the warning/access policy message as per the organization needs. The TOE also provides the ability to configure an inactivity timeout, which terminates the session after a specified period of inactivity. An administrator can also terminate their own session.

4.10 Trusted path/channels

The TOE communicates to external components in a secure manner using IPsec for VPN peers, syslog servers, or NTP servers. The TOE also employs SSH to secure remote administrative sessions.

4.11 Intrusion prevention

The TOE supports in-line inspection modes using both anomaly and signature-based detection along with IP filtering based on blacklists. Anomaly-based detection can be determined by throughput (packets per second), time of day, frequency, and/or thresholds. Signature-based detection can be determined by packet headers, string-based pattern-matching, attacks. and/or patterns.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
- PP-Module for Intrusion Prevention Systems (IPS), 1.0, 11 May 2021 (IPS10)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)
- PP-Module for VPN Gateways, Version 1.3, 25 August 2023 (VPNGW13)

That information has not been reproduced here and the NDcPP22e/IPS10/STFFW14e/VPNGW13 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/IPS10/STFFW14e/VPNGW13 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

5.2 Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need 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 assurance activities specified in the collaborative Protection Profile for Network Devices and the Intrusion Prevention, Firewalls, and VPN Gateways Modules and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Firewall, VPN Gateway, Router, Intrusion Prevention Systems models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives 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 NDcPP22e/IPS10/STFFW14e/VPNGW13 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not

covered by this evaluation. This may have left unevaluated some of the capabilities mentioned in the TOE Description in section 3. In particular, the full set of tests necessary to evaluate the comprehensive firewall rules for restricted access or preventing unauthorized access has not been demonstrated through this evaluation. This also includes comprehensive testing of alert generation and subsequent blocking of malicious traffic due to suspicious activities, whether due to unexpected network behavior or a known threat signature. The evaluation addressed the parts of the Suricata engine needed to meet the requirements including IPv4 and IPv6 events. The evaluation did not assess any predefined rules associated with the engine.

6 Documentation

The following documents were available with the TOE for evaluation:

- Berryville Holdings LLC, Warden v1.2 CC Administrator Guide, July 3, 2025

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 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 Detailed Test Report for Berryville Warden, Version 0.3, July 1, 2025 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/IPS10/STFFW14e/VPNGW13 including the tests associated with optional requirements. Testing took place from April 2024 through May 2025 within the Gossamer Security Solutions laboratory in Columbia, MD following the procedures in the Gossamer Quality Manual with no deviations. The developer was available to assist during the testing phase. The AAR, in section 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE consists of a single instance of virtual Berryville device running the Warden software v1.2 on a physical device running Ubuntu 22.04’s KVM hypervisor.

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 assurance 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 Warden TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/IPS10/STFFW14e/VPNGW13.

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 Berryville Warden 1.2 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e/IPS10/STFFW14e/VPNGW13 related to the examination of the information contained in the TSS.

The validator 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.

9.3 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

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

The validator 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 NDcPP22e/IPS10/STFFW14e/VPNGW13 and recorded the results in a Test Report, summarized in the AAR.

The validator 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.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “Berryville”, “Warden”, “Dexter Edwards”, “Intel i7-1165G7”, “i7-1165G7”, “Linux Kernel 5.15”, “Linux Kernel 6.5”, “rsyslog 8.2112.0-2ubuntu2.2”, “Linux strongSwan U5.9.5/K5.15.0-87-generic”, “OpenSSL 3.0.10”, “OpenSSH 8.9p1”, “chronyc 4.2”, and “QEMU 6.2.0”. The latest search was done on June 25, 2025.

The validator 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.

9.7 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 testing 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 followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guidance documents listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. 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. All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Berryville Holdings, LLC Warden v1.2 Security Target,* Version 0.6, July 3, 2025.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] *PP-Module for Intrusion Prevention Systems (IPS)*, 1.0, 11 May 2021 (IPS10).

[6] *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e).

[7] *PP-Module for VPN Gateways*, Version 1.3, 25 August 2023 (VPNGW13).

[8] *Berryville Holdings, LLC Warden v1.2 Security Target*, Version 0.6, July 3, 2025 (ST).

[9] *Assurance Activity Report for Berryville Warden 1.2*, Version 0.3, July 1, 2025 (AAR).

[10] *Detailed Test Report for Berryville Warden 1.2*, Version 0.3, July 1, 2025 (DTR).

[11] *Evaluation Technical Report for Berryville Warden*, Version 0.4, July 3, 2025 (ETR).