National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

VMware Workspace ONE Boxer Email Client 5.4

Report Number: CCEVS-VR-VID10840
Version 1.0
June 27, 2019

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Sheldon Durrant, Senior Validator
Linda Morrison, Lead Validator
Clare Olin
Chris Thorpe

MITRE Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Alex Massi
Christopher Rakaczky

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 VMware Workspace ONE Boxer Email Client 5.4 provided by VMware. 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 February 2019. 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 *Protection Profile for Application Software Version 1.2* (APP_PP), dated 22 April 2016 and *Extended Package for Email Clients v2.0* (EC_EP), dated June 18, 2015.

The Target of Evaluation (TOE) is the VMware Workspace ONE Boxer Email Client 5.4 software application, installed on a mobile device platform running iOS 11 (VID10851) as well as a mobile device host running Android 8.0 (VID10898), in the evaluated configuration. The Boxer application containerizes enterprise data from personal data that resides on the user's mobile device. Boxer supports the use of Exchange, Office 365, Outlook, Gmail, Yahoo and Cloud email services. Enterprise management support only applies to the use of Exchange. The evaluated TOE functionality includes only the security functional behavior that is defined in the claimed APP_PP and EC_EP.

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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the APP_PP and EC_EP. 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 APP_PP and EC_EP 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 *VMware Workspace ONE Boxer Email Client 5.4 Security Target v1.0*, dated June 13, 2019 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). 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	VMware Workspace ONE Boxer Email Client version 5.4
Protection Profile	Protection Profile for Application Software Version 1.2 dated April 22, 2016 and Extended Package for Email Clients v2.0 dated June 18, 2015, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	VMware Workspace ONE Boxer Email Client 5.4 Security Target v1.0, dated June 13, 2019
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "VMware Workspace ONE Boxer Email Client 5.4" Evaluation Technical Report v1.0 dated June 13, 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	VMware
Developer	VMware
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	MITRE Validators: Jenn Dotson Sheldon Durant Linda Morrison Clare Olin Chris Thorpe

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.

- The TOE relies upon a trustworthy computing platform for its Execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.FLAWED_ADDON** – Email client functionality can be extended with integration of third-party utilities and tools. This expanded set of capabilities is made possible via the use of add-ons. The tight integration between the basic email client code and the new capabilities that add-ons provide increases the risk that malefactors could inject serious flaws into the email client application, either maliciously by an attacker, or accidentally by a developer. These flaws enable undesirable behaviors including, but not limited to, allowing unauthorized access to sensitive information in the email client, unauthorized access to the device's file system, or even privilege escalation that enables unauthorized access to other applications or the operating system.
- **T.LOCAL_ATTACK –** An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
- **T.NETWORK_ATTACK** – An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
- **T.NETWORK_EAVESDROP –** An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
- **T.PHYSICAL_ACCESS –** An attacker may try to access sensitive data at rest.

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 *Protection Profile for Application Software Version 1.2 and Extended Package for Email Clients v2.0*, including all relevant NIAP Technical Decisions. A subset of the “optional” and “selection-based” security requirements defined in the APP_PP and EC_EP 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 Boxer Email Client support using Office 365, Outlook, Gmail, Yahoo, and Cloud email services 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.

In the evaluated configuration, the TOE is installed on a mobile device running iOS 11 (VID10851) as well as a mobile device host running Android 8.0 (VID10898). The mobile device that the TOE is installed on is managed by a Mobile Device Management software product called VMware Workspace ONE Unified Endpoint Management (UEM). UEM consists of a server and an agent that resides on the mobile device. The UEM agent is used to enroll the mobile device with the UEM server so that it can be managed by the UEM server. Also, the UEM agent consumes policy and configuration information for the device and VMware applications, such as Boxer, operating on the device, as well as providing status and policy information about the mobile device to the UEM server. The operating system, UEM agent, and UEM server are considered part of the operational environment.

Boxer uses ActiveSync to communicate with the Exchange server and is protected using TLS v1.2. The Exchange server resides in the operational environment and is for sending and receiving enterprise data such as email, calendar information and appointment data. Whether installed on an Android or iOS device, the application validates the certificates using OCSP. The OCSP responder is also considered part of the operational environment.

The TOE includes administrative guidance in order to instruct Security 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 email client software application that is installed on mobile devices as defined in the APP_PP and EC_EP which state: “Applications include a diverse range of software such as office suites, thin clients, PDF readers, and downloadable smartphone apps … Email clients are user applications that provide functionality to send, receive, access and manage email.” The TOE is an email client that allows the user to receive, send, manage, and access enterprise email on a mobile device. Thus, the TOE is an email client software application.

4.2 Physical Boundary

The TOE is an application software product. All hardware that is present is part of the TOE’s Operational Environment. In the evaluated configuration, the TOE is installed on a VID10851 certified iOS 11 device and VID10898 certified Android 8.0 device. For testing, this evaluation used a Samsung Galaxy S8+ (Android) and on an iPhone 8 (Apple).

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
OCSP Responder	A server deployed within the Operational Environment which confirms the validity and revocation status of certificates.
VMware Workspace ONE UEM v9.4.0.0	The mobile device has the VMware Workspace ONE Intelligent Hub (UEM agent) installed and is managed by the VMware Workspace ONE UEM server (UEM server).
Windows Server 2012 R2 Exchange server	Exchange server for sending and receiving emails to and from the Operational Environment.
Mobile Device	The hardware that runs the OS in which the application is installed on.

Table 2 – IT Environment Components

5 Security Policy

5.1.1 Cryptographic Support

Depending on which OS the application is installed on, the TOE either invokes the underlying platform or implements its own cryptographic module to perform cryptographic services. All cryptographic mechanisms, whether platform or application provided, use DRBG functionality to support cryptographic operations. Cryptographic functionality includes encryption/decryption services, credential/key storage, key establishment, key destruction, hashing services, signature services, key-hashed message authentication, and key chaining using a password-based derivation function.

Cryptographic services for the application's S/MIME functionality and TLS communications are provided by the underlying platform when the application is installed on a device running the iOS. When installed on a device running the Android OS, the TOE invokes the underlying platform cryptographic libraries for TLS communications and implements an OpenSSL cryptographic module to perform the cryptographic functionality required to support S/MIME (consolidated Certificate number C631).

OpenSSL Algorithm for S/MIME	SFR	Consolidated CAVP Cert. #
HMAC-SHA-256, 256 bit key	FCS_CKM_EXT.5.3	C631
AES-128-CBC and AES-256-CBC	FCS_SMIME_EXT.1.2	C631
SHA-256, SHA-384, SHA-512	FCS_SMIME_EXT.1.3	C631
RSA (2048, SHA2-256)	FCS_SMIME_EXT.1.4	C631
DRBG CTR (AES-256)	FCS_RBG_EXT.1.1	C631
AES-256-CBC	FCS_COP.1(1) - Encryption of Boxer specific database used in support of FCS_STO_EXT.1(1) storage of specific keys.	C631

Table 3 – Cryptographic Algorithm Table (OpenSSL)

5.1.2 User Data Protection

The TOE uses S/MIME to digitally sign, verify, decrypt, and encrypt email messages. The TOE stores all application data in an encrypted Boxer database which is created on the mobile device during installation. The TOE requires that the host platform have full disk encryption enabled to securely store the data. The TOE restricts its network access and provides user awareness when it attempts to access hardware resources and sensitive data stored on the host platform. The TOE displays notification icons that show S/MIME status. Each status is shown as a different color so that the user can quickly identify any issues.

5.1.3 Identification and Authentication

The TOE validates X.509v3 certificates for TLS communication to the Exchange server. X.509v3 certificates are also used for signing and encrypting emails for S/MIME. The TOE application, regardless of platform, performs the certificate validation using OCSP.

5.1.4 Security Management

The TOE enforces the application's enterprise policy set by the UEM administrator pushed out to the managed devices. The TOE does not use default passwords, and automatically installs and configures the application to protect itself and its data from unauthorized access while also implementing the recommended platform security mechanisms. Changing one's own password from the application is the only management function that can be performed by the owner/user of the mobile device with the TOE installed.

5.1.5 Privacy

The TOE does not transmit any personally identifiable information (PII) over the network unless voluntarily sent via free text email.

5.1.6 Protection of the TSF

The TOE does not support the installation of trusted or untrusted add-ons. The user is able to navigate the platform to check the version of the TOE and also check for updates to the application. All updates come from the Google Play Store (Android) or Apple Store (iOS). The digital signature of the updates is verified by the mobile device platform prior to being installed. The TOE does not replace or modify its own binaries without user interaction. The TOE implements anti-exploitation features, such as stack-based overflow protection, is compatible with security features provided by the OS, and will only use documented APIs and libraries.

5.1.7 Trusted Path/Channels

The TOE invokes the platform to provide the trusted communication channel between the TOE and the Exchange server. Communications is protected with TLS v1.2. Communication to the Exchange server uses ActiveSync to send and receive emails. The TOE, in conjunction with the platform, supports mutual authentication using X.509v3 certificates for TLS communications.

6 Documentation

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

- VMware Workspace ONE Boxer Email Client 5.4 Supplemental Administrative Guidance for Common Criteria – v1.0

Any additional customer documentation provided with the product, or 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 VMware Workspace ONE Boxer Email Client 5.4 software application, installed on a mobile device running iOS 11 (VID10851) as well as a mobile device host running Android 8.0 (VID10898). Section 4.2 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:

- OCSP Responder for certificate revocation checking
- VMware Workspace ONE UEM v9.4.0.0 for unified endpoint management (UEM)
- Windows Server 2012 R2 Exchange server for email
- Mobile Device for running the TOE software application

To use the product in the evaluated configuration, the product must be configured as specified in the *VMware Workspace ONE Boxer Email Client 5.4 Supplemental Administrative Guidance for Common Criteria Version 1.0* document, dated March 20, 2019.

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 "VMware Workspace ONE Boxer Email Client 5.4" Assurance Activities Report v1.0 dated June 13, 2019*.

8.1 Test Configuration

The evaluation team conducted testing at the VMware Headquarters in Atlanta, GA on an isolated network. The evaluation team configured the TOE for testing according to the *VMware Workspace ONE Boxer Email Client 5.4 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 TOE was configured with specific IP addresses when outside the firewall and assigned another set of IP numbers when connected to the test enterprise network (inside firewall).

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

- OCSP Responder server (Windows Server 2012 R2 (Build 9600)).
  - Microsoft Online Certificate Status Protocol Responder
  - OpenSSL 1.0.2k-fips[1]
- VMware Workspace ONE UEM v9.4.0.0 server was (Windows Server 2012 R2 (Build 9600)).
- Exchange server Windows Server 2012 R2 ((Build 9600)).
  - Exchange Server 2013 CU20; Release: March 20, 2018; Build: 15.0.1367.3
- Mobile Device for running the TOE software application

The following test tools were installed on multiple test workstations and servers for testing purposes:

- Binary Analysis Tool
- ClamAV version 0.101.1
- DB Browser for SQLite version 3.10.1
- iOS Network Analysis Tool
- Memory Dump Tool
- Man-in-the-Middle (MITM) Packet Modification Tool
- postfix version 3.3.0
- PuTTY version 0.70
- Python version 3.6.4
- Python version 3.7.1
- Wireshark version 2.6.5

The following test tools were installed on the mobile device for testing purposes:

- iOS Keychain Dump Tool
- Memory Dump Tool
- Packet Capture Tool

[1] Used for negative and control testing required as part of Test Cases 52, 53, and 54 as documented in the Test Plan.

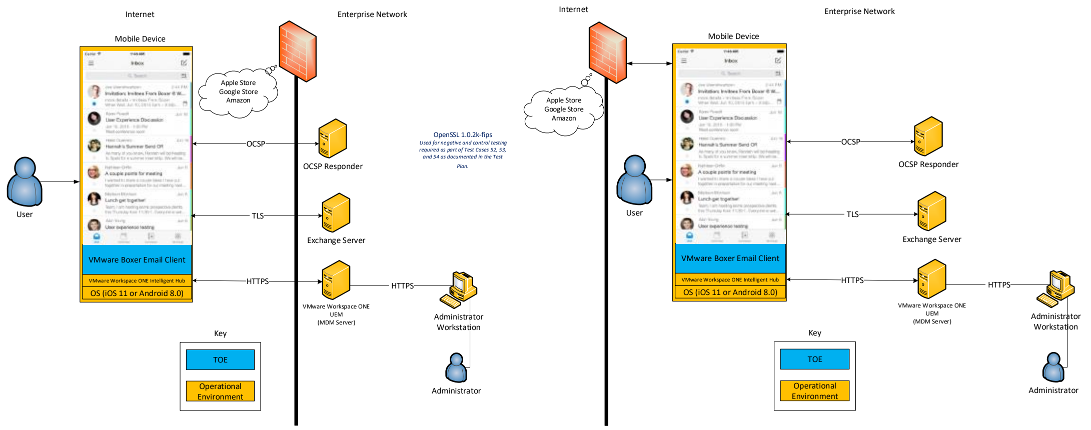

Figure 1 - Test Configuration

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 APP_PP and EC_EP 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 the APP_PP and EC_EP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
VMware	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Boxer	This is a generic term for searching for known vulnerabilities for the specific product.

Keyword	Description
Workspace ONE UEM (version 9.4.0.0)	This is a generic term for searching for known vulnerabilities for the MDM used to remotely manage the TOE application.
OpenSSL Android: (version 1.0.2p)	This is a generic term for searching for known vulnerabilities for the cryptographic library used by the TOE application.
WebView	This is a generic term for searching for known vulnerabilities for the email document (HTML) viewer used by the TOE application (Android).
Polaris Office (version 4.0.7.4)	This is a generic term for searching for known vulnerabilities for the email attachment viewer used by the TOE application (Android).
WKWebView	This is a generic term for searching for known vulnerabilities for the email document (HTML) and attachment viewer used by the TOE application (iOS).

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (updated June 11, 2019). The following public vulnerability sources were searched:

- Common Vulnerabilities and Exposures:
  http://cve.mitre.org/cve/
  https://www.cvedetails.com/vulnerability-search.php
- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below):
  https://web.nvd.nist.gov/view/vuln/search
- Security Focus:
  http://www.securityfocus.com/vulnerabilities/
- Vendor Vulnerability Sources:
  https://www.vmware.com/security/advisories.html
  https://source.android.com/security/bulletin
  https://support.apple.com/en-us/HT201222
  https://www.openssl.org/news/vulnerabilities.html
- CXSecurity:
  http://www.cxsecurity.com/

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. Testing that was conducted under the functional testing that would have been duplication of a vulnerability tests were not re-run. This left one remaining exploit to further explore: malicious binary.

The team tested the following areas:

- Virus Scan
  This test scans the TOE binary with a virus scanner using the most current virus definitions against the application files and then the evaluator verifies that no files are flagged as malicious.

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 4 and CEM version 3.1 rev 4. 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 APP_PP and EC_EP.

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 VMware Workspace ONE Boxer Email Client 5.4 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 APP_PP and EC_EP 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 APP_PP and EC_EP 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 APP_PP and EC_EP 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 unit and the extended assurance requirement ALC_TSU_EXT.1 defined in the App PP. The evaluation team found that the TOE was identified and a method of timely updates was described.

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 APP_PP and EC_EP 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 validated that the vendor fixed all findings with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the App PP were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

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 APP_PP and EC_EP, 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 *VMware Workspace ONE Boxer Email Client 5.4 Supplemental Administrative Guidance for Common Criteria Version 1.0, dated March 20, 2019* document. 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 functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *VMware Workspace ONE Boxer Email Client 5.4 Security Target v1.0,* dated June 13, 2019.

13 List of Acronyms

Acronym	Definition
CA	Certificate Authority
CC	Common Criteria
CPU	Central Processing Unit
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure over a bidirectional TLS encrypted tunnel
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAS	Mobile Application Store
MDM	Mobile Device Management
NIAP	National Information Assurance Partnership
OCSP	Online Certificate Status Protocol
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UEM	Unified Endpoint Management

14 Terminology

Term	Definition
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data.
Security Administrator	Synonymous with Authorized Administrator.
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.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Protection Profile for Application Software Version 1.2, dated April 22, 2016
6. Extended Package for Email Clients v2.0, dated June 18, 2015
7. VMware Workspace ONE Boxer Email Client 5.4 Security Target v1.0, dated June 13, 2019
8. VMware Workspace ONE Boxer Email Client 5.4 Supplemental Administrative Guidance for Common Criteria Version 1.0, dated March 20, 2019
9. Assurance Activity Report for a Target of Evaluation “VMware Workspace ONE Boxer Email Client 5.4” Assurance Activities Report v1.0 dated June 13, 2019