Security Target

VMware Horizon 6

Document Version: 0.8
Date: August 11, 2016

Prepared For:

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

***Prepared By*:**

CGI Global IT Security Labs.

1410 Blair Place, 7th floor
Ottawa, ON K1J 9B9, Canada
www.cgi.com/securitylab

Revision History

Ver #	Description of changes	Modified by	Date
0.1	Initial Draft	Danielle Freebourne	05/8/2015
0.2	ORs updates and corrections from the lab with input from VMware	Danielle Freebourne	08/11/2015
0.3	ORs #2 updates from lab	Danielle Freebourne	08/18/2015
0.4	ORs #3 updates	Danielle Freebourne	09/22/2015
0.5	ORs #4 updates	Danielle Freebourne	12/5/2015
0.6	Minor updates	Danielle Freebourne	3/11/2016
0.7	Updates from lab and VMware	Danielle Freebourne	4/7/2016
0.8	ORs updates	Danielle Freebourne	8/11/2016

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

This section identifies the Security Target (ST), Target of Evaluation (TOE), document conventions, and terminology. It also provides TOE overview and describes the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE.

1.1 ST Reference

ST Title	Security Target VMware Horizon 6
ST Revision	0.8
ST Publication Date	August 11, 2016
ST Author	CGI Global IT Security Labs – Canada Danielle Freebourne

1.2 Target of Evaluation Reference

TOE Developer	VMware, Inc.
TOE Name	VMware Horizon 6
TOE Version	VMware Horizon 6 Version 6.2.2 and Horizon Client for Windows 3.5.2
TOE Type	Desktop and Application Virtualization

1.3 Conventions

The Common Criteria allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and selected presentation choices are discussed below to aid the Security Target reader:

An assignment operation is indicated by [**bold text within brackets**].

Selections are denoted by [underlined text within brackets].

Refinement of security requirements is identified using **bold text**. Any text removed is indicated with a strikethrough (Example: ~~TSF~~).

Iterations are identified by appending a number in parentheses following the component title, for example, FIA_UAU.1 (1) and FIA_UAU.1 (2) refer to two iterations of the FIA_UAU.1 security functional requirement component.

1.4 TOE Overview

VMware Horizon 6 (the TOE) is a virtualization environment that delivers virtual desktops and applications that run in the datacenter to remote users, allowing them to securely access their desktops and applications from any number of devices either within the enterprise or elsewhere. The TOE does not perform the vitalization itself. Horizon 6 manages large numbers of desktops and applications. A single administration console provides granular levels of control, allowing customization of the end-user experience, access, and personalization to support corporate policy, along with centralized control, efficiency, and security by having desktop data in the data center. The names View and Horizon 6 are used interchangeable for the Horizon 6 components.

Major features of the TOE include improved user experience, centralized security and control, and scalability. The TOE supports location-aware resource availability, host USB access, and multi-monitor support. USB devices residing on the client are available to virtual desktops via RDP or the PCoIP remote display protocol chosen. Additionally, PCoIP allows for the use of multi-monitor displays presented as either a single large monitor or as a true collection of monitors. All remoting features, including PCoIP, HTML Access, RDP, USB redirection, and session management work in the same way, as if the user was physically co-located with the desktop.

Horizon 6 supports roaming profiles between desktop sessions via the View Persona Management tool which is not in scope. To maximize scalability, Horizon 6 provides a View Connection Server to broker connections between users and their desktop running within the clustered virtualization environment. Furthermore, View Composer allows multiple desktop images to share virtual disks with a master image, allowing disk space savings and enhanced provisioning times.

Horizon 6 provides several security features, including access control of user environments and 2FA[1] authentication. Additional controls are available through the use of existing Active Directory services. The TOE provides access to virtual desktops and applications via web-based and remote desktop protocols. Communication is secured via TLS tunneling.

Using a vSphere virtual machine as a desktop source, administrators can automate the process of making as many identical virtual desktops as required. Administrators can set a minimum and maximum number of virtual desktops to be generated for the pool. Setting these parameters ensures that there will be enough remote desktops available for immediate use but not so many that available resources are overused. Managing desktops pools and application farms allows users access to applications and desktops that run on servers in a data center instead of on their personal computers or devices. Users can access applications from anywhere on the network. Administrators can easily and quickly grant or remove access to applications for one user or a group of users.

The management capabilities of Horizon 6 allow administrators to provide a familiar, personalized environment to users that they can access from any number of devices anywhere throughout the enterprise or from remote locations. The View Administrator allows centralized administration of both physical and virtual machines.

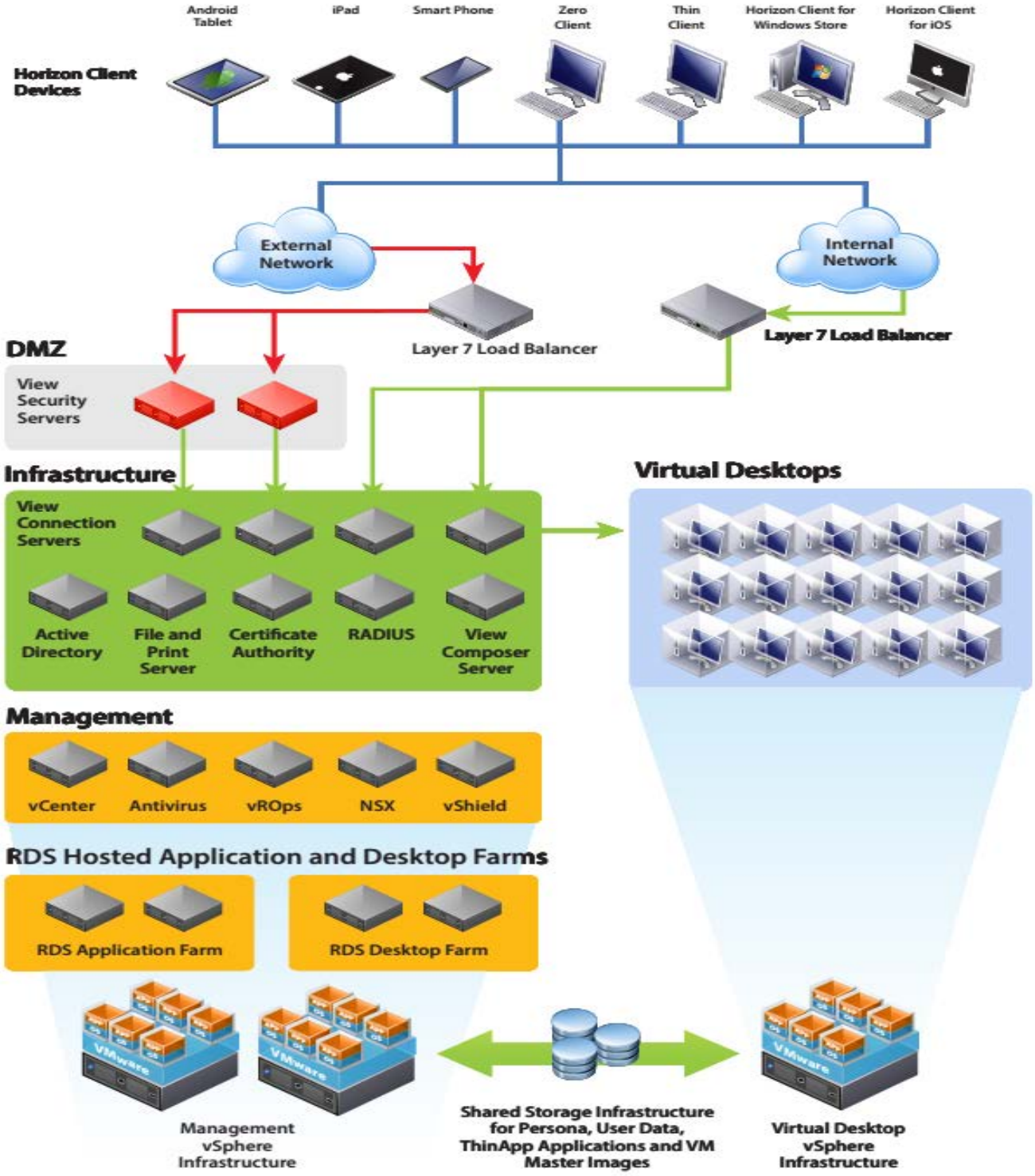
The TOE, as a core capability, allows operating system environments to be run without dependence on client hardware types. This further promotes access via the client, as any user device capable of running the Horizon Client software can access any of the operating system environments available in the (VMware virtualization environments) TOE's datacenter deployment. Internet access extends this

[1] 2FA is two factor authentication

capability beyond PCs, Macs, and thin clients to any device or application supporting one of the featured display protocols.

The TOE provides the following security functionality: User Data Protection, Identification and Authentication, Security Management, Cryptographic operations and trusted communication between TOE components.

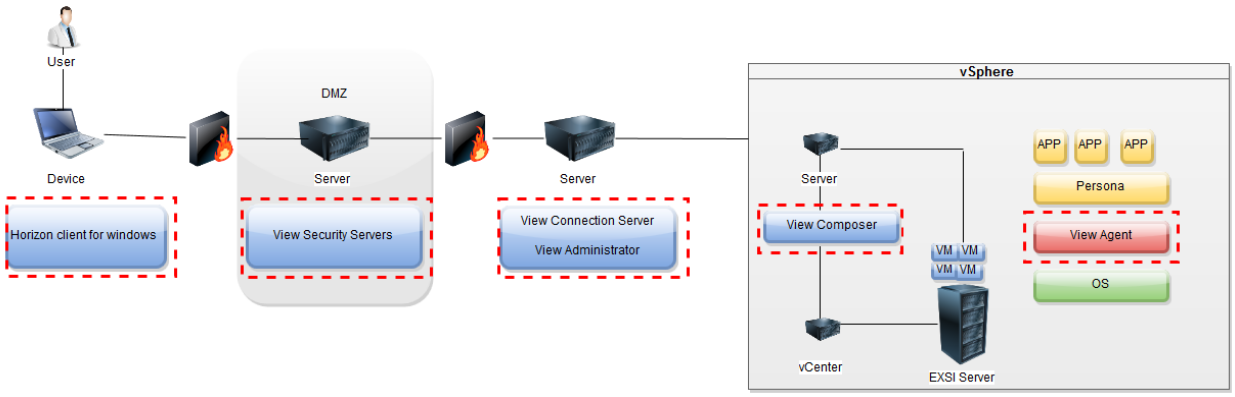
Figure 1: Typical VMware Horizon 6 deployment.



1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

Figure 2: VMware Horizon 6.



1.5.1 Physical Boundary

VMware Horizon 6 is a software-based TOE including:

1. **View Administrator:** View Administrator is a web based application that allows administrators to configure View Connection Server deploy and manage remote desktops and applications, control user authentication, and troubleshoot end-users issues. The View Administrator provides management configuration to the PcoIP Secure Gateway and the Blast Secure Gateway components.

2. **View Connection Server:** View Connection Server streamlines the management, provisioning, and deployment of virtual desktops and applications. View Connection Server can operate in standard[2] or replica[3] mode. As an administrator, you can centrally manage thousands of virtual desktops from a single console. End users connect to View Connection Server to securely and easily access their personalized virtual desktops and applications.

   View Connection Server acts as a broker for client connections by authenticating and directing incoming user desktop requests to the resources that the user is entitled to and wishes to access.

3. **View Security Server:** Outside the corporate firewall, for example within a DMZ, you can install View Connection Server in *security server mode*[4]. Security servers in the DMZ communicate with connection servers inside the corporate firewall. Security servers ensure that the only client traffic that can enter the corporate data center is appropriately secured, including the credentials passed on to the connection server.

   The PCoIP Secure Gateway and Blast Secure Gateway are modules within the View Security Server. The PCoIP Secure Gateway component ensures that the only remote traffic that can

[2] Standard mode
Generates a View Connection Server instance with a new View LDAP configuration.
[3] Replica mode
Generates a View Connection Server instance with a View LDAP configuration that is copied from an existing instance.
[4] Security server mode
Generates a View Connection Server instance that is used to implement an additional layer of security.

enter the corporate data center is traffic on behalf of a strongly authenticated user. When the PCoIP Secure Gateway is enabled, after authentication, clients that use PCoIP can make another secure connection to a security server. You use View Administrator to configure the use of the secure tunnel and PCoIP Secure Gateway. These components ensure that only authenticated users can communicate with remote desktops and applications. This connection allows clients to access remote desktops and applications from the Internet. The Blast Secure Gateway ensures that only authenticated users can communicate with remote desktops by using HTML Access.

4. **View Composer:** View Composer Server is a service that enables you to manage pools of "like" desktops, called linked-clone desktops, by creating master images that share a common virtual disk. Linked-clone desktop images are one or more copies of a parent virtual machine that share the virtual disks of the parent, but which operate as individual virtual machines. Linked-clone desktop images can optimize your use of storage space and facilitate updates. You can make changes to a single master image through the vSphere Client and use View Composer Server to apply the updates to all cloned user desktops that are linked to that master image, without affecting users' settings or persona data.

5. **View Agent:** The View Agent is responsible for the implementation of actions between the guest OS and a user device. You must install View Agent on all managed systems so that connection servers can communicate with them. View Agent also provides features such as session management, virtual printing, persona management, and enforces an access policy to the local clipboard, drives and connected USB devices. View Agent is installed in the guest operating system.

6. **Horizon Client:** Horizon Clients are available for Windows, Mac, Ubuntu Linux, Mobile devices and web browsers to provide the connection to remote desktops and applications from your device of choice. However Mac, Ubuntu Linux, Mobile devices are out of scope for the evaluation.

The physical components of the TOE include the software that is installed during installation of Horizon 6. The TOE software is installed on user devices and on VMWare ESXi hypervisor hosts.

1.5.1.1 Guidance Documentation

The following lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

- VMware Horizon 6 Version 6.2.2 Administration Guide
- VMware Horizon 6 Version 6.2.2 Security Guide
- VMware Horizon 6 Version 6.2.2 Installation Guide
- VMware Horizon 6 Version 6.2.2 Architecture and Planning Guide
- Using VMware Horizon Client for Windows 3.5.2
- Release Notes for VMware Horizon 6 version 6.2.2
- Reviewer's Guide for View in Horizon 6
- Operational User Guidance and Preparative Procedures for VMware Horizon 6 v0.2

1.5.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

User Data Protection

View Administrator provides roles which determine what specific administrators can access and manage. Role membership is determined through Active Directory user and group affiliations. All user roles provide access control measures to the pool of virtual desktops and applications. The TOE allows a single sign-on to be used for authenticating client sessions and remote Windows sessions. View Composer allows users to separate user data from the operating system.

Identification and Authentication:

The TOE requires administrative users to provide unique identification and authentication data before any administrative access to the system is granted. User identification and authentication is done by the TSF through username/password authentication or by an external authentication server. The TOE allows two factor authentication, utilizing smart cards to provide authentication.

Management

View requires integration with Microsoft Active Directory services for user authentication and management. Active Directory is a Windows service for authenticating and authorizing users and computers, applying and enforcing security policies and more. View Connection Server leverages to the existing Active Directory and sets up a lightweight directory services instance for storage of View configuration information.

Cryptographic Operation

The TOE uses FIPS algorithms for the application of cryptography to all communications between TOE components as well as with external users and administrators. These connections are encrypted for transport using TLS, ESP or View Message Security protocols which rely on standard encryption implemented by FIPS 140-2 validated modules within the TOE as well as cryptographic services from the FIPS 140-2 validated Windows cryptographic module in the operational environment.

Trusted Communications between the TOE Components:

The TOE consists of distributed components. Communication between TOE components takes place over TLS, ESP or View Message Security protected connections.

1.5.3 Hardware, firmware, and Software provided by the IT environment

The following hardware, firmware, and software, which are supplied by the IT environment, are required for the TOE to operate. External cryptographic modules used by the TSF must be FIPS 140-2 accredited.

Horizon Client

Table 1 Horizon Client Requirements

HARDWARE COMPONENT	REQUIREMENTS
Version	Horizon Client for Windows v3.5.2
Processor	x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed
Memory	1 GB
Model	Standard x86 or x86 64-bit compatible desktop or laptop computer
Operating System	Windows 10 32-bit/64-bit Enterprise Windows 8/8.1 32-bit/64-bit Pro/Enterprise Windows 7 32-bit/64-bit Home/Enterprise/Professional/ Ultimate

View Connection Server & Security Server

Table 2 View Connection Server & Security Server Requirements

HARDWARE COMPONENT	REQUIREMENTS
Version	View Connection Server v6.2.2 Security Server v6.2.2
Processor	4 CPUs
Memory	10GB RAM or higher
Network Card	1Gbps NICs
Operating System	Windows Server 2008 R2 SP1 64-bit Standard/Enterprise Windows Server 2012 R2 64-bit Standard

View Composer

Table 3 View Composer Requirements

COMPONENT	MINIMUM REQUIREMENTS
Version	View Composer v6.2.2
Processor	1.4 GHz or faster Intel 64, or AMD 64 with 2 CPUs
Network	One or more 10/100Mbps network interface cards (NICs)

COMPONENT	MINIMUM REQUIREMENTS
Memory	4GB RAM or higher
Disk Space	40GB
Operating System	Windows Server 2008 R2 SP1 64-bit Standard/Enterprise/Datacenter Windows Server 2012 R2 64-bit Standard/Datacenter
DBMS	Microsoft SQL Server 2008 SP4 (express, standard, enterprise) Microsoft SQL Server 2008 R2 (express, standard, enterprise, datacenter) Microsoft SQL Server 2012 (express, standard, datacenter) Microsoft SQL Server 2014 (stand, enterprise) Oracle Database 11g Release 2 (latest -11.2.0.4) Oracle Database 12c Release 1 (any version to latest)

View Agent

Table 4 View Agent Supported Operating systems

SUPPORTED OPERATING SYSTEMS
Windows 10 (64-bit and 32-bit) Enterprise and Professional
Windows 8.1 (64-bit and 32-bit) Enterprise and Professional No SP and Update
Windows 8 (64-bit and 32-bit) Enterprise and Professional No SP
Windows 7 (64-bit and 32-bit) Enterprise and Professional SP1
Windows Server 2012 R2 (64-bit) Datacenter No SP
Windows Server 2008 R2 (64-bit) Datacenter SP1

Network

The following hardware, firmware, and software, which are supplied by the operational environment, are required for the network configuration. These components are not part of the TOE.

- VMware ESXi 6.0.0b
- VMware vCenter Server 6.0.0b
- VMware vSphere 6.0.0b
- Microsoft Active Directory

Web Browser

View Administrator is a web-based application that is deployed when you install View Connection Server (except View Connection Server in security server mode). The computer on which you launch View

Administrator must trust the root certificate of the connection server's TLS certificate. Supported web browsers already trust the root certificates of well-known certificate authorities (CAs). You can access and use View Administrator with the following Web browsers:

Table 5 Web Browsers for View Administrator

SUPPORTED WEB BROWSERS
Internet Explorer 10, 11
Firefox latest releases
Safari 6 and later releases

Optional Hardware and Software to support the TOE

The following hardware, firmware, and software are supplied by the operational environment if needed.

- Smartcard readers is required if Horizon View is configured to use a Smartcard authentication system.

1.5.4 Product Features and Functions not included in the TOE

Physical/logical features and functions of Horizon 6 that are not part of the evaluated configuration of the TOE are:

- Stand-alone (non-clustered) operation
- View Persona Management
- Horizon vRealize
- Virtual volumes
- Client Drive Redirection
- Cloud Pod Architecture
- Windows Media MMR
- API usage and 3rd party scripting
- Connections via Remote Desktop Protocol (RDP)
- Horizon Client software on Mac, Ubuntu Linux, Mobile devices
- Zero clients

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The Security Target is conformant to Common Criteria Version 3.1 Revision 4, September 2012, Part 2 extended and Part 3 conformant. The ST claims conformance to Evaluation Assurance Level 2 EAL2+ augmented with ALC_FLR.2

2.2 Protection Profile Conformance Claim

The Security Target does not make any PP conformance claims.

3 SECURITY PROBLEM DEFINITION

This section defines the security problem which the TOE and its operational environment are supposed to address. Specifically, the security problem makes up the following:

- Any known or assumed threats encountered by the TOE or its operational environment.
- Any organizational security policies with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This section identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

This section identifies the threats to the assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.

TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

The table below lists threats applicable to the TOE and its operational environment:

Table 6 Threats

Threat	Description
T.ATTACK_ACCESS	An attacker may gain unauthorised access to a desktop or application.
T.USER_ACCESS	A TOE user may gain unauthorised access to a desktop or application.
T.USER_DATA	A TOE user may gain unauthorised access to another user's data or use the TOE to infiltrate data.
T.SPOOF	An attacker may cause communication between a TOE user and a TOE service to be redirected, such that users of the TOE may incorrectly believe they are accessing the TOE when they are not. This may lead to compromise of user data or credentials.
T.INTERCEPT	An attacker may intercept communication channels. This may lead to compromise of users' credentials.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following table lists Organizational Security Policies (OSP) applicable to the TOE and its operational environment:

Table 7 Organizational Security Policies

OSP	Description
P.CRYPTO	Cryptographic functions shall be validated to FIPS 140-2 Level 1

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to operate. The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 8 Assumptions

Assumption	Description
A.PHYSICAL	It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TSF and the value of the stored and processed information.
A.VM_HOST	The VM host software provides virtual machine isolation and is operating correctly and securely
A.CHANNEL_PROTECTION	Operational Environment administrators are assumed to have configured IPsec associations between security servers and connection servers such that forwarded requests from client components to connection servers, and responses to such requests, are confidentiality and integrity protected. (Forwarded requests are carried over TCP connections to IP port 8009 of connection servers that have been paired with security servers.)

4 SECURITY OBJECTIVES

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. This high-level solution is divided into two parts: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are as follows:

Table 9 TOE Security Objectives

Security Objective	Description
O.AUTH_USER	The TOE users and administrators must be successfully identified and authenticated before being granted access to the TOE
O.USER_ACCESS	The TOE will grant access only to desktops, applications, and desktops resources for which the user has been entitled
O.SECURE_SETUP_DATA	The TOE will provide confidentiality and integrity of data required for setup and assignment of a desktop, applications, and desktops resources during transmission between TOE components and TOE and non-TOE components.
O.USE_FIPS	The TOE components must use or invoke cryptographic modules validated in a FIPS 140-2 level 1 configuration
O.CONFIG_ACCESS	The TOE allows desktops, applications, and desktops resources to be configurable by an administrator
O.ENDPOINT_RESOURCE	The TOE allows an administrator to control the use of the clipboard, drives and USB access by authorised desktop and application users
O.CHANNEL_PROTECTION	Communication between TOE components and trusted IT products and TOE to TOE components must have confidentiality and integrity protection, whether provided entirely by the TSF or by a combination of the TSF and the operating environment.

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

Table 10 Operational Environment Security Objectives

Security Objective	Description
OE.CONFIG_SERVER	The operating systems of the server components must be securely configured, including appropriate file protection. This includes memory used by TOE components supporting a user session once the session has ended.
OE.CONFIG_VM_HOST	VM Host software must be securely configured. The deployment must provision a VM Host that provides a suitable virtual machine isolation since this is relied upon to effect separation of user's virtual desktops.
OE.CONFIG_TP_SW	Trusted third-party software must be securely configured. Trusted third-party software is defined as: • Oracle database • Microsoft Windows (including Active Directory) • Microsoft SQL server Applications must be configured by administrators such that it is not possible for users to gain access to the underlying operating system or hardware.
OE.AUTHENTICATE	Users and administrators must be authenticated by Active Directory, smart card.
OE.CHANNEL_PROTECTION	Communication between TOE components and trusted IT products and TOE to TOE components where not protected entirely by the TOE, must use channel protection functionality of the underlying operating system. Where necessary, the operational environment will invoke and provide secure channels between the TOE and trusted IT products.
OE.ENCRYPTION	Secure encryption modules in the Operational Environment that are used to provide channel protection must be configured per the FIPS 140-2 level 1 security policy.
OE.SERVER_PHYSICAL	The operational environment shall provide physical protection to all TOE components, except the Horizon Client, to ensure only administrators are able to gain physical access.
OE.ADMIN_USERS	Configuration data stored outside the TOE, such as in a database, must be accessible only by administrators.

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies if applicable. The following table provides a high level mapping of coverage for each threat, assumption, and policy:

Table 11 Cross Reference of Threats, Assumptions and Policies

Objectives mapped to Assumptions , Threats and Policies	T.ATTACK_ACCESS	T.USER_ACCESS	T.USER_DATA	T.SPOOF	T.INTERCEPT	P.CRYPTO	A.PHYSICAL	A.VM_HOST	A.CHANNEL_PROTECTION
O.AUTH_USER	X	X							
O.USER_ACCESS	X	X	X						
O.SECURE_SETUP_DATA					X				
O.USE_FIPS						X			
O.CONFIG_ACCESS		X	X						
O.ENDPOINT_RESOURCE									
O.CHANNEL_PROTECTION			X	X	X				
OE.CONFIG_SERVER	X		X						
OE.CONFIG_VM_HOST	X		X					X	
OE.CONFIG_TP_SW	X		X						
OE.AUTHENTICATE	X	X	X						
OE.CHANNEL_PROTECTION			X	X	X				X
OE.ENCRYPTION			X		X	X			
OE.SERVER_PHYSICAL							X		
OE.ADMIN_USERS							X		

Table 12 - Detailed Rationale of Threats, Policies and Assumptions

Threats, Policies and Assumptions	Objectives	Rationale
T.ATTACK_ACCESS An attacker may gain unauthorised access to a desktop or application.	O.AUTH_USER O.USER_ACCESS OE.AUTHENTICATE OE.CONFIG_SERVER OE.CONFIG_VM_HOST OE.CONFIG_TP_SW	O.AUTH_USER ensures all users, including an attacker, must be successfully authenticated and authorised before granting access to a desktop or application. OE.AUTHENTICATE ensures all users are authenticated by an external authentication server (if configured) prior to granting access to desktop or application. O.USER_ACCESS ensures that users can access only desktops and applications they have permission to, thus preventing any unauthorized user access. OE.CONFIG_SERVER ensures the servers and the underlying OS have been set up properly and securely, thus preventing unauthorised access by the attacker due to misconfiguration. OE.CONFIG_VM_HOST ensures the VM host software is securely configured thus any compromise by the attacker will be contained and isolated to the affected VM host only. OE.CONFIG_TP_SW ensures securely configured third-party software will prevent any users, including an attacker from accessing the TOE's underlying OS.
T.USER_ACCESS A TOE user may gain unauthorised access to a desktop or application.	O.AUTH_USER O.USER_ACCESS OE.AUTHENTICATE O.CONFIG_ACCESS	O.AUTH_USER ensures all users must be successfully authenticated and authorised before granting access to a desktop or application. OE.AUTHENTICATE ensures all users are authenticated by an external authentication server (if configured)

Threats, Policies and Assumptions	Objectives	Rationale
		prior to granting access to desktop or application. O.USER_ACCESS ensures that users can access only desktops and applications they have permission to, thus preventing any unauthorized user access. O.CONFIG_ACCESS ensures that only administrators have the ability to entitle users to desktops and applications, thus centralizing and securely managing TOE user's access. The will prevent any users, other than the trusted administrator in granting unauthorized access to users.
T.USER_DATA A TOE user may gain unauthorised access to another user's data or use the TOE to infiltrate data.	O.USER_ACCESS O.CHANNEL_PROTECTION OE.CHANNEL_PROTECTION OE.ENCRYPTION O.CONFIG_ACCESS OE.CONFIG_SERVER OE.CONFIG_VM_HOST OE.CONFIG_TP_SW	O.USER_ACCESS ensures that users can access only desktops, applications, and desktop resources they have permission to, thus preventing access to another user's desktop or application. O.CHANNEL_PROTECTION, OE.CHANNEL_PROTECTION and OE.ENCRYPTION ensure the confidentiality and integrity of data, including authentication credential and session establishment data are not tampered with thus preventing unauthorised access to another user's data. O.CONFIG_ACCESS ensures that the virtual desktops, published applications and desktops resources have been set up properly by the trusted administrator disallowing inadvertent unauthorised access. OE.CONFIG_SERVER ensures the servers have been configured properly in order to enforce the content of the virtual desktop memory is reserved for that user after the user has logged out of the virtual desktop which prevents

Threats, Policies and Assumptions	Objectives	Rationale
		another user's access to this content. OE.CONFIG_VM_HOST and OE.CONFIG_TP_SW ensure potentially privileged programs on the VM Host and trusted third-party software do not undermine security thus allowing unauthorized user data access.
T.INTERCEPT An attacker may intercept communication channels. This may lead to compromise of users' credentials.	O.SECURE_SETUP_DATA O. CHANNEL_PROTECTION OE.CHANNEL_PROTECTION OE.ENCRYPTION	O.SECURE_SETUP_DATA ensures the confidentiality and integrity of setup and assignment data communicated between TOE components are secured thus preventing an attacker to decipher or read the transmitted data. O.CHANNEL_PROTECTION, OE.CHANNEL_PROTECTION and OE.ENCRYPTION ensure the confidentiality and integrity of communications between TOE components are encrypted and secure thus preventing an attacker to interpret the intercepted data.
T.SPOOF An attacker may cause communication between a TOE user and a TOE service to be redirected, such that users of the TOE may incorrectly believe they are accessing the TOE when they are not. This may lead to compromise of user data or credentials.	O.CHANNEL_PROTECTION OE.CHANNEL_PROTECTION	O.CHANNEL_PROTECTION and OE.CHANNEL_PROTECTION ensure the communication channel between the TOE and the TOE user has confidentiality and integrity protection to detect modification to data that will identify an attacker's redirection.
A.PHYSICAL It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TSF and the value of the stored and processed information.	OE.SERVER_PHYSICAL OE.ADMIN_USERS	OE.SERVER_PHYSICAL and OE.ADMIN_USERS ensure that servers are physically protected and only accessible by administrators. The TSF does not protect the assets co-located with the Horizon client.
A.VM_HOST	OE.CONFIG_VM_HOST	OE.CONFIG_VM_HOST ensures that

Threats, Policies and Assumptions	Objectives	Rationale
The VM host software provides virtual machine isolation and is operating correctly and securely.		these requirements are met.
A.CHANNEL_PROTECTION Operational Environment administrators are assumed to have configured IPsec associations between security servers and connection servers such that forwarded requests from client components to connection servers, and responses to such requests, are confidentiality and integrity protected. (Forwarded requests are carried over TCP connections to IP port 8009 of connection servers that have been paired with security servers.)	OE.CHANNEL_PROTECTION	OE.CHANNEL_PROTECTION ensures that channel protection that is not wholly provided by the TSF is provided in whole or part by the underlying operating system.
P.CRYPTO Cryptographic functions shall be validated to FIPS 140-2 Level 1	OE.ENCRYPTION O.USE_FIPS	OE.ENCRYPTION ensures that the servers are configured to use FIPS 140-2 Level 1 validated algorithm implementations. O.USE_FIPS ensures that the TOE components invoke the cryptographic functions in accordance with the conditions of the validation.

5 EXTENDED SECURITY REQUIREMENT COMPONENTS DEFINITION

This section defines the extended Security Functional Requirements (SFRs) and extended Security Functional Assurance Requirements (SARs) met by the TOE.

5.1 Extended TOE Security Functional Requirement Components

There are no extended TOE Security Functional Requirement Components.

5.2 Extended TOE Security Assurance Requirement Components

There are no extended TOE Security Assurance Requirement Components.

6 SECURITY REQUIREMENTS

This section defines the Security Functional Requirements (SFRs) and Security Functional Assurance Requirements (SARs) met by the TOE.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

Table 13 TOE Security Functional Requirements

Requirement Class	Requirement Name	Description
FCS Cryptographic support	FCS_CKM.1 (1)	TOE cryptographic key generation for AES
	FCS_CKM.1 (2)	TOE cryptographic key generation for RSA
	FCS_CKM.4	TOE cryptographic key destruction
	FCS_COP.1	TOE cryptographic operation
FDP User Data Protection	FDP_ACC.1(1)	Access control policy (for Desktop)
	FDP_ACC.1(2)	Access control policy (for Application)
	FDP_ACC.1(3)	Access control policy (for Resources)
	FDP_ACF.1(1)	Access control function (for Desktop)
	FDP_ACF.1(2)	Access control function (for Application)
	FDP_ACF.1(3)	Access control function (for Resources)
FIA Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UID.2	User identification
	FIA_UAU.2	User authentication
	FIA_UAU.5	User authentication multiple mechanisms
FMT Security Management	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security management roles
FPT Protection of the TSF	FPT_ITC.1	Confidentiality of exported TSF data
	FPT_ITI.1	Integrity of exported TSF data
	FPT_ITT.1	Internal TOE TSF data transfer
FTA Session locking and termination	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination

6.1.1 Cryptographic Support (FCS)

6.1.1.1 FCS_CKM.1(1)/AES Cryptographic Key Generation

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***AES***] and specified cryptographic key sizes [***128- and 256-bit***] that meet the following: [***FIPS 197***].

6.1.1.2 FCS_CKM.1(2)/RSA Cryptographic Key Generation

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA**] and specified cryptographic key sizes [**2048- and 3072-bit**] that meet the following: [**FIPS 186-4**].

6.1.1.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**FIPS140-2 standard**].

Application note Cryptographic keys in memory are protected by the TOE against unauthorized access and are destroyed by the object re-use functions of the TOE.

6.1.1.4 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [
encryption and decryption] in accordance with a specified cryptographic algorithm [**AES**] and cryptographic key sizes [**128- or 256-bit**] that meet the following: [**RFC 5246**; **FIPS 140-2**].

Application note Communication channels identified above use the TLSv1.2 protocol as defined in RFC 5246. Cipher suites are selected from the following list:
TLS_RSA_WITH_AES_256_CBC_SHA256, or
TLS_RSA_WITH_AES_256_CBC_SHA, or
TLS_RSA_WITH_AES_128_CBC_SHA256, or
TLS_RSA_WITH_AES_128_CBC_SHA.

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1(1)/Desktop Subset access control

FDP_ACC.1.1(1) The TSF shall enforce the [**Desktop Access Policy**] on [Subject: user session, Object: desktop, Operation: connect to the desktop].

6.1.2.2 FDP_ACF.1(1)/Desktop Security attribute based access control

FDP_ACF.1.1(1) The TSF shall enforce the [**Desktop Access Policy**] to objects based on the following: [User session: resource group, *Desktops:* resource group/permission pair, *View Agent*].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

A desktop running the Agent shall be accessible[5] by a user only if the user provided to the TSF contains a matching resource group with permission to access the requested agent].

FDP_ACF.1.3(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**None**].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**The user's session exceeds the allocated VM resource quotas for that group, or the Agent and Guest OS are not running or not available**].

6.1.2.3 FDP_ACC.1(2)/Application Subset access control

FDP_ACC.1.1(2) The TSF shall enforce the [**Application Access Policy**] on [**Subject: user session, Object: application, Operation: access**].

6.1.2.4 FDP_ACF.1(2)/Application Security attribute based access control

FDP_ACF.1.1(2) The TSF shall enforce the [**Application Access Policy**] to objects based on the following: [*User session: resource group, Application: resource group/permission pair, View Agent*].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

[5] Once this access is granted via this access policy the user still requires authentication to that desktop's OS.

An application running the Agent shall be accessible by a user only if the user provided to the TSF contains a matching resource group with permission to access the requested agent].

FDP_ACF.1.3(2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**None**].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**The application is not published or not available**].

6.1.2.1 FDP_ACC.1(3)/Resources Subset access control

FDP_ACC.1.1/Resources The TSF shall enforce the [**Resources Access Policy**] on [**Subject: user session, Object: desktop resources (USB, Clipboard, CD/DVD), Operation: access**].

6.1.2.2 FDP_ACF.1/Resources Security attribute based access control

FDP_ACF.1.1/Resources The TSF shall enforce the [**Resources Access Policy**] to objects based on the following: [*User session: resource group, Application: resource group/permission pair, View Agent*].

FDP_ACF.1.2/Resources The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

A Desktop Resource shall be accessible by a user only if

- **The user is a member of a resource group which provides permission to the requested desktop resource]**

FDP_ACF.1.3/Resources The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**None**].

FDP_ACF.1.4/Resources The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**The requested resource is unavailable**].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **desktop users and application** users: [*Resource Group, password, role, userID*].

6.1.3.2 FIA_UID.2 User identification

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UAU.2 User authentication

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.4 FIA_UAU.5 User authentication multiple mechanisms

FIA_UAU.5.1 The TSF shall provide [**credential capture and authentication system interfaces for:**

- **Active Directory username and password, and**
- **Active Directory alternate security identity (from client certificates, CAC cards, and PIV cards)**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**authentication setting for that user**].

6.1.4 Security Management (FMT)

6.1.4.1 FMT_SMR.1 Security management roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrators, Administrators (Read only), Agent Registration Administrators, Global Configuration and Policy Administrators, Global Configuration and Policy Administrators (Read only), Inventory Administrators, Inventory Administrators (Read only), Local Administrators, Local Administrators (Read only)**].

Application note Additional roles can be added as required.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.4.2 FMT_SMF.1 Specification of Management Functions

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

- **Administration of policy, including idle session policy**
- **Allocation of roles to administrative users**
- **Administration of access to desktop resources**
- **User authentication management**
- **Administration of entitlements to published applications**
- **Administration of entitlements and assignments to desktops**].

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

6.1.5.2 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [**a single message authentication code error during transmission**].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [**discontinuation of the communication channel or disregard of the data**] if modifications are detected.

6.1.5.3 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

6.1.6 Session locking and termination (FTA)

6.1.6.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**configurable amount of time**].

6.1.6.2 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2 Security Assurance Requirements

This section defines the Security Assurance Requirements (SARs) for the TOE. The assurance requirements are taken from EAL 2 components as specified in Part 3 of the CC and are augmented with ALC_FLR.2 requirements. The assurance components are summarized in the following table:

Table 14 – Security Assurance Requirements

CLASS	FAMILY	DESCRIPTION
ASE: Security Target	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6.3 Dependency Rationale

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 15 – Dependency Rationale

SFR	DEPENDENCY	RATIONALE
FPT_ITC.1	None	None
FPT_ITI.1	None	None
FPT_ITT.1	None	None
FCS_CKM.1 (1)-(2)	FCS_CKM.4, FCS_COP.1	Satisfied
FCS_CKM.4	FCS_CKM.1	Satisfied
FCS_COP.1	FCS_CKM.1, FCS_CKM.4	Satisfied
FDP_ACC.1 (1)	FDP_ACF.1 (1)	Satisfied
FDP_ACC.1 (2)	FDP_ACF.1 (2)	Satisfied
FDP_ACC.1 (3)	FDP_ACF.1 (3)	Satisfied
FDP_ACF.1 (1)	FDP_ACC.1 (1)	Satisfied.
FDP_ACF.1 (2)	FDP_ACC.1 (2)	Satisfied
FDP_ACF.1 (3)	FDP_ACC.1 (3)	Satisfied
FIA_ATD.1	None	None
FIA_UID.2	None	None
FIA_UAU.2	FIA_UID.1	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies the dependency.
FIA_UAU.5	None	None
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Satisfied
FTA_SSL.3	None	None
FTA_SSL.4	None	None

6.4 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

Table 16 – Mapping of SFR's to Objectives

SFR Mapped to Objectives	O.AUTH_USER	O.USER_ACCESS	O.CHANNEL_PROTECTION	O.USE_FIPS	O.CONFIG_ACCESS	O.ENDPOINT_RESOURCE	O.SECURE_SETUP_DATA
FPT_ITC.1			X				X
FPT_ITI.1			X				X
FPT_ITT.1			X				X
FCS_CKM.1 (1)			X	X			
FCS_CKM.1 (2)			X	X			
FCS_CKM.4			X	X			
FCS_COP.1			X	X			
FDP_ACC.1 (1)		X			X		
FDP_ACC.1 (2)		X			X		
FDP_ACC.1 (3)		X			X	X	
FDP_ACF.1 (1)		X			X		
FDP_ACF.1 (2)		X			X		
FDP_ACF.1 (3)		X			X	X	
FIA_ATD.1	X	X					
FIA_UID.2	X						
FIA_UAU.2	X						
FIA_UAU.5	X						

SFR Mapped to Objectives	O.AUTH_USER	O.USER_ACCESS	O.CHANNEL_PROTECTION	O.USE_FIPS	O.CONFIG_ACCESS	O.ENDPOINT_RESOURCE	O.SECURE_SETUP_DATA
FMT_SMF.1		X			X	X	X
FMT_SMR.1		X			X	X	X
FTA_SSL.3	X						
FTA_SSL.4	X						

The following table provides detailed evidence of coverage for each security objective:

Security Objective	SFR	Rationale
O.AUTH_USER	FTA_SSL.3 FTA_SSL.4 FIA_UID.2 FIA_UAU.2 FIA_UAU.5 FIA_ATD.1	FIA_UID.2, FIA_UAU.2, and FIA_UAU.5 ensure that desktop users and administrators are successfully identified and authenticated before they can use TOE functionality. FTA_SSL.3 and FTA_SSL.4 ensures user identification and authentication are required after termination. FIA_ATD.1 contributes to satisfying this objective by maintaining attributes used for user identification and authentication.
O.USER_ACCESS	FIA_ATD.1 FMT_SMR.1 FMT_SMF.1 FDP_ACC.1(1)-(3) FDP_ACF.1(1)-(3)	FIA_ATD.1 ensures users can be granted access permissions to desktops and applications based on security attributes assigned. FMT_SMR.1 and FMT_SMF.1 ensure that administrators can assign permissions to the users in order to access desktops and applications. FDP_ACC.1 (1)/Desktop and FDP_ACF.1(1)/Desktop ensure that only desktop users with the correct access permissions can gain access to a desktop. FDP_ACC.1 (2)/Application and FDP_ACF.1 (2)/Application ensure that only application users with the correct access permissions can

Security Objective	SFR	Rationale
		gain access to an application. FDP_ACC.1(3)/Resource & FDP_ACF.1(3)/Resource ensure that only users with the correct permissions can gain access to desktop resources.
O.CHANNEL_PROTECTION	FPT_ITC.1 FPT_ITI.1 FPT_ITT.1 FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.4 FCS_COP.1	FPT_ITC.1, FPT_ITI.1 and FPT_ITT.1 ensure a distinct communication channel is used and FCS_CKM.1(1)/AES, FCS_CKM.1(2)/RSA, FCS_CKM.4 and FCS_COP.1 ensure cryptographic supports is used to secure the communication channel.
O.SECURE_SETUP_DATA	FPT_ITC.1 FPT_ITI.1 FPT_ITT.1 FMT_SMR.1 FMT_SMF.1	FPT_ITC.1, FPT_ITI.1 and FPT_ITT.1 ensure the confidentiality and integrity of communications between TOE components and TOE and non-TOE components . FMT_SMR.1 and FMT_SMF.1 ensure that administrators can manage configuration data.
O.USE_FIPS	FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.4 FCS_COP.1	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4 and FCS_COP.1 ensure that the cryptographic functions are invoked in conformance with any conditions of the FIPS 140-2 level 1 validation of the cryptographic modules being used.
O.CONFIG_ACCESS	FMT_SMR.1 FMT_SMF.1 FDP_ACC.1(1)-(3) FDB_ACF.1(1)-(3)	FMT_SMR.1 and FMT_SMF.1 ensure that administrators can add, modify or delete desktop and application, and desktop resources configuration data. FDP_ACC.1/Desktop, FDB_ACF.1/Desktop, FDP_ACC.1/Application, and FDP_ACF.1/Application ensure that only administrators can gain access to desktop and application configuration data. FDP_ACC.1 (3)/Resource and FDP_ACF.1 (3)/Resource ensure that to access to desktop resources is configurable by an administrator.
O.ENDPOINT_RESOURCE	FMT_SMR.1	FMT_SMR.1 and FMT_SMF.1 ensure that only authorized administrators can enable

Security Objective	SFR	Rationale
	FMT_SMF.1 FDP_ACC.1(3) FDP_ACF.1(3)	or disable cut and paste, client drive mapping, and USB device access functions. FDP_ACC.1 (3)/RESOURCES and FDP_ACF.1 (3)/RESOURCES ensure that desktop users can only cut and paste data between virtual desktop and the user device operating system clipboard, access user device client drives from the virtual desktop, or access USB devices on a user device from the virtual desktop if such functionality has been enabled by an administrator and the user has permitted the access.

6.4.2 Security Assurance Requirements

This section defines the Security Assurance Requirements (SARs) for the TOE. The assurance requirements are taken from EAL 2 components as specified in Part 3 of the CC and are augmented with ALC_FLR.2 requirements. The assurance components are summarized in the following table:

Table 17 – Security Assurance Requirements

CLASS	FAMILY	DESCRIPTION
ASE: Security Target	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6.4.3 Security Assurance Requirements Rationale

Assurance level EAL2 was chosen to provide a low to moderate level of assurance that is consistent with standard commercial practices. The chosen assurance level is appropriate given the threats defined for the operational environment.

7 TOE SUMMARY SPECIFICATION

This section presents information to detail how the TOE meets the security functional requirements described in previous sections of this ST.

7.1 Administrator access control

Administrators and users must have valid accounts in Active Directory and must be identified and authenticated. Administrators must log in to the View Administrator Console. This is done by forming an HTTPS connection to a View Connection Server from a web browser. Attempts to connect to View Administrator over HTTP result in an error.

The TOE requires all administrators to authenticate successfully, using single- or two-factor credentials, before any administrative access to the system is granted. The roles in FMT_SMR.1 control which management features user perform.

The Administrator access control satisfies the following requirements: FIA_UID.2, FIA_UAU.2, FMT_SMR.1.

7.2 Administration of user authorization

The TOE management is integrated with Active Directory, allowing TOE administrators to assign roles to other administrative users and to entitle users to desktops and applications. Configuration includes:

- Access permissions for administrators (roles and permissions), determining whether administrative users can access configuration data;
- Access permissions for users (entitlements and assignments), determining which desktops and applications each user can access.
- Access permissions for desktop resources

These administration mechanisms satisfy the FDP_ACC.1 (1), FDP_ FDP_ACC.1 (2), FMT_SMR.1 and FMT_SMF.1 requirements as well as the FIA_ATD.1 requirement.

7.3 User access control

View Connection Server in security server mode provides the means for a user to log in to the TOE across an untrusted network in order to gain access to their virtual desktops and applications. This entity is typically located at the edge of the corporate or departmental network in a DMZ, providing access to View without exposing the entire view infrastructure. The security server receives the user's credentials, which may be username and password, or multifactor authentication such as a smart card. The security server forwards the credentials to a View Connection Server on the internal network, which interacts with Active Directory, perhaps in conjunction with another authentication system in order to identify and authenticate the user. Access is granted to a user only if they can logon successfully to Active Directory and have an entitlement to at least one desktop or application.

The Desktop Access Policy controls user access to desktops based on the View Agent and the permissions assigned to the user's matching resource group. The Application Access Policy controls user access to published applications based upon the permissions assigned to the user's matching resource group. The Resource Access Policy controls the user's ability to access the desktop resources.

Once a user has logged out of a virtual desktop, the virtual desktop and its virtual machine may be preserved and available only for that user, or the desktop may be reset for a subsequent login.

The TOE disconnects all desktops and applications after an administrator-specified number of minutes have passed since the user logged in to View, including all SSO credentials. This feature protects application sessions using a combination of session timeouts and detecting when there is no keyboard or mouse activity on the client device. In addition users are allowed to terminate their own session.

Users must log in again to reconnect to the applications that were disconnected, or launch a new desktop or application.

The user access control mechanisms satisfy the FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 identification and authentication requirements for users, as well as the access policy requirements (FDP_ACC.1 (1), FDP_ACF.1(1), FDP_ACC.1(2) FDP_ACF.1(2), FDP_ACC.1 (3), FDP_ACF.1(3) and termination requirements (FTA_SSL.3, FTA_SSL.4)).

7.4 Cryptographic Support

All cryptographic services in the TOE are provided by leveraging the FIPS 140-2 Level 1 validation of either VMware Horizon JCE[6] or OpenSSL with FIPS Canister 2.0, which are within the TOE. Some implementations are performed by the underlying operating system, where the TOE initiates the connection but invokes cryptographic operations by calling into the Microsoft CNG. These cryptographic services are provided by the operational environment.

All TLS-protected channels use TLSv1.2 only, using some or all of the following cipher suites, as defined in RFC 5246:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

The TOE and its subsystems use the OpenSSL FIPS Object Module (#1747) in Approved mode of operation. The OpenSSL binary is created from the same source code as listed on CMVP certificate #1747 and is statically bound to each subsystem. The binary is built following the exact methods prescribed in Appendix A of the Security Policy document. VMware directly received the code that makes up certificate #1747 from the OpenSSL Software Foundation on physical CDs. Those CDs were physically handed off to a member of VMware's Build Team, who loaded and re-verified the SHA hash before creating OpenSSL builds using the specification provided by the OpenSSL Software Foundation. Those builds were checked into VMware's source and object control system repository for consumption by VMware products. Horizon 6 was then built, pulling those binaries into all TOE components that use OpenSSL. The TOE has been configured to use the OpenSSL builds per the security policy listed on the CMVP site. The VMware affirms that the OpenSSL builds used on each platform contain the same binaries as those provided from the OpenSSL Software Foundation which were verified by the SHA hash.

OpenSSL is used by:

- View clients on all platforms

[6] VMware Horizon JCE completed FIPS validation with certificate #2559

- PCoIP Secure Gateway and Blast Secure Gateway
- PCoIP and Blast servers
- Composer for its ESX communication channel

The TOE's cryptographic modules can generate cryptographic 128-bit and 256-bit cryptographic keys using the AES key generation algorithm, meeting FIPS 197. The TOE's cryptographic modules can generate cryptographic 2048-bit and 3072-bit cryptographic keys using the RSA key generation algorithm, meeting FIPS 186-4. In addition, the cryptographic modules perform key destruction using zeroization.

Where the TOE invokes cryptographic operations implemented by the underlying operating system, calls are made via the FIPS-140 validated modules listed in the table below:

Table 18– Microsoft Modules Certificates

Microsoft Modules	Certificate Number
Windows 7 and Windows 7 SP1	#1329, #1330,
Windows Server 2008 R2 and Windows Server 2008 R2 SP1	#1329, #1337
Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8	#1892, #1894

Microsoft CNG must be located in the operational environment and run in a FIPS validated configuration.

Cryptographic support satisfies the following security functional requirements: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4, FCS_COP.1.

7.5 Secure communications

Communication between a Horizon client component and a View Connection Server is protected by TLSv1.2, whereby the server certificate is verified using Public Key Infrastructure mechanisms, after which data is encrypted to provide confidentiality and integrity.

There are many secure communication channels between the TOE components and trusted IT components such as VMware vCenter, VMware ESX, and Oracle DB which are protected by TLSv1.2. In some cases, channels are created and managed by operational environment services invoked by the TOE. Protection is then provided and enforced by the operational environment on behalf of the TSF.

The TOE consists of distributed components. Communication between TOE components is protected either by TLS, ESP or View Message Security[7]. The View Message Security provides authentication through the messaging router for communication between View Connection Server (TOE server) components and View Agent components. This component supports Java Message Service (JMS) API, which is used for messaging in View. In addition, View Message Security provides confidentiality and integrity of the data transmitted. The TSF relies on the prior establishment of an IPsec association

[7] View Message Security is an AES-128-CTR encryption with DSA-2048 signing

between a security server and a connection server in order to protect data over a (AJP) endpoint communication.

TLS provides authentication of TOE server and View Agent components as part of the secure channel protocol, as well as providing confidentiality and integrity. Implementation of TLS or ESP is predominantly within the TOE, leveraging either the FIPS modules within the TOE or within the operational environment. The TOE invokes the uses of TLS, ESP or View Message Security in most case, regardless of whether the cryptographic module resides in the TOE or in the operational environment. Additional details are located in the tables below.

7.5.1 Connection Server

The connection server makes use of several cryptographic libraries and functions to secure messages in transit. The following ports and interfaces are cryptographically secured by the TOE:

Table 19 - Connection Server Cryptography Usage

Direction	Endpoint Communication	Provider	Protection
Incoming	View Agents and Security Servers over JMS (4001) [bootstrap]	VMware JCE	AES-128-CTR encryption with DSA-2048 signing
Incoming	View Agents and Security Servers over JMS (4002)	VMware JCE	TLS 1.2
Bi-Directional	Connection Servers over JMS-IR (4101)	VMware JCE	TLS 1.2
Incoming	Security Servers over AJP	Windows (OE protection relied upon by TOE – see A.CHANNEL_PROTECTION)	ESP (IPsec transport mode)
Incoming	Horizon Clients and web browsers over HTTPS (443)	VMware JCE	TLS 1.2
Incoming	Web browsers over HTTPS/websocket (88443)	OpenSSL	TLS 1.2
Incoming	Horizon Clients over PCoIP (TCP)	OpenSSL	TLS 1.2
Bi-Directional	Horizon Clients over PCoIP (UDP)	OpenSSL	ESP (AES-128-GCM)
Outgoing	Composer	VMware JCE	TLS 1.2
Outgoing	VMware vCenter	VMware JCE	TLS 1.2
Outgoing	Oracle DB	VMware JCE	TLS 1.2
Outgoing	Authentication Server	Windows (OE service requested by TOE; service	SSPI

Direction	Endpoint Communication	Provider	Protection
		enforces protection)	
Outgoing	View Agents over TCP (32111)	VMware JCE	TLS 1.2
Outgoing	View Agents over HTTPS/websocket (22443)	OpenSSL	TLS 1.2
Outgoing	View Agents over PCoIP (TCP)	OpenSSL	TLS 1.2
Bi-Directional	View Agents over PCoIP (UDP)	OpenSSL	ESP (AES-128-GCM)

TOE Security Functional Requirements Satisfied: FCS_COP.1, FPT_ITC.1, FPT_ITI.1, FPT_ITT.1

7.5.2 View Security Server

The security server makes use of several cryptographic libraries and functions to secure messages in transit. The following ports and interfaces are cryptographically secured by the TOE:

Table 20 -Security Server Cryptography Usage

Direction	Endpoint Communication	Provider	Protection
Incoming	Horizon Clients and web browsers over HTTPS (443)	VMware JCE	TLS 1.2
Incoming	Web browsers over HTTPS/websocket (88443)	OpenSSL	TLS 1.2
Incoming	Horizon Clients over PCoIP (TCP)	OpenSSL	TLS 1.2
Bidirectional	Horizon Clients over PCoIP (UDP)	OpenSSL	ESP (AES-128-GCM)
Outgoing	Paired Connection Server over JMS (4001) [bootstrap]	VMware JCE	AES-128-CTR encryption with DSA-2048 signing
Outgoing	Paired Connection Server over JMS (4002)	VMware JCE	TLS 1.2
Outgoing	Paired Connection Server over AJP	Windows (OE protection relied upon by TOE – see A.CHANNEL_PROTECTION)	ESP (IPsec transport mode)
Outgoing	View Agents over TCP	VMware JCE	TLS 1.2

Direction	Endpoint Communication	Provider	Protection
	(32111)		
Outgoing	View Agents over HTTPS/websocket (22443)	OpenSSL	TLS 1.2
Outgoing	View Agents over PCoIP (TCP)	OpenSSL	TLS 1.2
Bi-Directional	View Agents over PCoIP (UDP)	OpenSSL	ESP (AES-128-GCM)

TOE Security Functional Requirement Satisfied: FCS_COP.1, FPT_ITC.1, FPT_ITI.1, FPT_ITT.1

7.5.3 View Composer

Composer uses Windows services for secure communications principally, but also uses OpenSSL. The following ports and interfaces are cryptographically secured by the TOE:

Table 21 - Composer Cryptography Usage

Direction	Endpoint Communication	Provider	Protection
Incoming	Connection Server	Windows (OE service requested by TOE; service enforces protection)	TLS 1.2
Outgoing	VMware vCenter	Windows (OE service requested by TOE; service enforces protection)	TLS 1.2
Outgoing	VMware ESX	OpenSSL	TLS 1.2
Outgoing	Active Directory	Windows (OE service requested by TOE; service enforces protection)	SSPI

TOE Security Functional Requirement Satisfied: FPT_ITC.1, FPT_ITI.1, FPT_ITT.1

7.5.4 View Agent

The agent makes use of several cryptographic libraries and functions to secure messages in transit. The following ports and interfaces are cryptographically secured by the TOE:

Table 22 - Agent Cryptography Usage

Direction	Endpoint Communication	Provider	Protection
Incoming	Horizon Clients, Connection Servers and Security Servers over TCP (32111)	Windows (OE functionality invoked by TOE; TSF enforces protection)	TLS 1.2
Incoming	Connection Servers, Security Servers and web browsers over HTTPS/websocket (22443)	OpenSSL	TLS 1.2
Incoming	Horizon Clients, Connection Servers and Security Servers over PCoIP (TCP)	OpenSSL	TLS 1.2
Bidirectional	Horizon Clients, Connection Servers and Security Servers over PCoIP (UDP)	OpenSSL	ESP (AES-128-GCM)
Outgoing	Connection Servers over JMS (4001) [bootstrap]	VMware JCE	AES-128-CTR encryption with DSA-2048 signing
Outgoing	Connection Servers over JMS (4002)	VMware JCE	TLS 1.2

Direction	Endpoint Communication	Provider	Protection
Outgoing	Authentication Server	Windows (OE service calling into TOE for credentials; service enforces protection)	SSPI

TOE Security Functional Requirement Satisfied: FCS_COP.1, FPT_ITC.1, FPT_ITI.1, FPT_ITT.1

7.5.5 Horizon Client

The client makes use of OpenSSL to secure messages in transit. The following ports and interfaces are cryptographically secured by the TOE:

Table 23 - Client Cryptography Usage

Direction	Endpoint Communication	Provider	Protection
Outgoing	Security Server or Connection Server over HTTPS	OpenSSL	TLS 1.2
Outgoing	View Agents over TCP (32111)	OpenSSL	TLS 1.2
Outgoing	View Agents, Security Server or Connection Server over PCoIP (TCP)	OpenSSL	TLS 1.2
Bi-Directional	View Agents, Security Server or Connection Server over PCoIP (UDP)	OpenSSL	ESP (AES-128-GCM)

TOE Security Functional Requirement Satisfied: FCS_COP.1, FPT_ITT.1

8 ACRONYMS & GLOSSARY

Table 24 – Acronyms

Acronym	Definition
BSG	Blast Secure Gateway
CC	Common Criteria
CEM	Common Evaluation Methodology
DMZ	Demilitarized zone
FIPS	Federal Information Processing Standard
OSP	Organizational Security Policy
PP	Protection Profile
PCoIP	PC over IP display protocol
PSG	PCoIP Secure Gateway
RBG	Random Bit Generator
RDP	Remote Desktop Protocol
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
SSPI	Security Support Provider Interface
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual machine
VRRP	Virtual router redundancy protocol

Table 25 – Glossary

Glossary	Definition
assignments	Delegates users to assigned machines in a desktop pool
DMZ	A physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet.
Data store	A disk resource where VMs can run
entitlements	Adding and removing desktop pools, users, and groups and deleting global entitlements and modify global entitlement attributes and policies.
group	A set of users who are assigned a common set of privileges. A group can contain other groups.
host	A computer that uses virtualization software to run virtual machines. Also called the host machine or host computer. The physical computer on which the virtualization (or other) software is installed.
PSG	PCoIP Secure Gateway forwarding packets to/from the client and the agent for the PCOIP protocol.
replica	Replica installation generates a View Connection Server instance with a View LDAP configuration that is copied from an existing instance.
standard	Standard installation Generates a View Connection Server instance with a new View LDAP configuration.
Security server	Security server installation generates a View Connection Server instance that adds an additional layer of security between the Internet and your internal network.