VMware® Horizon Workspace™ Security Features

WHITE PAPER

vmware®

Table of Contents

Introduction

Today's workers want the freedom to work from anywhere, at any time, using a variety of devices including laptops, home computers, tablets, and mobile phones. Corporate management and IT departments want to give them that freedom—if the devices can be properly secured.

VMware® Horizon Workspace™ provides the level of security and control over corporate data and applications needed to meet the stringent requirements of corporate policies and comply with industry standards and regulatory mandates. It delivers an integrated workspace that gives end users secure access to their applications, data, and desktops from any of their devices—while enabling IT to easily manage entitlement and policy controls.

For the administrator, the result is simpler, centralized, policy-based management. For end users, the benefit is the liberating experience of anytime, anywhere access to any authorized resource from virtually any device.

Simply put, VMware Horizon Workspace can transform security from a source of risk and worry into a source of strategic advantage and business empowerment. This document details the enterprise-grade security features provided by VMware Horizon Workspace and provides recommendations for taking full advantage of its security capabilities.

Horizon Workspace vApp Security

VMware deploys Horizon Workspace as a virtual appliance (vApp) within the customer datacenter. The Horizon Workspace vApp consists of five different virtual appliances: Horizon Gateway, Horizon Configurator, Horizon Connector, Horizon Service, and Horizon Data. The following are the key security considerations and recommendations for Horizon Workspace vApp security.

Virtual Machine Security Hardening

SUSE Linux is the underlying operating system for the Horizon Workspace virtual appliances, which are hardened to bare-minimum requirements. All virtual machines follow the VMware security hardening guidelines:

- Remove unnecessary software packages (RPM packages)
- Close network ports and disable `runlevel` system services
- Close network ports and disable `xinetd` services
- Review `inittab` and `boot` scripts
- Restrict system access from servers and networks
- Secure SSH
- Secure Postfix
- Secure sendmail
- Secure NFS
- Copy files using SSH without providing login prompts
- Tune security parameters available at kernel
- Enforce stronger passwords
- Restrict use of previous passwords
- Restrict direct login access for system and shared accounts
- Restrict SU access to system and shared accounts
- Prevent accidental denial of service

All components of the Horizon Workspace vApp undergo routine in-house and external security testing.

The vApp is deployed inside the customer network with an external proxy or load balancer, which forwards all requests via SSL (port 443) to the Horizon Gateway virtual appliance.

Horizon Gateway is the component that receives all Web and API traffic over SSL and proxies the request to the individual virtual machines.

We recommend that you configure the external proxy to exclude `/admin` URLs so the administrator console is not exposed to external attack.

Horizon Workspace is configured with the Horizon Configurator virtual appliance using a Web UI over SSL. Use Horizon Configurator as the component for bootstrapping the setup and configuration of the other virtual appliances (Horizon Connector, Horizon Service, Horizon Gateway, and Horizon Data).

Horizon Configurator uses `SSL REST` APIs to configure Horizon Connector.

Authentication

Use Horizon Configurator to set up Horizon Connector with Active Directory information, which authenticates and synchronizes users. The setup requires an Active Directory-based DN (distinguished name) and a non-administrative credential.

Active Directory can be configured with SSL as follows:

- **Username and Password Validation** – Perform an LDAP bind with credentials provided over SSL on the Horizon Connector login page.
- **RSA SecurID** – Use RSA APIs to validate the username and passcode against the internal RSA Access Manager. The login page is on Horizon Connector.
- **Kerberos** – Configure the connector with Active Directory Service principal credentials.

Horizon Workspace provides the ability to prompt users for stronger authentication credentials based on their location. For example, if users are on the local network, the Kerberos (desktop login) ticket can be used to provide access.[1] However, if the user is outside the network, strong authentication such as RSA SecurID is needed. This is configured by the administrator who defines which range of IP addresses authenticate with specific Horizon Connectors. The administrator sets up Horizon Connector to provide the appropriate authentication type, including username and password, Kerberos, or RSA SecurID.

Activation

Activate Horizon Workspace with an encoded activation string sent by Horizon Connector over SSL REST APIs. The activation string is sent to Horizon Service over SSL REST APIs, where it is validated against the activation code sent by Horizon Connector. On successful validation, Horizon Connector is provided an *OAuth 2.0 token.* (For more information about OAuth tokens and standards, visit the OAuth Web site.) The OAuth token is used for subsequent communication between Horizon Connector and Horizon Service over SSL.

Horizon Configurator

Horizon Configurator makes API calls over SSL to Horizon Service using the OAuth token. Horizon Configurator also updates the SSL certificate information for Horizon Gateway. Horizon Configurator calls APIs to manage the identity provider record associated with Horizon Connector. Horizon Configurator also provides an attribute map to the Horizon Service, which can be used for creating access control groups within Horizon Service.

Authentication Tokens

Two kinds of tokens are used for authentication depending on whether a user is logging in from a Web browser or Horizon Agent. The first is the *Suite token*, delivered to the user's browser after the user successfully authenticates. The other is the *OAuth* token, delivered to the Horizon Client after successful authentication.

With a Suite token session timeout, the time-to-live (TTL) is set by default to 8 hours. The administrator can change this by referring to the VMware Horizon Workspace documentation.

With OAuth token timeout and refresh where the client or device is registered as an OAuth Client, two kinds of tokens exist: *Access token* and *Refresh token*. Access tokens by nature are short-lived and Refresh tokens are long-lived. Devices registered with Horizon Service use the OAuth template to receive the Access and Refresh tokens, and the TTL for each token is part of the template. The default value for the Refresh token is one year, for the Access token, one hour. The administrator can change this by referring to the VMware Horizon Workspace documentation.

1. See the documentation for each Web browser for information on how to configure the browser to support Kerberos.

Horizon Service Data Encryption

Sensitive information such as OAuth credential secrets and signing certificates are encrypted and stored in Horizon Workspace as illustrated below.

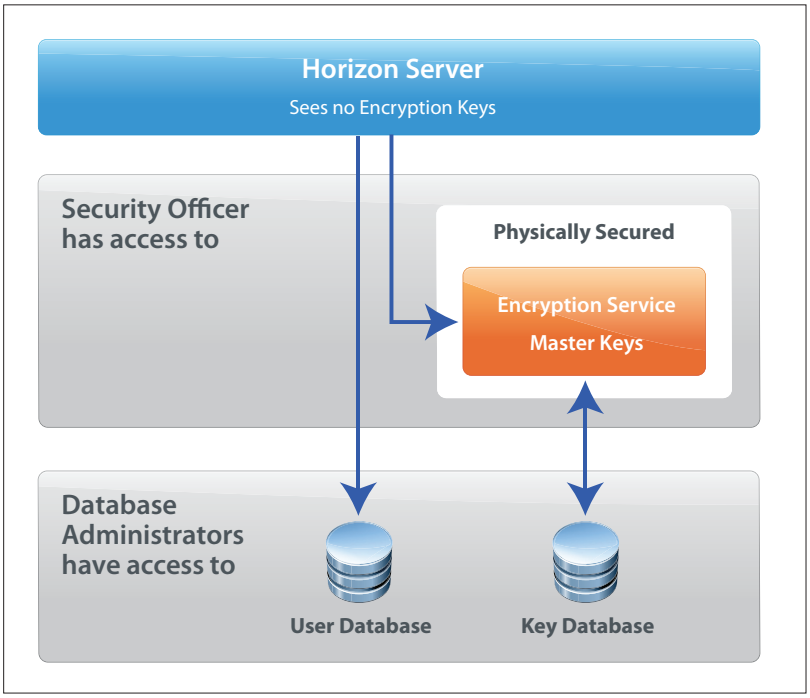

Figure 1: Security Credentials Are Stored Encrypted in Horizon Workspace

The *User Database* stores all user data. Sensitive data is encrypted in the User Database. The *Key Database* stores the keys for decrypting the data. All the keys in the Key Database are encrypted with a master key. Both these databases can be managed by a regular DBA, and can use standard backup, restore, and disaster recovery processes.

The master keys are stored on the hard drive of the servers that make up the *Encryption Service*. These servers are the only servers to read and write to the Key Database and never allow unencrypted keys to be released. All communication to the Encryption Service is through SSL, requiring both client and server certificates.

The encryption service provides UUID key identifiers to match the encrypted BLOB of data with the key needed to decrypt it. The *Encryption Service API* uses these keys to look up the encrypted keys from the database and perform an encryption or decryption operation.

The Encryption Service provides a mechanism for reliable key changes. If keys for an organization are updated, each record is converted and saved along with the new key ID, which is stored in the same transaction. Even if a failure occurs partway through a transaction, each piece of data contains a reference to the key needed to decrypt it. When the system recovers, the key conversion will be able to complete successfully.

Decrypted keys never leave the Encryption Service. Its API provides operations for encrypting, decrypting, and versioning keys, but never provides access to the key material. This way, an attacker who has gained root access on a Horizon Workspace server can never have enough information to perform an offline attack on the database itself.

Horizon Data Sharing and Security

Horizon Data gives IT administrators single-dashboard control, allowing internal users to access and synchronize data while limiting external users to the data in folders that the internal users designate.

File Sharing Using Public Links

Horizon Data allows users to share their documents as public links. Anyone with access to the public link has access to the content. The URLs are randomly generated long strings that are protected from brute-force attacks. The content accessed using shared links is securely transferred over SSL. This public sharing can be enabled or disabled by administrators at Account or Class of Service (COS) levels. Sharing expiration can also be set up by administrators at Account or COS levels.

Internal Folder Sharing

Folders can be shared among provisioned users (internal) using read, read/write or read/write/share permissions. Administrators can set up expiration policies for internal shares.

External Sharing

Content can be shared with company employees who are not provisioned for data, as well as with external collaborators who are not part of the company. This is referred to as *external sharing*. Upon sharing, external users receive an invitation email with a self-provisioning login link. The username is the email ID of the external user. External users self-select a password, which is stored in a local LDAP bundled with the Horizon Data virtual appliance. Upon login, external users have access only to the folders shared with them and can manipulate the data only within those contexts. External users have access only via a Web client.

External users cannot be administrators of the folder; only read and read/write permissions can be granted to them. To recover a forgotten password, the external user receives an email similar to the initial share invitation with a URL for the login page. The URL is time-sensitive and will expire if the password is not reset within the set period. Administrators can turn external sharing off at the Account or COS level. Administrators can configure selective domains for blacklisting or white-listing of access. Administrators can also set the expiration policy for the shares to be automatically revoked upon the end of such a period. These settings are made at the Account or COS level.

Horizon Workspace iOS Client Security

When users access data through their own devices running iOS, the data is encrypted and all communications are through SSL.

Access and Authentication

Horizon Workspace authenticates entitled end users with a standards-based OAuth 2.0 protocol and their AD credentials or RSA SecurID. Administrators can set up the session timeouts and other authentication token–related configurations from the Horizon Workspace administrator console.

Transit Data Security

All communications to the Horizon Workspace server are secured by using SSL.

Content Security

The only content stored persistently in the Horizon Workspace iOS native application are files marked *Favorite* and cached for offline access. The files selected for preview or *Open With* are also temporarily stored on the disk. The next section provides details on encryption to secure content stored on the device at any time.

Encryption

The encryption algorithm is AES 256 with a key length of 32 bytes.

Setting Up the Encryption

The first time the application is installed and loaded, it checks for an encryption flag. If the flag indicates that *no key* has been generated then any cached files are removed. A random key is generated using the built-in Cocoa libraries and immediately put in the keychain. The random generator guarantees that practically no two users will ever have the same key. The application is now set with an empty cache and a unique, strong encryption key that is stored securely in the keychain.

Files Marked Favorite

When a *Favorite* file is cached for offline usage, it is encrypted instantly after download.

File Previews and Encryption Flow

For preview, downloaded files must be presented in their unencrypted state to be displayed by the iOS previewer. Before the preview, the file is briefly in the unencrypted stage. Upon successful preview loading, it is immediately encrypted and written back to disk. A flag will track and indicate any unencrypted files. If this flag is found, the application immediately removes any unencrypted files, which must be downloaded again.

Using the "Open With" Menu

Similar to the above process, the file must be briefly decrypted for a third-party program to load. As soon as the user selects a program to open the file, it is decrypted and a flag is set to capture this state. If the program successfully loads the file, it is encrypted once again and the flag is removed. If the third-party program cannot successfully report loading the file, then the Horizon Workspace application will check the flag, find the files in decrypted state and immediately remove them, thereby requiring a fresh download.

Policies

The following considerations and recommendations are offered to administrators to help optimize the use of Horizon Workspace for iOS device security.

Application Passcode Policy

To protect against data theft from lost or stolen devices, administrators can require end users to set an *application passcode*. The application passcode must be a minimum of four characters and both numbers and letters are allowed. After a user sets a passcode, he or she has the option to select the inactivity period. Whenever the inactivity period is exceeded the application locks itself and prompts the user to enter the passcode. Whether an application is in the background, the user is inactive within the application, or the application has been restarted, this passcode enforcement can effectively prevent data theft in the event of device loss.

"Open With" Control

In order to protect the data from leaving the Horizon Workspace application, administrators can disallow the *Open With* option. This will effectively prevent Horizon Workspace data from leaking to unsanctioned applications.

Remote Wipe

Administrators and end users can remotely wipe the Horizon Workspace application and all its content. Note that this will not wipe the device, only the content in the Horizon Workspace application. When the application connects to the server, it receives the remote wipe command and removes all the content. The end user will have to enter server information and valid credentials to re-link to the Horizon Workspace server.

Protection Against Jailbreak

If the device is rooted, the keys in the keychain are compromised, creating a potential threat. To protect against jailbreak, do not root the device.

Horizon Android Client Security

When users access data through their own Android devices, the data is encrypted and all communications are through SSL.

Access and Authentication

Entitled end users are authenticated using OAuth 2.0 based on their AD credentials. The session timeouts and other authentication token–related configurations can be set up from the Horizon Workspace administrator console.

Transit Data Security

All communications to the Horizon Workspace server are secured by using SSL.

Content Security

The Android platform supports storing secure and insecure files. Android refers to secure file storage as *internal storage*. It is limited to small files and key-value pairs, and is not appropriate for storing large files. Insecure storage is referred to as *external storage*. It is implemented on removable flash storage (SD cards), or internal flash storage on modern devices. Insecure storage may be used to store large amounts of data. All data in insecure storage on an Android device is readable by any application. It is accessible from a desktop computer by mounting the device as USB mass storage, or via MTP on modern devices that support it. Android guidelines insist that you not store sensitive data in insecure storage.

The Horizon Workspace Android native application stores files marked *Favorite* for offline access, transient cached content for previews, and metadata related to files and folders. All content stored in the application is always encrypted. The next section provides details on encryption to secure content stored on the device at any time.

Encryption

The encryption algorithm is AES 256 with a key length of 32 bytes.

Setting up the Encryption
When the application is initially installed and loaded, it generates a random key using the standard library included in the Android SDK. The key is immediately put in secure storage. The random generator assures that no two users will ever have the same key.

Files Marked Favorite
Files that are marked *Favorite* are cached on the device for offline access. These files are encrypted and written to the disk as they are read from the server. The content is always in an encrypted state.

File Previews and Encryption Flow
For Android file preview, the data server converts files to images. The preview does not require downloading original files. All image files are cached to disk in an encrypted state.

Using the "Open With" Menu
To support *Open With* functionality, Android holds data in insecure storage, unencrypted, for a very brief period of time. Upon a successful read from another application, the unencrypted content is immediately deleted.

In Android, applications access external content based on URIs (uniform resource identifiers). For example, when a user opens a Horizon Workspace document in an external application, Horizon Workspace decrypts the file and provides a URI to access the content. In order to protect against URI caching, Horizon Workspace expires the URIs after a short time window. This prevents applications from caching and reusing the URI to the content.

Policies

The following considerations and recommendations are offered to administrators to help optimize the use of Horizon Workspace for Android device security.

Application Passcode

To protect against data theft from lost or stolen devices, administrators can require end users to set an *application passcode*. The passcode must be numeric with a minimum of four digits.

After a user sets a passcode, he or she has the option to select the inactivity period. Whenever the inactivity period is exceeded, the application locks itself and prompts the user to enter the passcode. Whether an application is in the background, the user is inactive within the application, or the application has been restarted, this passcode enforcement can effectively prevent data theft in the event of device loss.

"Open With" Control

In order to protect data from leaving the Horizon Workspace application, administrators can disallow the *Open With* option. This will effectively prevent Horizon Workspace data from leaking to unsanctioned applications.

Remote Wipe

Administrators and end users can remotely wipe the Horizon Workspace application and all its content. Note that this will not wipe the device, only the content in the Horizon Workspace application. When the application connects to the server, it receives the *Remote Wipe* command and removes all the content. The end user will have to enter their server information and valid credentials to re-link to the Horizon Workspace server.

Protection Against Jailbreak

If the device is rooted, the keys stored in its secure memory can be compromised, creating a potential threat. To protect against jailbreak do not root the device.

Horizon Client Security on Windows and Macintosh

Encrypted desktops are required if users access their data through their own laptop running Windows or the Mac OS.

Access and Authentication

Entitled end users are authenticated using OAuth2.0 based on their AD credentials. The session timeouts and other authentication token–related configurations can be set up from the Horizon Workspace administrator console.

Transit Data Security

All communications to the Horizon Workspace server are secured by using SSL.

Content Security

Currently the Horizon folder in Mac OS or Windows is just like any other folder on the end user's system. If a customer requires an endpoint laptop to be encrypted, then they must perform disk encryption. This ensures that the Horizon Workspace content is encrypted as well.

Encryption

Enterprises can use third-party software to encrypt the disks.

Policies

The following considerations and recommendations are offered to administrators to help optimize the use of Horizon Workspace for Windows and Macintosh device security.

Remote Wipe
Administrators and end users can remotely unlink and remove the Horizon Workspace content from the device.

Protection Against Device Theft
Enterprise laptops are commonly required to be password-protected. In the event of theft, VMware relies on password protection at the OS level.

About the Authors

Vijay Pawar, Product Line Manager, Horizon Product Management at VMware, and Arvind Soni, Senior Product Manager, Horizon Product Management at VMware, wrote this document.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com