HITACHI
Inspire the Next

WHITE PAPER

Hitachi Content Platform Anywhere Security

By Hitachi Vantara

June 2019

Contents

Executive Summary

In the world of cloud and data mobility, there is an expectation that information can be accessed anytime, anywhere and from any device. While this expectancy was originally driven in the form of public cloud services, enterprise users quickly took advantage of these services as corporate IT struggled to keep up.

This user-driven move to store corporate assets in the public cloud was not without risk. Corporate information began to leak into public clouds outside of the traditional enterprise security perimeter and was stored in places that lacked an appropriate level of enforceable security and compliance.

Today's enterprises have no doubt about the advantages of mobility for business advantage and agility. Hitachi Vantara supports this capability by enabling enterprises to allow their users to securely access data anytime, anyplace and from any device through Hitachi Content Platform Anywhere (HCP Anywhere). This white paper describes the security aspects of HCP Anywhere.

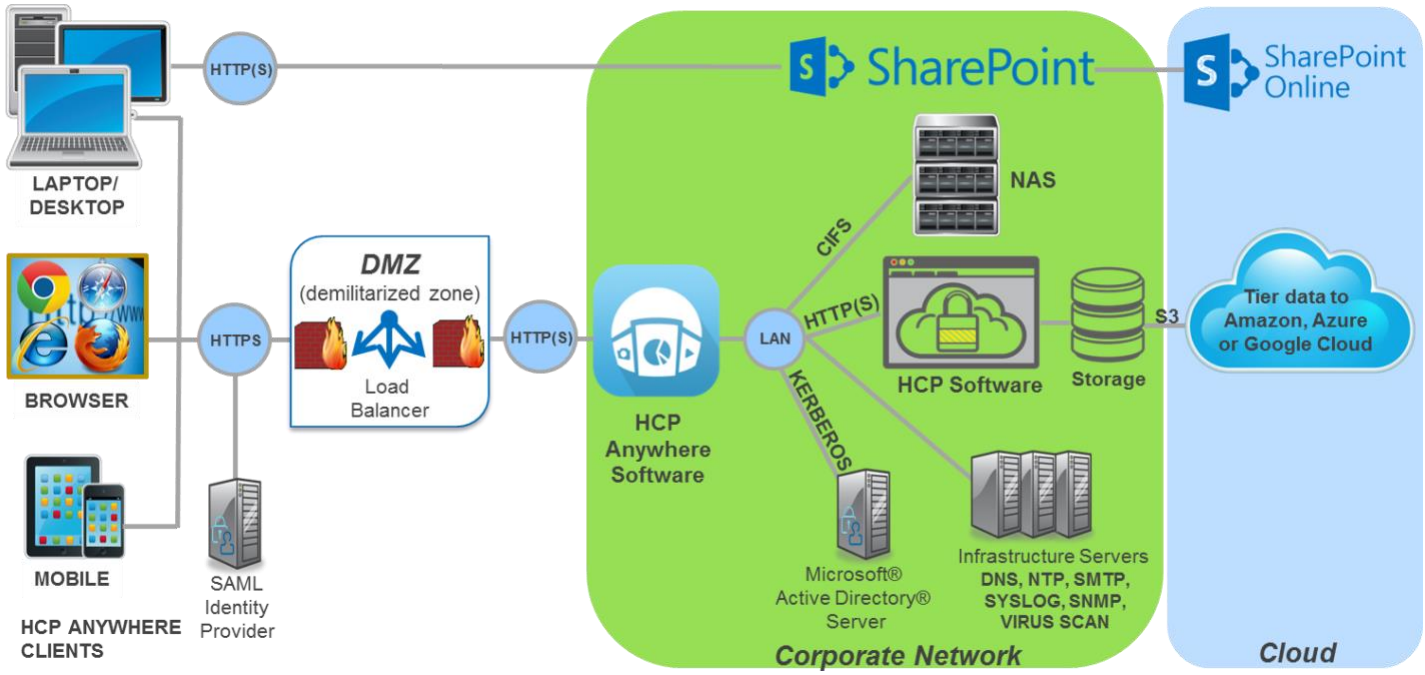
Introduction

Hitachi Content Platform Anywhere (HCP Anywhere) provides an enterprise mobility platform, including file-sync-and-share (FSS) capabilities, end-point data protection (EDP), and enterprise data mobilization (EDM). The primary goal is to provide the ease of use and simplicity of a consumer-class product with enterprise-class security and functionality that organizations can host securely on-premises. At the core of HCP Anywhere is the Hitachi Content Platform (HCP) object store, which provides the security foundation of this offering.

A fundamental design goal for HCP Anywhere is to be “simply secure.” This means that HCP Anywhere is designed with security as core tenet of its development (see Figure 1). HCP Anywhere allows ease of user experience and the enforcement of organizational security policies simultaneously.

This document describes the security aspects of the HCP Anywhere product related to secure access to the system, secure access to data, and protection from threats as well as data corruption.

Figure 1. HCP Anywhere Architecture



HCP = Hitachi Content Platform, SAML = Security Assertions Markup Language, CIFS = Common Internet File System, DNS = domain name system, NTP = network time protocol, SMTP = simple mail transfer protocol, SYSLOG = system log, SNMP = simple network management protocol, Azure = Microsoft Azure, SharePoint = Microsoft SharePoint, S3 = Amazon Simple Storage Service

User Access and Security

Hitachi Content Platform Anywhere controls user access by leveraging existing authentication and authorization infrastructure in the customer environment.

End-User and Administrative Authentication

In HCP Anywhere, administrators and end users are authenticated against Microsoft Active Directory (AD) via the Kerberos protocol. HCP Anywhere maintains lists of authorized AD groups that are permitted to access the system. Each user that requires access must be a member of at least one authorized AD group.

Also, HCP Anywhere supports SAML 2.0 protocol to authenticate users via identity providers (IdP) including Active Directory Federation Services (AD FS). This allows HCP Anywhere to authenticate users located in multiple AD forests.

User management and access on HCP Anywhere is done via profiles. Each profile contains a list of policy settings and a list of authentication units (Active Directory groups or SAML IdP) with which those settings are associated.

When logging into the web portal or management console (via browser), the user's credentials are authenticated against AD or SAML IdP credentials.

On Microsoft Windows, Apple Mac OS, Google Android and Apple iOS, the user can authenticate using their AD or SAML IdP credentials. The access token received back by the HCP Anywhere client application is used to connect to the HCP Anywhere system. By default, the access token is valid for a specific period, after which the user is prompted to re-authenticate. HCP Anywhere allows the administrator to configure the lifetime of the access token. The clients do not store user credentials.

In addition, on Android and iOS devices HCP Anywhere can enforce lock code usage. The administrator controls the policy for whether a lock code is required, as well as the lock code length and type.

Clear Credentials

At any time, an administrator can issue the clear credentials command against any user devices. Once issued, regardless of single sign-on configuration or security token validity, the user will be prompted for login credentials the next time that the HCP Anywhere client attempts any communication with the HCP Anywhere system.

Active Directory Status Change

The user's status must remain active within AD in order to authenticate. A user will lose the ability to authenticate and access HCP Anywhere if his or her user account is:

- Removed from all AD groups that are registered with HCP Anywhere.
- Expired in AD.
- Deleted from AD.
- Locked or disabled in AD.

In all these cases, the user will lose access to HCP Anywhere from mobile clients and browsers. Users will still be able to access data saved locally on their laptop or desktop, but that content will no longer be synchronized with the HCP Anywhere system. Administrators can take additional action to **remotely wipe** the HCP Anywhere data from any and all user devices.

Disable User

At any time, an administrator can choose to disable a user in HCP Anywhere from the management console. At that point, all user clients, including web portal, will no longer be able to access the HCP Anywhere system and synchronize data. The user will still be able to access the data saved locally on their laptop or desktop and mobile

clients, but any changes made will not be sent to the HCP Anywhere system for synchronization. Once a user is re-enabled, all normal operations resume and any changes made while the user was disabled will synchronize.

Delete User

At any time, an administrator can choose to delete a user in HCP Anywhere. All user's data will be deleted from the HCP Anywhere system, all shared links will become invalid, and the user's shared folders will be unshared and deleted. Additionally, all user's devices will be deregistered, and by default all HCP Anywhere data will be wiped.

This does **not** prevent the user from accessing HCP Anywhere. In fact, a user who accesses the web portal will be prompted to register, as if they are a new user. Preventing a user from accessing HCP Anywhere is done via AD or IdP, or by removing the AD group or IdP from the profile.

Support for Smart Card or Certificate-Based Authentication

In release 4.1, HCP Anywhere introduced certificate-based authentication to support access from HCP Anywhere devices and management console. Certificate-based authentication uses the digital certificate stored on a smart card or installed on the device itself to identify a user rather than asking for username and password. The certificate-based authentication can be configured via **Access -> Authentication -> Active Directory -> Active Configuration -> Authentication Configuration** located in the HCP Anywhere management console. This allows the admin to:

- Enable certificate-based authentication.
- Enable and disable username/password authentication.
- Configure other related settings.

Administrator Controls

Hitachi Content Platform Anywhere provides a variety of controls to enforce security no matter how end users want to access their data.

Device Access

Each user is permitted to register up to a specified number of devices (desktop and mobile) with HCP Anywhere. The HCP Anywhere administrator can configure the number and type of devices allowed for each user or profile.

Deregister Device and Data Wipe

At any time, the user or an administrator may deregister any registered device. On the next connection with the HCP Anywhere system, the deregistered device will note its state change and no longer synchronize. All HCP Anywhere data on the client is automatically deleted (by default) when it is deregistered. Additionally, administrator-configurable system settings allow deregistration of inactive devices after a certain number of days.

Browser Access Timeouts

Administrators can set a configurable inactivity timeout period for authenticated access to the web portal and management console. After timeout, the user is auto-logged out of the browser session.

Maintenance Access

Should a circumstance arise such that Hitachi Vantara support personnel need to access the HCP Anywhere system, measures are in place to ensure that access is secure. Support can only access the system via SSH. On connecting to SSH, public key authentication logon is required. The support person will use the private key and password known only to Hitachi Vantara support. New key pairs are generated with each release of HCP Anywhere. The HCP Anywhere administrator can enable or disable this access from HCP Anywhere management console.

Restrict Clients To Run on Corporate Approved Devices

By default, users can download HCP Anywhere desktop applications from the My Devices page in the web portal. The HCP Anywhere administrator has a choice to disable the download of clients from the web portal and instead use their corporate approved distribution platform. This also allows the administrator to specify the registration information for the clients being distributed, thus facilitating installation and registration process for the users. Additionally, the administrator can configure how many devices and which type of devices any end user can have, thus creating a policy inline with corporate best practices.

Enterprise Mobility Management Integration

For mobile devices HCP Anywhere integrates with mobile device management (MDM) or enterprise mobility management (EMM) software like MobileIron and Blackberry Good Technology, which can secure the mobile app life cycle while preserving corporate policies.

Content Exclusion Policy

An administrator can define a policy to exclude (blacklist) certain file types (MP3, EXE and so forth) from being uploaded into HCP Anywhere for security and compliance to corporate policy. Once the policy is set, users will receive an error message during an attempt to upload a blacklisted file type. The blacklisting is configured via user profiles, allowing the administrator to define different blacklist policies for different groups.

Data Security Controls

Data-in-Flight Encryption

Data flows from the HCP Anywhere clients via the HCP Anywhere system to the Hitachi Content Platform object store for storage. No copies of the data remain on HCP Anywhere system.

As data moves between the client and the HCP Anywhere system, all network communication occurs over HTTPS with TLS (transport layer security) to prevent eavesdropping or tampering. Data in transit is always encrypted. The administrator can determine how this encrypted network traffic is terminated.

There are three options for implementing data-in-flight encryption on HCP Anywhere:

- The TLS protocol session can take place from the client all the way to the HCP Anywhere system.
- The TLS protocol session can take place from the client to the organization's load balancer or firewall, terminate there, then transition to an unencrypted socket connection to the HCP Anywhere system.
- The TLS protocol session can take place from the client to the organization's load balancer or firewall, terminate there, then transition to a new TLS session (with a new key) from the load balancer to the HCP Anywhere system.

In addition, administrators can configure the communication between HCP Anywhere system and HCP object storage to use HTTPS with TLS, for security.

Certificate Management

HCP Anywhere system allows organizations the choice of using self-signed or trusted third-party certificates. HCP Anywhere can generate a certificate signing request if required or certificates can be uploaded in PKCS12 format. Optionally, self-signed certificates can also be generated. The mobile and desktop connections will leverage these certificates for secure transmission of data to and from HCP Anywhere.

Data-at-Rest Encryption

- HCP Anywhere application's storage device, the HCP system, can be configured to encrypt all data at rest within it. Data at rest is encrypted using 256-bit AES.
- All HCP Anywhere data on iOS clients is natively encrypted on disk without option by iOS itself. Please refer to "iOS Security" published by Apple Inc.
- HCP Anywhere currently does not perform data-at-rest encryption on the other client devices. HCP Anywhere clients are compatible to operate with corporate deployed disk encryption software technologies.

Data Protection

Versioning

To protect users from accidental file or folder deletion, or unwanted file content changes, HCP Anywhere has a versioning capability. There are two versioning policies: latest versioning and extended versioning.

The HCP Anywhere administrator can set limits on the versioning policy. They can set both the length of time that any historical version remains accessible in the system, and the number of historical versions that remain accessible in the system. These parameters operate independently.

The administrator can configure extended versioning policy, designated as: daily, weekly and monthly. The administrator can also configure and enable Microsoft Volume Snapshot Service or Volume Shadow Copy Service (VSS) capability for data protection of locked files (like PST) on Windows-based systems. The administrator can specify a frequency (in hours) to sync and save these locked files to the HCP Anywhere system.

Versioning provides data protection from viruses and ransomware, as well as accidental deletes, by allowing the user to recover the previous version of the file(s).

Self-Service Restore

Self-service restore allows users to restore selected file(s), folder(s) or all their data at a particular point in time. The user can select a restore point (now, daily, weekly, monthly), to restore data to due to corruption, virus or ransomware, and so forth.

Also, for any folder, a user can view a list of deleted items and choose to restore any of them.

For any file, a user can view the previous versions of the file including the ability to view the historical file's contents. The user can select any prior version of a file and restore it to become the current version.

For disk failure or lost laptop or desktop, the user can just re-install the HCP Anywhere desktop client to restore a local copy of their data from HCP Anywhere system.

Endpoint Protection (Backup)

Endpoint protection allows users to select folders on their laptop or desktop that they want backed up to HCP Anywhere system. The backup is continuous and happens as files are modified or added. Backup is different from file sync and share because it only syncs data one way to the HCP Anywhere system and NOT across devices. Blacklisting policy can be set by the administrator to prevent certain file types from being saved to the HCP Anywhere system.

Auditing

Audit Logging

HCP Anywhere provides detail auditing of the data and actions for each user in the HCP Anywhere system. An administrator who has been assigned the role of "auditor" can do an audit against any user. The auditor can review:

- All user files and folders, including the file contents.
- All user authentication attempts.
- When and which files have been shared by a link and whether they were shared privately or publically.
- Any shared link access attempts. For private links, the user attempting access is captured in the log.
- All file and folder activity, create, update, delete, rename and so forth. This information is available for all the data in a user's private HCP Anywhere folder, folders that the HCP Anywhere user has shared with others, and shared folders owned by others to which the HCP Anywhere user is a member.

Audit Reports

A user with auditor role can use reporting APIs to generate the following audit reports:

- **File events made by a specific user** in root folder, all shared folders that the user has ever been a member of, all team folders that the user has ever been a member of, all folders ever owned by the user, all currently mounted mobilized shares.
- **Events on files owned by a specific user,** including events made by *other* users in a shared folder owned by the user.
- **Events on specific path owned by a specific user,** including events made by all users to the path (if the path is or was in a shared or team folder).

- **All nonfile share activity for a specific user** corresponds to what appears on the web portal page Activity -> Collaboration Activity -> Shares.
- **All nonfile link activity for a specific user** corresponds to what appears on the web portal page Activity -> Collaboration Activity -> My Links.
- **All nonfile account activity for a specific user** corresponds to what appears on the web portal page Activity -> Account Activity.

Data Sharing

Shared and Team Folders

A user can share HCP Anywhere folders with other registered HCP Anywhere users in the system. A shared folder includes all files and subfolders, currently, with no exclusions of files for subfolders. If enabled by the administrator, a user can create a team folder by converting an existing shared folder or creating a new team folder.

- The owner or manager of a shared or team folder can control the level of access each user has to the folder contents. Permission levels are "viewer" and "collaborator". A user with **collaborator** permissions can perform all CRUD (create, read, update and delete) operations on the folder contents. A user with **viewer** permissions is limited to read-only.
- Users participating in the shared or team folder can view a list of other participants.
- Users participating in the shared or team folder can view a detailed activity log for themselves and other users.
- At any time, a member of a shared folder may choose to leave the shared or team folder. After leaving a folder, the user will no longer have access to the content and the data will be wiped from all users' devices.
- At any time, the owner or manager of a shared or team folder may remove a user from the shared folder. Again, this action will automatically wipe the folder data from all the user's devices.

Link Sharing

Additionally, link sharing can be used for sharing data with other users. A user can create links to any files or folders within HCP Anywhere. Shared links have the following properties:

- **Internal link**: The receiver of an internal link must be a registered user and is prompted to provide login credentials that are validated before the link will be resolved.
- **Public link**: If the user chooses the "public" link option, then any receiver of the link will be able to download a copy of the file. Note, HCP Anywhere administrators can choose by policy to disallow public link sharing.
- **Expiration date**: The user can specify the number of days that the link will be active. After the specified number of days, the link will expire and will no longer be valid.
- **Access code:** Users have the option to set an access code on a link; the access code is system generated.
- **Manage link**: The user can manage existing active links and choose to delete, extend the expiration, or add an access code.
- HCP Anywhere administrators can define the policy for link-sharing usage. The policy enforces:
  - Choice to allow link sharing of any type (internal or public).

- Choice to allow internal link sharing only and disallow public link sharing.
- Maximum period that any link can be active for in HCP Anywhere.
- Default period that a link is active for in HCP Anywhere.

External User Data Upload

An administrator can enable secure file transfer by external users via HCP Anywhere. If enabled, a user can create a link to a folder that allows external users to upload files into that folder. All activity is recorded for auditing and security purposes. In addition to the shared links properties described above, folder links have the following additional property:

- **Folder Permissions**: read only, upload only, both read and upload

Hitachi Content Platform Object Store Security

HCP Anywhere stores its data onto the HCP object store and takes advantage of its legacy of offering enterprise-class security. The application leverages the multitenancy capabilities of HCP such that all HCP Anywhere data is isolated to its own private tenant. Within the HCP Anywhere tenant inside HCP, the application creates additional private namespaces to securely store the user files and backup copies of the HCP Anywhere database. These namespaces can only be accessed by the HCP Anywhere system.

A properly configured HCP has many additional features to safeguard that integrity of the data. These features, taken in aggregate, ensure that the system does not require backup.

Availability

HCP tracks each object in a database distributed across all HCP nodes (minimum of four) with each node containing a shard of the database and a different shard owned by another node. The shards and shard copies are stored on separate groups of disks to ensure that failure of a whole disk group will not cause the loss of both the primary and copy of any particular shard. If a single shard is lost, it can quickly be regenerated from its copy. With this design, HCP is protected from losing its ability to find objects on the system. This design is referred to as metadata protection level 2 (MDPL2).

Data Integrity

HCP scans all objects on a regular basis for integrity. It captures and stores separate hashes for the file and custom metadata that make up the object. If during a scan, an object is found to no longer match its hash, it is automatically repaired from either local or remote object replicas.

Replication

HCP supports asynchronous replication for disaster recovery and site failover. Also, any lost or damaged object is automatically repaired from a replica object.

Encryption

HCP system can be configured to encrypt all data at rest using 256-bit AES.

HCP Anywhere Deployment

HCP Anywhere enables secure deployment within a company's IT environment with the following elements:

HCP Anywhere Networking

HCP Anywhere has two separate networks.

- **Corporate Network**:
  - Communicate with HCP Anywhere clients. This traffic comes over the internet and/or is routed over internal networks and should be configured through the company load balancer or firewall infrastructure. HCP Anywhere supports multiple options for SSL termination.
  - Communicate with corporate infrastructure behind the firewall, with, for example AD, DNS, NTP server, Virus Scanning Engine, NAS System, and HCP storage. For security purposes, corporate infrastructure should be segregated from HCP Anywhere.
- **Private Network:** This network is only used for HCP Anywhere internode communication and troubleshooting.

HCP Anywhere Node Hardening

- If a user is logged into the management console or the web portal and clicks on logout, all browser sessions will be terminated.
- HCP Anywhere software makes no direct SQL calls. All database functionality is passed through stored procedures to prevent SQL injection attacks.
- HCP Anywhere is validated against an industry-standard vulnerability scanner to identify and resolve common security issues such as:
  - Weak SSL ciphers.
  - Form injection attacks.
  - Cross-Site Scripting (XSS) attacks.
  - Cross-Site Request Forgery (CSRF) attacks.
- Product code upgrades are online, fast and customer executable. This enables rapid reaction to any newly discovered security threat.
- Monitoring of system access attempts via both the web portal and management console so that a user or administrator can spot suspicious activity.
- External security assessment and audit completed on a periodic basis.

Virus Scanning

The HCP Anywhere system can be configured to communicate to a corporate virus scanning engine (Symantec, McAfee and Trend Micro). When an HCP Anywhere user adds or changes a file on their client, the file is sent to the HCP Anywhere system. Before storing that file and making it available to all the other devices for that user, the HCP Anywhere system forwards the file to the virus scanner using the ICAP (IETF.ORG RFC 3507) protocol. If the virus

scanner deems that the file is infected and requires to be quarantined, then the file will not be saved by the HCP Anywhere system. On the user client where the file was added, an HCP Anywhere error status will be raised, identifying the file as containing a virus.

Port Documentation

Organizations are provided with complete documentation of all required and optional network accesses to or from the HCP Anywhere system so that the network administrator can perform port lock down in accordance with company policy.

Conclusion

In summary, HCP Anywhere allows an organization to select the appropriate level of security that is required for its environment. The comprehensive list of HCP Anywhere security features includes:

- AD and SAML authentication of users.
- Restrict access to specified device types, deregister devices and remote wipe select data.
- EMM and MDM integration.
- Data encryption.
- Virus and ransomware protection.
- Full data recovery.
- Full audit logging.
- Secure sharing and collaboration.
- Security and penetration testing.

Security is a core tenet of HCP and the HCP Anywhere system. Hitachi Vantara is committed to continue expanding the security capabilities of HCP Anywhere in future versions of the product while maintaining a positive user experience for end users and administrators alike. HCP Anywhere enables users to be more productive and teams to collaborate effectively, while maintaining high security and compliance certification standards.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
www.HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact

WP-590-A BTD June 2019