HITACHI
Inspire the Next

Modernize file services by replacing traditional file servers with cloud storage gateways and object storage. Simplify management, reduce cost and improve data access without changing user or application behavior.

DATASHEET

Hitachi Content Platform Gateway for Object-Based File Services

Organizations struggle with the cost and complexity of file services in the data center, at remote and branch offices, and on user devices. This results in over- or under-provisioning of storage resources, long backup times, compliance issues and escalating costs. While attractive at first, public cloud-based solutions pose potential cost and compliance issues. Hitachi Content Platform Gateway (HCP Gateway) lets you retain visibility and control over data while simplifying and controlling the cost of file services. All data from remote and branch offices flows to the data center, where it can be tracked, managed and governed properly, even if part of that life cycle means sending a copy to public clouds. By automatically synching files to the data center, HCP Gateway offers more reliable data protection than traditional backup technologies at sites where IT staff and skills are limited, such as remote and branch offices.

File-based data accounts for more than 80% of capacity demand in a typical IT infrastructure. Traditional infrastructure requires the labor-intensive management of file servers, NAS and data protection appliances, and software. These efforts support activities like data protection and recovery, performance management, migrations and capacity planning, making traditional file services very costly to maintain. A modern, cloud-based approach to file services is much more efficient and easier to manage. HCP Gateway gives you a private or hybrid cloud solution to address the shortcomings of traditional NAS and file server deployments. This solution enables users and applications to read and write data as they always have and copies all files to Hitachi Content Platform (HCP), where they are efficiently stored, well protected and properly governed (see Figure 1).

HCP Gateway presents the traditional CIFS share or NFS protocols to users and applications using virtual file systems (see Table 1). The virtual file systems are not integrated with the host operating system; hence, things like stubs, links, DFS or junction points are not used, and, therefore, operating system limitations (for example, file count or size of file system) are not imposed. Users and applications will continue to view the file system directory structure to which they are accustomed, but now the content can be stored where appropriate for the business. This means that with HCP Gateway handling the translation, the front-end access protocol can be different from the back-end storage protocol, without any updates to client or application access.

Compliance, Governance and Data Protection

HCP Gateway enables you to meet compliance requirements for “write once, read many” (WORM), retention, legal hold and data disposition. It also helps you deliver a more secure, flexible and efficient approach to long-term archiving needs using HCP object storage.

HCP is one of the most trusted data storage compliance and data governance offerings in the market, with over 2,500 customers and 5,000 systems in operation. It is the core of a broad DataOps for governance solution that not only achieves compliance, but also goes far beyond by helping to protect data, share information, simplify management and reduce costs. Some key attributes of HCP include:

- **Retention.** WORM functionality is employed to set a specific file retention period. The retention period can be extended but not shortened. Retention can be set on an object-by-object basis or by selecting related retention policies. Once the retention period has been met, files can be deleted from the system.
- **Data destruction.** Files can be deleted upon expiration of the retention period, but cannot be deleted when a retention policy is in effect. HCP incorporates a “digital shredding” feature that overwrites deleted files with a random pattern, a technique that complies with the United States Department of Defense (DOD) specification 5520.22-M. These actions can be performed on individual objects, or a policy can be assigned to automatically govern the deletion of content. All delete actions are logged, and the logs can be extracted with the auditing mechanisms in HCP.
- **Authenticity.** A digital signature for each incoming file is created using any one of the following hashing algorithms to ensure data integrity: MD5, SHA-1, SHA-256, SHA-384 or SHA-512. The system periodically computes the digital signature and compares it with the original value stored when the file was first archived, ensuring data integrity.
- **Encryption.** All data is automatically encrypted using the NSA-approved AES encryption algorithm before being written to disk. On reads, the data is decrypted and presented back to the requestor in its original format. The encryption and decryption operations are transparent to users and applications. The encryption key is generated at system installation time and stored internally, eliminating

the need for external key management schemes. The encryption key is broken into a number of pieces and distributed among the nodes in the system, ensuring that if a disk or a node were stolen, the data would be unreadable.

- **Access controls and auditing.** Administrative access can be restricted to individual IP addresses or a range of allowable addresses. Each access gateway has its own security mechanisms. In addition, all ports not needed for the interfaces are protected by an embedded firewall. The HCP logs significant events, such as object deletion, so that these actions can be audited.
- **Data protection.** By combining versioning of data with WORM functionality, content integrity checks, data authenticity, replication, erasure coding and a host of other technologies, Hitachi Content Platform eliminates the need for traditional tape-based backups, greatly reducing the cost and complexity of file services.
- **Discovery.** Hitachi Content Intelligence provides full content and metadata search and indexing that enables rapid location of documents related to keywords, file properties and custom metadata. Content Intelligence can also be used to create pipelines and workflows that automatically identify, classify and assign data management policies to files based on their metadata and content to ensure proper governance of your data.

These capabilities and much, much more make HCP with the HCP Gateway a more elegant and future-ready solution for providing file services in your organization.

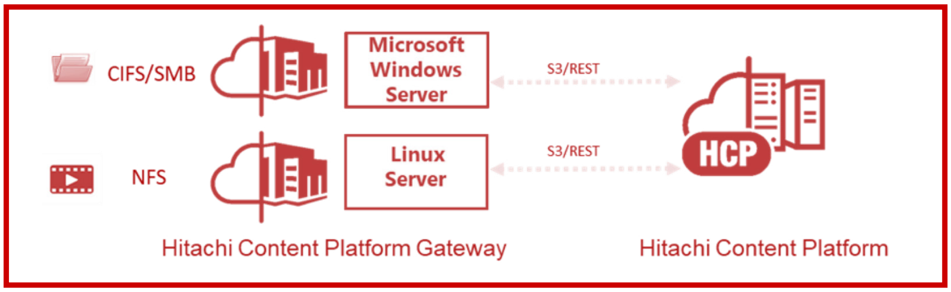

Figure 1. HCP Gateway lets you meet compliance requirements by using HCP object storage data governance capabilities.

TABLE 1. HCP GATEWAY SPECIFICATIONS

	Bold Subtitle
Supported Operating Systems	• NFS only – Linux, Debian Server 10.x • CIFS only – Microsoft Windows Server 2016
Supported Virtual Machine Hosts	• VMware ESXI • Microsoft Hyper-V • KVM

Transforming from traditional to modern file services has many benefits and is not as complicated as you might think. See why: Watch a lightboard overview of the Hitachi Content Platform portfolio.

We Are Hitachi Vantara

DataOps is the data practice for the AI era, connecting data consumers with data creators to accelerate collaboration and digital innovation. We are analytics, industrial expertise, technology and outcomes rolled into one great solution partner. Get Your DataOps Advantage.

Hitachi Vantara

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

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

DS-522-A BTD December 2019