# Cloud FastPath: Highly Secure Data Transfer

Tervela has been a leader in high performance data transfer technology for over a decade. Tervela's customers include Fortune 100 companies in the financial services, healthcare and media industries and hundreds of small and medium sized businesses. All of Tervela's customers share a common interest in achieving the highest level of security while their data is in motion.

Tervela's flagship product, Cloud FastPath, is a fast and automated solution for securely migrating, syncing, and backing up data. Cloud FastPath supports transfer between on-premises systems and cloud systems and between cloud systems.

This whitepaper describes the robust security measures Tervela has put in place to protect customer data as it moves.

## Cloud FastPath Certifications and Important Links

HIPAA
Health Insurance Portability and Accountability Act

Privacy Shield Framework

Massachusetts Data Protection Regulation

End User License Agreement | Privacy Policy | Acceptable Use Policy

## Transfer Security Begins at the Point of Presence

Cloud FastPath's unique distributed architecture allows customers to configure and manage data transfers between locations anywhere in the world using an easy-to-use web-based interface that can be accessed from anywhere.

The Cloud FastPath Point of Presence (POP) is the mechanism used to locate Tervela's software near the data source and target. These POPs are configured and controlled from the Cloud FastPath service, which instructs the POPs to communicate with each other to facilitate the data transfer. The POPs use Tervela's WAN-optimization protocol to transfer data in a highly efficient form between them. By putting a POP near the source and target, chatty, latency-sensitive native protocols are limited to very short distances.

Points of Presence take two forms: cloud-based virtual machines, automatically provisioned by the Cloud FastPath service; and on-premises agents, available in an easy-to-install package for Microsoft Windows.

The following steps describe how customers transfer data from on-premises storage to the cloud:

1. A lightweight Cloud FastPath software agent is installed on a computer behind the firewall. This constitutes the source POP.
2. The source POP accesses the source data using standard protocols such as SMB (for file server data), a Sharepoint API (for on-premises Sharepoint data), etc. depending on the source system type. This communication happens behind the firewall and may or may not be encrypted, depending on the policies in place in the source environment.
3. The source POP encrypts the source data with TLS using the AES-256 cipher.
4. The source data streams directly via TLS to a cloud POP near the target
5. The target POP decrypts the TLS stream and makes a series of secure REST API calls over HTTPS to store the data at the target platform, most typically a cloud service or infrastructure.

When the source data resides in a cloud-based service rather than an on-premises system, one or two cloud POPs are used. In some cases the cloud POPs may be in different geographical locations or from different vendors, depending on the most efficient transfer topology.

Cloud POPs are virtual machines in Amazon Web Services, Microsoft Azure, or Google Cloud Platform. These cloud service providers' data centers are compliant with SSAE 16 Type II requirements, and use advanced measures for redundancy, availability, physical security and continuity. In most cases, customers choose which provider they prefer to run their POPs in. To facilitate simple dynamic provisioning, most Cloud POPs are created using Tervela's account with the respective cloud services provider: all have strict access management protocols in place. A customer may choose to host their POPs within their own AWS, Azure, or Google account instead, with some limitations in available functionality.

amazon web services

Amazon Web Services Security Information

Google Cloud Platform

Google Cloud Platform Security Information

Microsoft Azure

Microsoft Azure Security Information

In the Cloud FastPath architecture, customer data never touches the cloudfastpath.com service. It is transmitted directly between customer POPs that are uniquely provisioned for each customer; POPs are not shared between customers. Customer data is never stored in the POPs: it is never written to disk, cached, staged or persisted in any way. All data is kept encrypted at every stage as it moves from the source to the destination.

## Understanding Cloud FastPath's Data Transfer Protocol

Each POP connects to the Cloud FastPath orchestration service using industry-standard Transport Layer Security 1.2, sometimes known as SSL. The orchestration service is located by a well-known DNS name and presents a TLS certificate signed by a well-known Certificate Authority. POPs cryptographically validate that they are communicating with Tervela's service using this certificate. This connection is used for command and control, but not data transfer.

The data transfer connection between the source POP and the destination POP uses Tervela's proprietary WAN-optimized streaming protocol, which is also protected by TLS. For this data transfer connection, the Cloud FastPath service generates an ephemeral TLS certificate at the start of every data transfer, and sends this certificate over the TLS-secured orchestration channel to each POP simultaneously. One of the POPs acts as the initiator of the connection (this will be the on-premises POP if there is one) and connects to the other POP, at which time each POP cryptographically verifies that it is communicating with an entity that has the private key of the ephemeral certificate, and also that the randomly generated Common Name (CN) field in the ephemeral certificate matches.

Because these ephemeral keys are generated just before the transfer starts, and are securely transmitted to each POP and nowhere else, it is assured that only the two POPs known to the Cloud FastPath service can communicate with each other. Any other entity would not have access to the necessary certificate. The certificate keypairs are then used to exchange the AES-256 session key using the standard TLS mechanisms. Perfect forward secrecy is enabled, so even if the ephemeral certificate's private key was recovered in the future by a bad actor it could not be used to decrypt a recorded transfer stream.

Cloud FastPath ensures data integrity between source and target via MD5, SHA-1, or similar data integrity hashes. The integrity verification algorithm varies based on the specific source and target involved, and its name, along with the hash value itself, are recorded in the transfer report for each file.

# How Cloud FastPath Uses File System Properties

Cloud FastPath obtains file system properties as part of analysis, simulation, and transfer jobs. This information is used to facilitate file synchronization, map user names, map file permissions, and for reporting and accounting purposes. Basic file system properties that may be retrieved by Cloud FastPath include file name, file size, file type, creation date, last modification date/time, file owner, and the access control list / permissions.

The file information is encrypted and streamed to the Cloud FastPath service, where it is stored in an encrypted database. The properties are used for reporting and analytics on transfer results and to generate the user and group permission mapping spreadsheet. This spreadsheet can be downloaded, modified, and re-uploaded to provide the necessary configuration details for data transfer jobs that map users and permissions between different source and target systems. The spreadsheet itself is also stored in an encrypted database, and is uploaded and downloaded via TLS.

## Account Credential Security

A Cloud FastPath account requires a valid email and password. Passwords must be at least eight characters, mixed case, and contain one digit. The Cloud FastPath service does not store the passwords directly. The industry-standard Password-Based Key Derivation Function 2 (PBKDF2) algorithm is used to key-stretch and derive a salted non-reversible hash of the password which is stored in a secure database.

Cloud FastPath accounts will be automatically locked out after multiple failed login attempts. Users will be automatically logged out after thirty minutes of inactivity.

Multiple users may be added to a single Cloud FastPath account. One or more of these users may be designated the administrator of the account, with the ability to add new users and remove existing users.

For cloud storage providers Cloud FastPath authenticates to the third party service with OAuth2, which means that Cloud FastPath does not have access to the user's third party service credentials. For more information on how OAuth2 works, visit this resource.

For on-premises systems the Cloud FastPath agent will run under the credentials it is invoked as, with the same access level. This can be a limited-scope service account, a standard user account, or an administrator account.

Cloud FastPath accounts are enforced by two-factor authentication via a TOTP application

Cloud FastPath does not collect or store login credentials for cloud providers or on-premises systems except in the following cases:

1) When using on-premises Sharepoint in a non-default configuration where Windows Integrated Authentication is disabled.
2) When using Amazon S3, Google Cloud Storage, or other object store where an access key ID and secret key are required. It is simple to provision a dedicated limited-access keypair for this purpose.

Cloud FastPath includes a programmable interface, or API. The API uses the same login credentials as the web application. In both cases, it is incumbent on the user to protect the security of their credentials.

## Building Security into Tervela's Policies and Procedures

Tervela's employees are trained on Tervela's policies and procedures which are maintained, reviewed and updated regularly. The following represent some of the many internal policies Tervela enforces as part of Tervela's ongoing commitment to the highest levels of security:

- Employee background checks
- Regular employee security training
- Corporate facility access
- Disaster recovery and redundancy
- Software upgrade and patch management
- Incident response procedures
- Access privileges
- Password management

Tervela also works to maintain the security of corporate networks and files, with:

- Network and host intrusion detection systems
- Log reporting, analysis, archiving and retention
- Internal monitoring and reporting
- Proactive vulnerability scanning
- Remote network access through VPNs with multi-factor authentication

Tervela uses third-party security testing resources such as Qualys. In addition, third-party penetration testing has been performed on Cloud FastPath systems.

## Responding to Security Events

Tervela's Incident Response Team handles any significant security events per Tervela's defined policy. If customer data is accessed without authorization Tervela will immediately notify the customer.

Cloud FastPath is designed to ensure Tervela can respond quickly if new security issues arise. The Cloud FastPath architecture ensures that the service components and the POPs can be quickly and remotely upgraded and patched without customer intervention.

## Managing Insider Risk

Managing insider risk is simplified by the design of Cloud FastPath. For on-premises systems Tervela has no direct access to the customer's data. Any access must be given indirectly via the POPs, which are under customer control. For cloud systems OAuth2 authentication ensures that Tervela has no access to customer login credentials.

Furthermore, any access to production or development environments is limited and requires VPN access. A limited number of employees have access to the production environment and access can be revoked at any time. Their credentials for access to those services are protected by two-factor authentication.

Thank you for your interest in Cloud FastPath.

If you have additional questions, please contact us at: cfp-info@tervela.com