Cloud FastPath: Highly Secure Data Transfer

Tervela helps companies move large volumes of sensitive data safely and securely over network distances great and small. Tervela has been creating high performance data transfer technology for over a decade. Tervela's customers range from Fortune 100 companies in the financial services sector to small businesses. Despite this diversity, all of Tervela's customers are bound by a common interest: achieving the highest level of security while their data is in motion.

Cloud FastPath's secure architecture moves data to and from cloud-based storage services and on-premises systems.

This whitepaper describes how Tervela continuously invest in robust security measures to protect customer data as it moves.

Security Begins at the Point of Presence

The Tervela Cloud FastPath architecture achieves exceptional data security and performance through the use of "Points of Presence", or "POPs" near the source and destination. Customers control the POPs via Tervela's easy-to-use web application.

When customer data needs to travel from on-premises systems, it needs to flow through an on-premises POP, to a cloud POP, then to the destination in the following steps:

1. A lightweight software agent is deployed near the source behind the firewall
2. Since the agent is behind the firewall, data is transferred between the system and the agent in its unencrypted form
3. The data is then encrypted with AES-256 cipher
4. The data streams directly via TLS to a cloud POP near the destination
5. It moves from the POP to its end destination, and is unencrypted

When customer data needs to travel from a cloud-based file service rather than an on-premises system a cloud POP is used at the source. **Cloud FastPath employs TLS at all points of a data transfer.**

With the exception of on-premises POPs, all POPs are virtual machines in Amazon Web Services, Microsoft Azure, or Google Cloud Platform. The customer can choose which provider they would like to run their POPs in. POPs are managed under Cloud FastPath's accounts where strict access management protocols are in place. A customer can also host POPs within their own accounts.

This data flow is key to ensuring that customer data remains safe. With the Cloud FastPath architecture, customer data never touches the cloudfastpath.com service. It is transmitted directly between customer POPs. Moreover, except for the few bytes flowing through the POP at a given moment, data is never stored in the POPs. Those few bytes are kept in a temporary buffer that is used for protocol transformation, and discarded at the completion of that operation. It is never cached, staged or persisted in any way. In fact, it never even touches a disk as it is being transferred. And all the data is kept encrypted at every possible stage as it moves from the source to the destination.

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. Passwords are stored in Tervela's encrypted servers using salted password hashing. Cloud FastPath has automatic lock out after a number of failed login attempts and has automatic logout after a period of inactivity.

For cloud storage providers Cloud FastPath authenticates with OAuth2 through a user with admin privileges. For on-premises systems the user needs admin permissions to install Cloud FastPath's agent.

Cloud FastPath includes a programmable interface, or API. When using the API, it is up to the user to ensure that the information it requires to authenticate with the service is not exposed to untrusted parties. Two schemes are available for providing these credentials to the API: a securely permissioned configuration file and industry standard OAuth2.

Understanding Cloud FastPath's Data Transfer Protocol

Cloud FastPath's web application orchestrates the entire transfer by instructing the source and destination POP how to contact each other. This enables the POPs to establish a high bandwidth connection while a transfer takes place.

To ensure the transfer is secure, this connection is encrypted using Transport Layer Security (TLS), or SSL.

Each POP authenticates with the other POP using TLS certificates issued by the Cloud FastPath in-house certificate authority. Cloud FastPath uses in-house certificates due to the dynamic nature of the POP architecture. Additionally, a secret is generated by each POP and is transferred securely via our in-house certificates. These certificates can be revoked remotely. TLS connections are terminated upon the deletion of a POP or an account closure. Cloud FastPath's infrastructure ensures one customer never has access to a POP of another.

Cloud FastPath ensures data validity between sources via a MD5 or SHA-1 checksums. Checksum method and validation status are given in the transfer reports.

How Cloud FastPath Uses File System Properties

The Tervela Cloud FastPath service queries a limited set of file system properties to orchestrate secure data migration. This information is used to facilitate file synchronization, to map user names, file permissions, for reporting and accounting purposes. File system properties that may be retrieved by Cloud FastPath include basic file information such as file name, file size, creation date, last modification time, and the access control list for each file.

Cloud FastPath queries the file system of the machine or service on which it is running. This information is encrypted and streamed to the Cloud FastPath secure servers where it is encrypted at rest. The metadata is used for reporting and analytics on transfer results, and to generate an account mapping spreadsheet in xlsx format. The operator edits the spreadsheet to assign or retain permissions. This spreadsheet is sent over an encrypted network connection both to and from the operator, and the resulting records are stored in a secure database.
NOTE: access control lists are only queried when using the account and permission mapping features of Cloud FastPath.

Cloud FastPath's Hosted Data Centers

The Cloud FastPath service is hosted and managed in data centers that are compliant with SSAE 16 Type II reporting requirements, and use advanced measures for redundancy, availability, physical security and continuity.

This means:

- the data centers are highly available and offer n+1 or greater redundancy to ensure disaster recovery and business continuity
- the equipment is physically secure with on-site monitoring, guards, access controls and logging

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
- Corporate facility access
- Password management
- Access privileges
- Software upgrade and patch management
- Incident response procedures
- Disaster recovery

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
- Vulnerability scanning
- Remote network access through VPNs with multi-factor authentication

Tervela also uses third-party network security testing resources to find potential vulnerabilities.

Tervela’s Incident Response Team handles any significant security or service events according to Tervela’s defined policy. If customer data is accessed without authorization Tervela will immediately notify the customer.

Responding to Security Events

Cloud FastPath is designed to ensure Tervela can respond quickly when new security issues arise. For example, Cloud FastPath’s security team monitors issues with TLS and implements patches immediately.

CFP architecture ensures that the cloud application and the POPs can be quickly and remotely upgraded with new components that address flaws in the software.

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 the user’s control. For cloud systems OAuth2 authentication ensures that Tervela has no access to customer login credentials.

Furthermore, Tervela limits who in the organization has access to the running services. Only certain employees have access to public and private keys and access can be revoked at any time. Their credentials for access to those services are protected by two-factor authentication.

Summary

Cloud FastPath’s POP architecture ensures end to end data security. No data is ever stored outside of memory and data moves directly from source to target. Data is encrypted with AES-256 protocol while in flight. TLS is used in all Cloud FastPath systems.