Resilio Connect

Technical Review

Security

INTRODUCTION

Resilio Connect uses cryptographic security that is built on industry standards to achieve maximum security for the product. The implementation is based on open-source OpenSSL cryptographic libraries that are used in addition to the operating system provided cryptographic APIs.

RESILIO CONNECT SECURITY MODEL OVERVIEW

- Mutual authentication and authorization of clients and Management Console
- Generation of one-time session encryption keys between clients
- Data in transit encryption
- Data integrity validation
- Standard encryption protocols: TLS 1.2, AES-256, SHA2

KEY FEATURES

Industry-standard cryptography using the open-source OpenSSL

Data integrity is based on the SHA2 and ED25519 signature algorithms

Admin configurable choice of standard cipher sets: AES-256 or AES-128

TLS 1.2

Perfect forward secrecy

System-wide event logging for security audit

Works inside your private infrastructure

SESSION ENCRYPTION

All the communications are end-to-end encrypted.

Agent to Agent Communication

The Management Console generates a pair of 256-bit keys for each transfer job. The pair includes a read-only and read-write private key that defines different access permission for the Agent. The Management Console provisions each agent with the right key depending on the job configuration. When an agent requires a data transfer it starts a transfer session. Each transfer session between two agents has a unique TLS 1.2 connection with a unique session key. Sessions are encrypted using TLS cipher suites DHE-PSK-AES 128-GCM-SHA256 or DHE-PSK-AES256-GCM-SHA384 and provide data forward secrecy that protects past sessions against future compromises of session keys.

Agent to Management Console Communication

Communication between the Agent and the Management Console is done over TLS 1.2.

AUTHENTICATION

Resilio Connect requires mutual authentication of all parties in the system. The Management Console and Agent mutual authentication relies on an agent's private token and servers X.509 certificate. The Management Console verifies that an agent provides a valid private token before starting any communication with the agent. The private token is unique for each agent. Agents verify that management console has a valid X.509 certificate fingerprint that validates the authority of the server running the Management Console.

Agent to agent authentication relies on TLS 1.2 Diffie-Hellman key exchange authenticated with a pre-shared job keys. An agent without a job key (that was provisioned by the Management Console to only authenticated agents) cannot negotiate a data transfer session key.

DATA ENCRYPTION

Data in transit is encrypted using TLS 1.2 and 128-bit or 256-bit AES encryption. TLS session keys are generated using the Diffie-Hellman key exchange protocol and a pre-shared job's private key. All the data within the session is encrypted with AES in Galois-Counter mode (GCM). The GCM mode is designed to be efficient in high-speed communication while providing authenticity (integrity) and confidentiality. The administrator has the ability to choose a 128-bit or 256-bit cipher length for data encryption.

DATA INTEGRITY

Resilio Agents split each file into blocks (32KB or more) and calculates the SHA2 hash of each block. The list of hashes is signed with the relevant job's 256-bit read-write key using the ED25519 algorithm. The list of hashes and the signature (file metadata) are transferred before the actual data transfer. The receiver validates the signature of the metadata and the integrity of each received block by validating its hash against meta information. Damaged or corrupted blocks are discarded and scheduled for retransmission. Once a file is assembled the receiver validates the hash of the complete file.

This approach ensures that only agents with proper permission can update information about files and prevents ingestion of malicious information inside a data transfer and modification of files without proper permission.

AGENT SECURITY

The Resilio Connect Agent is a single binary that has no external dependencies on libraries and frameworks. The Resilio Connect Agent uses a limited number of well-defined ports and protocols for all communications with other machines and the Management Console. The Resilio Connect Agent doesn't require any administrative privileges to run. It can be run in a sandboxed environment or by a user with limited permissions.

PRIVATE INFRASTRUCTURE

Resilio Connect runs completely within the Customer's private infrastructure. It doesn't require any external web services or connections to external resources.

FIREWALL CONSIDERATIONS

Resilio Connect is designed for deployment inside the enterprise. It has a well-defined list of ports and protocols required for the operation. Ports and protocols used are as follows:

PURPOSE	PROTOCOL	DEFAULT PORT
Tracker Service (Agent Discovery)	TCP and UDP	3000
LAN Discovery (optional)	UDP Broadcast	3838
Data Transfer	TCP and, or UDP	3939
Management Console Web Interface	TCP	8443
Agents Control and Status	TCP	8444
Agents Log Upload	TCP	8445

(For a detailed description of network usage, see the ***Ports & Protocols KB article****)*

DEVELOPMENT PRACTICES

Resilio, Inc, the developer of Resilio Connect, has achieved SOC 2 Type 1 compliance for the description of its system and on the suitability of the design of its controls relevant to security. Resilio maintains a quality assurance process for code testing. Each version of Resilio Connect undergoes penetration tests using Dynamic Application Security Testing (DAST) tools before release.

Additionally, the company's cryptographic technology used in its products has been reviewed by an expert independent third-party security auditing company and found to be sound in design.