RelaNet

# Security in RelaNet Cloud

An overview of how customer data is secured and protected within RelaNet Cloud

relanet.com

# Table of Contents

## Introduction

RelaNet Cloud is the hub of most of the online services that RelaNet offers. It integrates an email, a client portal, calendars, contact management, and more. RelaNet Cloud stores a great deal of confidential information, and our customers trust us to protect that information and keep it secure. We take that trust very seriously.

In order to protect the data stored within RelaNet Cloud, we employ multiple layers of security that work together keep your information safe. We build RelaNet Cloud on top of carefully chosen and trusted technologies. We employ defenses to harden RelaNet Cloud against malicious actors. We take steps to authenticate the identity of those who access RelaNet Cloud. And we provide tools that allow you to control who can access your data.

In this document we provide an overview of these security measures. It is our hope that this overview will give you confidence that we adequately protect your confidential information, and demonstrate that we make every effort to be worthy of the trust our customers place in us.

## Underlying Technologies

Like any software product, RelaNet Cloud is built upon other software and systems. These underlying technologies were chosen for their proven record of security, and together they create an environment that helps keep your information safe.

### Data Centers

All RelaNet servers reside in professionally managed data centers that have strict policies in place for the physical security of the hardware they host. All RelaNet data centers have completed SSAE-18 SOC 2 audits that attest that these data centers have controls in place to ensure the security, availability, processing integrity, confidentiality, and privacy of the hardware that they host.

### Linux

All servers that host RelaNet Cloud run up-to-date versions of the Linux operating system. Linux has long been an industry standard for servers, and is widely respected for its security. All RelaNet servers check for updates daily, and security updates are automatically applied.

### Apache

RelaNet Cloud is served by the Apache HTTP Server, one of the most established open source projects in existence. Apache is one of the most frequently used web servers on the Internet, serving almost 25% of the one million busiest websites.

### Nextcloud

RelaNet Cloud is based on Nextcloud, an open source productivity platform that is designed with privacy in mind. Deployed at thousands of organizations for tens of millions of users, Nextcloud is the most popular self-hosted collaboration solution available today. It is trusted by organizations such as Siemens, the French Ministry of Interior, and the German Federal Information Technology Center (ITZBund).

### MariaDB

RelaNet Cloud also relies on MariaDB, a community-developed, commercially supported version of the MySQL relational database management system. MariaDB is one of the most popular database servers in the world, and is trusted by organizations like Google, Mozilla, and Wikipedia.

# Security Hardening

Beyond the security that is provided by the technologies listed above, RelaNet Cloud also employs several strategies at the presentation, session, and transport layers to improve security and further protect the data it stores. These strategies include:

## HTTP Strict Transport Security

HTTP Strict Transport Security is a web security policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers should automatically interact with it using only encrypted HTTPS connections, which provide Transport Layer Security (TLS/SSL).

## Data Encryption

RelaNet Cloud enforces industry-standard TLS/SSL encryption for data in transit. Additionally, data at rest is stored encrypted using strong AES-256 encryption.

## Content Security Policy 3.0

Content Security Policy (CSP) is a HTTP feature that allows the server to set specific restrictions on a resource when it is opened in a browser. For example, policies can be set that only allow images or JavaScript to be loaded from specific targets.

CSP 3.0 is the latest and strictest version of the standard, increasing the barrier for attackers to exploit a Cross-Site Scripting vulnerability.

## Same-Site Cookies

Same-Site cookies are a security measure supported by modern browsers that prevent Cross-Site Request Forgery vulnerabilities and protect your privacy further. RelaNet Cloud requires same-site cookies to be present on every request by enforcing this within the request middleware.

RelaNet Cloud also includes the __Host prefix to the cookie (if supported by browser and server). This mitigates cookie injection vulnerabilities within potential third-party software sharing the same second level domain.

### Encrypted Session Data

RelaNet Cloud encrypts session data (including login state, user name and other data) before storing it. The encryption key is stored in a cookie on the client which has to be sent to the server with every request for data the user sends. Without that cookie, session content can not be decrypted and the user will have to log in again.

Encrypting the session provides an additional barrier against unauthorized access. An attacker would have to make modifications to the RelaNet Cloud server code to be able to intercept user data.

And if, intentionally or not, data from the session is stored or backed-up, it will not be readable, also avoiding compliance violations.

### Trusted Domains

RelaNet Cloud checks domains in the Host header to ensure that users can’t access the site using another domain. This prevents RelaNet Cloud from generating faulty URLs that redirect users to a compromised server.

## Directory Traversal Protection

The RelaNet Cloud internal file system code has a number of protections built in, such as forbidding character sequences like “..\” or “../”.

# Authentication

RelaNet Cloud employs a number of security measures that help ensure that only authorized people log into the system. These security measures include:

## Strong Password Policies

RelaNet Cloud requires that all passwords meet minimum requirements which consider the password’s length, and its use of different alphanumeric and symbolic character sets. All passwords are checked against lists of common passwords and lists of publicly compromised passwords, in order to prevent dictionary attacks.

## Brute-Force Protection

Brute Force Protection logs invalid login attempts and slows down multiple attempts from a single IP address (or IPv6 range). This feature protects against an attacker who tries to guess a password for one or more users.

## Two-Factor Authentication

RelaNet Cloud makes two-factor authentication available to all users. The particular type of two-factor authentication employed by RelaNet Cloud is a Time-based One-Time Password (TOTP). When two-factor authentication is enabled for a user, that user will need to generate a time-limited six digit code on his or her security device (typically a smartphone), and provide that code in addition to the usual username and password. This provides additional evidence that the user logging in is actually authorized to have access to the system.

# Data Control

Control is key to security. With RelaNet Cloud, you control your data and who has access to it. RelaNet Cloud gives you that control through a number of features designed to help you manage your files and how they are stored. These features include:

## Logging and Monitoring

RelaNet Cloud has built-in monitoring and logging tools that allow you to monitor when files are uploaded, downloaded, and shared.

## Permission System

Users can set permissions for sharing and accessing files they own on an individual user or group basis. With read, write, edit, and delete permissions available, access to a file or directory can be as restrictive or loose as is required.

## File Access Controls

The file access control features built into RelaNet Cloud allow you to satisfy legal or business requirements by setting system-wide policies to control who can access information. With file access controls, you can set up rules like "XLSX files from the human resources department are not to be accessible outside the company IP address range", or "Files tagged 'confidential' can only be accessed by members of the admin group". These rules are created at a system level are enforced by RelaNet Cloud no matter what the permissions on an individual file might be.

## Data Retention Rules

RelaNet Cloud allows administrators to define rules for data retention, allowing you to automatically delete files after a set amount of time, based on the characteristics of those files. These rules can be used to enforce compliance with corporate data retention policies, and manage the amount of storage that is used.