Link to article: https://discover.claromentis.com/knowledgebase/articles/568

Security Overview (Infrastructure and Application Security)

Introduction

This article covers both platform and application/framework security and describes how we protect against commons attacks. Information about security measures which you can configure yourself within the application is also detailed below.

Claromentis is a web-based application, meaning that it does not require any client installation. All files and data are stored on the server(s), unless downloaded onto a local machine.

Claromentis offers two main deployment options:

SaaS / Cloud: Software is installed and managed (on behalf of the client) on the Claromentis cloud infrastructure.

On Premise: Software is installed on an environment hosted on the client's infrastructure or within a data centre controlled by the client.

SaaS / Cloud - Security

The Claromentis Cloud infrastructure provides a proven, scalable and secure environment for a low initial cost. Under this arrangement, customers pay a single monthly/annual fee, which provides the software, hardware and support. The setup, maintenance and monitoring is taken care of by the Claromentis team, this takes the workload away from the client's organisation.

Our Cloud infrastructure is hosted within the Google Compute Platform (GCP). Google maintains the responsibility for the physical security of the solution, and the secure configuration and availability of the physical and network infrastructure.

The Google Cloud datacenters use start of the art security to protect and restrict access to client data, refer to https://cloud.google.com/security/whitepaper#state-of-the-art_data_- centers

Please refer to the Google Cloud security page at https://cloud.google.com/security/ and https://cloud.google.com/security/compliance - this includes information about:

- Data Center Physical Security
- Server and Software Stack Security
- Data Access
- Data Disposal
- Platform Security Features
- Data Encryption
- Intrusion Detection
- Compliances and certifications

Google Compute engine is a bit different to a public/private/hybrid cloud offering. Google Compute Engine is an Infrastructure As A Service or IaaS platform. Claromentis runs on it's own private network within Google Compute where we create private, single tenant environments for each client. For security reasons, Google keep their cards pretty close to their chest when it comes to topologies and infrastructure, but the information that Google provides is as follows: Google Infrastructure Whitepaper (2020)

Certifications / Compliance

We are ISO 9001, ISO 27001 certified and HIPAA compliant. Proof of certification can be provided on request.

Claromentis - Security Controls

In addition to the security that our hosting platform provides, we also maintain the following security controls:

- Multi-level firewall – We protect our infrastructure with a firewall set up in Google Cloud, stopping any unauthorised activity before it reaches our cloud network, as well as running an OS-level firewall for a double level of protection for each server.

- For anyone who chooses to go with one of our load-balanced systems, an added benefit is that the HTTPS load balancer that we use will protect against Layer 4 attacks.
- Network – Our Google cloud private network is completely private from any other business running on Google's cloud platform. Reducing the chance of a threat from within the infrastructure itself.
- Vulnerability Scanning - To ensure that each server is fully tested against vulnerabilities in the network, operating system or application, we run regular scans on our SaaS platform using a third party application
- Penetration Testing - We have penetration tests carried out by an external, Crest Certified organisation on a regular basis for external verification of our security controls. Customers can view this detailed report under NDA, or you may view a redacted version as proof of our most recent penetration test here.
- Patch Management - Devices are patched to remediate any vulnerabilities in the operating system or third-party packages.
- SELinux – All VM instances are protected with a Linux kernel security module called SELinux, originally developed by the NSA/United States Department of Defence.
- Brute force protection – All our machines are protected by monitoring brute force attempts on open ports.
- Secure server access only – Employees at Claromentis will only be granted access to the server using secure protocols and key-based authentication. With an account set up for each employee, all access is fully audited.
- Monitoring: We monitor the infrastructure for anomalies (for example, excessive resource usage) as well as using a third-party uptime monitoring solution to ensure we meet our SLA's.
- Logging – As well as server-side logging, all logs are automatically uploaded to the Google cloud monitoring tools so that we have an easy way to audit and monitor any unauthorised or malicious access.
- SSL – *see encryption 'In Transit', below.
- Encryption: Within the Claromentis/Google Cloud environment, data is encrypted In Use, In Transit and At Rest:
    - In use: Persistent disks attached to each VM instance are encrypted.
    - At rest: Backups stored in Google cloud storage are also encrypted.
    - In transit: We offer a free *.myintranet.com SSL certificate for each client. Alternatively, for non *.myintranet.com domains, we also offer an SSL certificate package for custom domains (e.g. site.yourcompany.com). Alternatively, we can install an SSL certificate provided by your team.
    - For further information on the type of encryption used, please refer to: https://cloud.google.com/security/encryption-at-rest/

On Premise - Security

In this instance, Claromentis is installed on your own infrastructure (i.e. office or private data centre).

The client's IT department will be responsible for everything that is described in the following guide:

On Premise - Hosting Recommendations & Requirements

As Claromentis is a web-based application, Claromentis will be responsible for the installation and maintenace of the web server, the Claromentis framework and any third party tools we install on your behalf.

Code / Framework Security

Claromentis is protected from the following attacks:

- SQL injection: Prevented using custom-made variable inserts.
- CSRF attacks: Prevented using tokens for all requests.
- XSS (Cross Site Scripting): Wherever possible, we restrict entering plain HTML with Javascript. In places where we have to use HTML, it is made safe using HTML Purifier (http://htmlpurifier.org).
- Session hijacking: We bind each session to the original IP address from where it was initiated.
- Brute force attack: User accounts will be locked for a period of time after a certain number of failed attempts to login (this is configurable).
- Obfuscation: PHP files are obfuscated to protect the source code.
- Error Handling: Claromentis also uses a special error handler, which prevents users (possible attackers) from seeing internal structure or the system itself, but alerts users to an error that has occurred.
- Penetration Testing: Our SaaS platform is regularly checked using penetration testing tools. We also invite customers to carry out penetration testing (or request a third party to do so), so long as we are made aware of this prior to any tests.

Standards / Compliance

Claromentis security guidelines are based on OWASP (The Open Web Application Security Project): https://owasp.org/Top10/

Application Security

Here is a list of security configurations you can enable yourself within the application. i

- Permissions System: Claromentis has a robust, in-built, permission system ensuring sensitive information may only be accessed by certain users.
- Security Level based on IP address: Security levels allow an additional permission layer within the DMS (Document Management System). There are 5 security levels ranging from Unclassified to Top Secret. If enabled, Administrators can define which security level is applied to each user. A security level can then be set on folders and documents, meaning only those users with the matching security level (or higher) will have access. Furthermore, IP ranges can be restricted to a certain security level. If there is a firewall or proxy between the web server and the user's computer, the firewall IP will be assumed.
- Password Policy: The password policy is fully configurable for each system. Options include the ability to enforce a strong password, maximum password age, login attempts before the account is locked, how many minutes a frozen user is locked out of an account as well as the functionality to send a notification to Administrators upon account lockout.
- Two Factor Authentication: Two factor authentication can be set up using any app that supports the Time-based One-Time Password algorithm. This includes Duo, Google Authenticator, Authy and Microsoft Authenticator - https://www.wikiwand.com/en/Time-based_One-time_Password_algorithm. This setting can be enforced for all or even just a subset of users (role, group or extranet).
- Password Storage: Passwords are securely hashed prior to being stored in the database and encrypted using the latest Blowfish encryption techniques.

- System Audit: Activity within Claromentis is monitored, unless you choose not to do so. This audit captures the date/time, IP address, user ID, data concerned and action performed.
- Document Content Signatures: MD5 is a one-way hash algorithm, used to determine the integrity of a file, by providing a 128 bit digital signature. If enabled in the system, an additional option will be available on the document properties page.

Created on 13 May 2019 by Will Emmerson. Last modified on 8 February 2024
Tags: claromentis, security, framework, protection, compliance, audit, certification