precisely

EngageOne Communicate

Security White Paper

Version 1.2

Table of Contents

1 - Security White Paper

1 - Security White Paper

June 2020

This document describes the security of EngageOne Communicate. It begins with a summary of the key security points. More detailed information is provided in the remainder of the document.

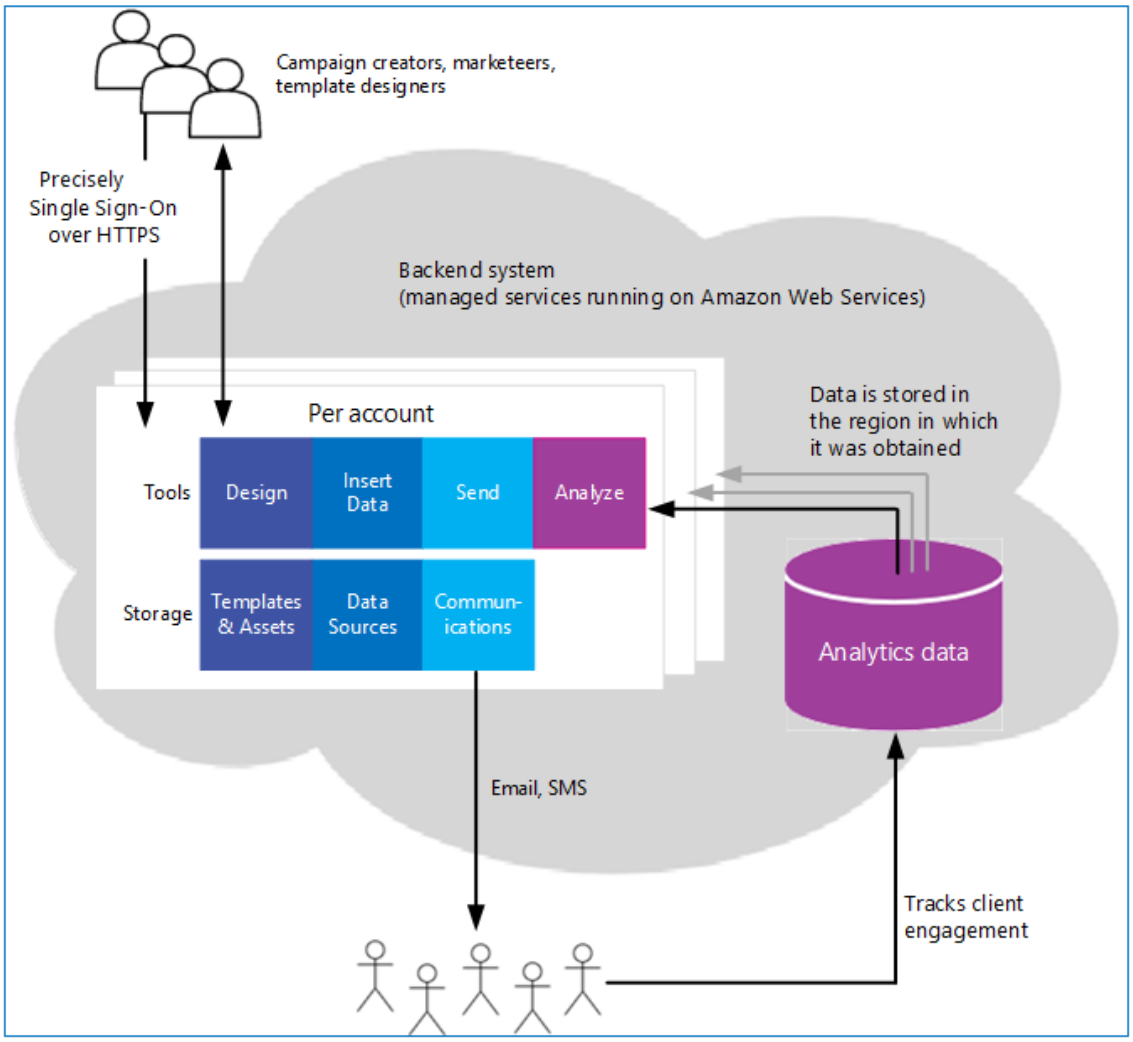
It is intended for EngageOne Software clients, partners and employees.

In this section

Introduction

This document describes the security of EngageOne Communicate, such as how it handles personal data and its use of Amazon Web Services (AWS). The main security considerations are shown in the figure below, with an overview in the **Communicate security summary** on page 5. For more detail on any points, refer to the remainder of the document.

Figure: Communicate – Main Security Considerations



Communicate security summary

This is an overview of the main security considerations for EngageOne Communicate. You can find more information about these points in the remainder of this document.

Communicate application

- Communicate is a cloud-based application.
- All internet traffic is over HTTPS (TLS 1.2).
- EngageOne Software has a global authentication mechanism for all its online services.
- Users only have access to their team account (tenant).
- A user's role determines what they can do in Communicate. Roles include Administrator, Developer, Designer, Reporter and Campaign Creator.
- EngageOne Software run annual penetration tests to examine the security of Communicate software.

Communicate backend: Amazon Web Services (AWS)

Communicate is a cloud-native application, implemented using microservices. It relies on managed services provided by AWS.

- Backend resources (such as compute resources, databases and storage) are configured and deployed by the Engineering team, following AWS best practises.
- AWS is responsible for the provision, administration and maintenance of the AWS resources used by Communicate.

Data handling

This includes both the data uploaded by users for use in communications and the analytics data captured by Communicate. Tracked data consists of dates and times, email open and click rates, SMS delivery rates, IP address and user agent.

- Stored in the region in which it was obtained.
- Uploaded data is segregated by company account. Analytics data is co-mingled.
- Data at rest is encrypted.
- Environments are available for US-based Healthcare clients that must adhere to stricter data protection and privacy laws as required for HIPAA eligibility. These environments cannot be accessed by staff outside the US.
- Routine operational procedures means that authorized EngageOne Software staff potentially have access to a company's data. These staff are authorized by management and require specific administrator privileges. However EngageOne Software makes no use of the data.

Communicate security in more detail

This section discusses the security of Communicate in more depth, in particular:

Use of Amazon Web Services

Communicate runs on a cloud computing platform provided by AWS. This includes both the physical infrastructure and managed services.

The highly-secure, physical infrastructure provided by AWS enables EngageOne Software to provide a world-class, scalable and affordable software solution that does not make any compromises concerning the security of client data. EngageOne Software follows best practice in the configuration and deployment of its serverless applications in order to offer a secure and reliable platform that meets the requirements of the most security sensitive organizations.

> **Note:** You can find comprehensive documentation on AWS' security measures on the AWS website. For example AWS: Overview of Security Processes which is available from **https://aws.amazon.com/whitepapers/#security**.

Managed services

EngageOne Communicate relies on AWS managed services. This means that EngageOne Software is responsible for securely configuring and deploying the application but AWS is responsible for provisioning, managing and protecting the resources (compute resources, databases and storage).

For example, AWS is responsible for the security of physical infrastructure such as their data centers, while EngageOne Software is responsible for enforcing security of resources such as S3 buckets, through configuration, to ensure they are not publicly accessible over the internet, and that technical measures are in place to segregate customer data.

> **Note:** Additional resources are automatically provisioned as demand for Communicate increases. The deployment configuration ensures that resources are provisioned with the correct specification to meet both technical and security requirements.

Logical access controls

EngageOne Software use AWS Identity and Access Management (IAM) to control staff access to its AWS resources. This means that:

- Staff access is enforced by automated provisioning processes.
- The AWS Console requires username and password access along with multi-factor authentication (MFA).
- The AWS CLI access is controlled by the use of AWS Identity and Access Management roles (IAM).
- Access to resources, including account creation, follows the principle of least privilege.
- AWS CloudTrail is used to automatically audit actions made on the AWS account.
- No default usernames and passwords for admin users.
- Passwords are rotated every three months.

Cloud Governance

EngageOne Software Cloud Governance enforces compliance with policy and best practice for all AWS users in EngageOne Software. Communicate regularly review its AWS Trusted Advisor security report and resolves any issues that are identified.

Software patching and security updates

AWS is responsible for protecting the resources used by Communicate, and ensuring that there is no disruption to the service provided to clients. This is automatically handled through AWS Lambda.

> **Note:** EngageOne Software is responsible for applying patches and security updates to the Communicate code base and development environment. For details, see **Communicate software** on page 9.

Business continuity and disaster recovery tests

Communicate is fault tolerant across availability zones in AWS. EngageOne Software reviews the Business Continuity and Disaster plan quarterly, and tests this annually.

Anti-virus software

Anti-virus software is installed on employee machines that are used to connect to AWS infrastructure. EngageOne Software uses McAfee as standard.

Logs

- Logs are stored indefinitely in AWS Cloudwatch Logs.
- Logs can only be accessed via the AWS Console or AWS Command Line Interface.
- The AWS Console requires username and password access along with multi-factor authentication (MFA).
- The AWS CLI access is controlled by the use of AWS Identity and Access Management roles (IAM).
- Access to the logs are restricted only to users who require it.

Databases

Database management

EngageOne Software uses Amazon DynamoDB. This is a NoSQL, distributed database with region-specific tables. This allows data originating in a specific AWS region to be stored in that region.

AWS is responsible for operating, scaling and managing the database.

The database resources are configured with:

- Point-in-Time Recovery. Incremental backups ensure that database tables can be restored to any point in time during the last 35 days.
- Encrypted backups, stored within the same AWS region.
- Monitoring for throughput capacity (request traffic).
- Storage and rotation of database transaction logs.

Data at rest

The database (including the replicas made for backup purposes) are encrypted using the AWS Key Management Service (KMS). EngageOne Software uses AWS managed keys. AWS keys use AES-256 encryption — one of the strongest block ciphers available.

> **Note:** EngageOne Software needs to store the passwords required for access to Spectrum Enterprise OnDemand data sources. These passwords are encrypted at field level using KMS custom keys.

Data in transit

All data is transmitted using a Secure Socket Layer (TLS 1.2).

Communicate software

EngageOne Software develops the software that is used to design communications and send campaigns.

Communicate software is updated on a regular cycle.

Access to the Communicate application

Note: This describes how users access the Communicate application. For details of how EngageOne Software staff access the backend system, see **Logical access controls** on page 7.

- All external and internal access is over a TLS 1.2 encrypted connection.
- Access is granted based on roles, and clients can only see the communications, data sources, and campaigns for their account.
- A password policy is applied (minimum requirement is: 8 characters, with 1 uppercase character, 1 numeric character or 1 special character).
- Following industry best practice, stored passwords are hashed with a salt (a cryptographically-strong random value).

Secure design and development

Infrastructure vulnerability scans

Infrastructure vulnerability scans run monthly. These cover both the Communicate production and development environments.

Static application security scans

EngageOne Software performs static code analysis on proprietary source code. Any high or medium vulnerabilities are fixed within two weeks.

Open source security

EngageOne Software uses an open source security and license compliance management platform. Alerts are raised when any security vulnerabilities are identified in open source libraries. Any issues are fixed within two weeks.

Dynamic application scans

EngageOne Software performs dynamic application scans every three months on a replica of the production environment. The aim is to discover any security weaknesses in the current release that would be useful to a hacker trying to gain access to the application or disrupt services.

Red Team testing

EngageOne Software has Red Team group that performs an in-depth penetration test on a replica of the production environment. Like an external penetration test, a Red Team test tries to discover any security weaknesses in the Communicate software that would be useful to a hacker trying to gain access to the application or disrupt services.

For Communicate this is done annually. Issues identified by a Red Team test are fixed within four weeks.

External penetration testing

EngageOne Software commissions a third-party to perform an annual threat scan and penetration test. Typically this follows the Red Team test. The tests try to discover any security weaknesses in the Communicate software that would be useful to a hacker trying to gain access to the application or disrupt services. This is run on a replica of the production environment. Issues are fixed within four weeks.

The results of the test are dependent on individual client requirements as not all services are the same. The results will be shared with clients under a non-disclosure agreement. Using a screen share, an EngageOne Software representative will show the report to the client and explain the results.

Access controls on components

Communicate software uses software components. The roles configured for components follow the principle of least privilege.

Development practice

EngageOne Software has a change management policy which includes code review and testing:

- Detailed code reviews are performed for all updates to Communicate software. This includes a review of security. Code review is followed by testing.
- A suite of automated tests runs regularly after reviewed changes are submitted to the code base. This includes monitoring of all open source components. See **Secure design and development** on page 9.
- All changes are tested before release.
- Regression testing is performed at every minor release (regression testing ensures that older parts of the software work with the new changes).

When deploying software updates, staff follow standard operating procedures. If an incident occurs, the circumstances are reviewed so that operating procedures can be updated if necessary.

All deployments are logged in AWS CloudTrail.

Notices

precisely

2 Blue Hill Plaza, #1563
Pearl River, NY 10965
USA

www.precisely.com