precisely

Security White Paper

Version 2.0

Table of Contents

1 - Security White Paper

1 - Security White Paper

January 2023

This document describes the security of EngageOne™ Communicate.

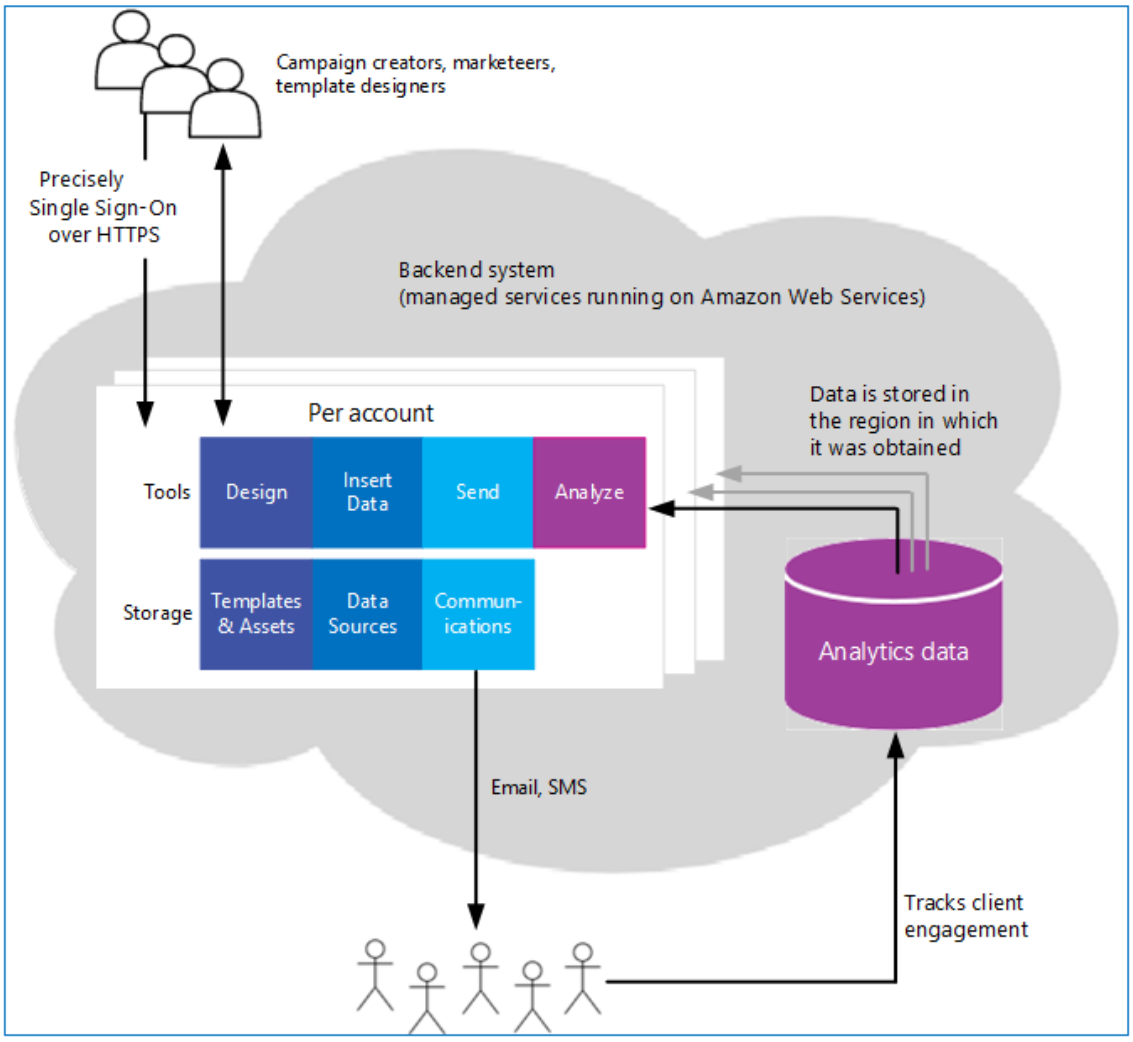
It is intended for EngageOne™ Software clients, partners and employees.

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.

Figure: Communicate – Main Security Considerations



- EngageOne™ Communicate is a cloud-based application.
- EngageOne™ Software has a global SSO authentication mechanism provided by OKTA for all its online services.
- Users only have access to their team account (tenant).

- EngageOne™ Communicate uses role-based access controls. Roles include Administrator, Developer, Designer, Reporter and Campaign Creator.
- EngageOne™ Software runs annual penetration tests to examine the security of EngageOne™ Communicate Software.
- Data is encrypted in transit and at rest.
- There is no co-mingling of customer data.

Common security controls

This section describes the common security controls.

Information security risk governance and compliance

Precisely's Board of Directors own security and are accountable for the organisation's risk management framework. At a product level the EngageOne™ Information Security Forum and Technical Security Group manage risk associated with products and services and own the associated Information Security Document Framework.

EngageOne™ maintains a comprehensive security control framework described within our information security policies and standards governing how our products, services, and teams are managed securely. All our information security policies are owned by our Information Security Forum and are reviewed at least annually or upon relevant business change.

We maintain security capability with an enterprise information security team made up of security risk, compliance and technical experts. In addition, security expertise is embedded within the EngageOne™ engineering team to ensure that security controls are implemented and working as intended. Where exceptions or deviations to our security control framework are identified through audit or internal review, we undertake action to remediate and implement corrective actions.

Our compliance team audit our security controls and we use a cycle of continuous improvement to ensure that our controls and associated frameworks are optimized and develop within the changing security landscape. We also commission independent external auditing of our security control framework and provide a SOC2 Type 2 report for the scope of our SaaS services and common controls.

Human resource security

Thorough non-disclosure agreements and employee terms and conditions are in place, and background screening and checks are a requirement for all employees and contractors prior to employment (where legally permissible).

A robust program of security education, awareness and training is in place for all employees at least annually with specific skills training in place for specialist roles.

Information classification, labelling and handling

A program of information classification is in place to ensure that information assets (including client and partner assets) is consistently applied. Labelling ensures that the classification is always visible and handling procedures and training are in place to ensure that information is protected accordingly.

Access management

Robust access management is in place across the organization's corporate systems and data. This utilizes industry leading authentication solutions and multi factor authentication is a requirement for all access.

The principles of 'least privilege' and 'need to know' is applied to all employee access which is regularly reviewed. Third party access is only permitted where third parties can demonstrate security posture and controls that meet or exceed those of Precisely's own policies and standards.

Equipment security

Equipment is configured, maintained, and is hardened (where possible) in line with vendor and industry best practice guidance. Anti-malware is deployed across the estate and is maintained with up to date definitions and a comprehensive program of asset management is in place to ensure the security of corporate equipment.

Business Continuity and Disaster Recovery

A regimen of business continuity and disaster recovery is in place across the organisation to ensure that it is ready to respond to a business continuity and/or disaster recovery event. Business continuity and disaster recovery is planned and is periodically tested at all levels of the business.

Vendor security management and compliance

A range of industry leading partners and vendors are used to support our products and services. A comprehensive vendor security management program is in place to ensure the same robust security requirements are in place throughout our supply chain. This involves a full lifecycle security oversight program. Critical suppliers are required to maintain industry recognised security certification for the scope of the services provided.

Information Security Incident Management

Our security incident management processes are robust and are tested to ensure a state of readiness. From planning to completion our approach ensures that we can quickly respond and recover from a security incident whilst minimising impact to products and services.

Systems development life cycle

Security cannot be considered without an effective systems development life cycle.

Our approach to a secure systems development lifecycle is to use a consistent methodology across the development teams. While not every project will be administered in the exact same way, the systems development life cycle has the primary functions to ensure that quality and security are a part of every product delivered to our customers.

The systems development lifecycle is a framework for consistently planning and managing current and future product releases. No matter the size of the initiative, the lifecycle can be used for the creation of new external or internally facing products.

There are six steps within the systems development lifecycle:

- **Plan**: Research by a product manager on the composition of needs including architectural and user experience design, operating environment needs and performance goals.
- **Code**: building the product using the OWASP, NIST frameworks.

- **Test**: Test automation, user validation, quality assurance.
- **Build/Release**: release packaging by release candidate (staging, prerelease, formal)
- **Cert**: Is defined in the review the goals defined in the product planning stage, quality, and performance metrics to gain approval to move the release forward.
- **Run**: base of packages, upgrade service.

Within these six steps, guidance for the planning, coding and testing for security within the application is necessary to support the delivery of products, that protect company and customer data.

Precisely's agile methodology follows the scrum approach to development and the methodology centres on a set of phases (epics) and activities (stories) for the development team to continuously be involved in. The approach is based on three principles:

- **Workflow** - visualising how the steps in a process interact with each other.
- **Work in Progress** - focus on what needs to occur to limit the scope of the overall effort.
- **Continuous Development** - based on resource capacity to continuously develop, test and release.

The overall goal is meant to bring the developer and end user closer together to architect and design business needs.

Oversight measures are included in the methodology to determine the impact and effectiveness of the initiative.

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

- Detailed code reviews are performed for all updates to EngageOne™ Communicate. 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. Issues must be resolved before deployment is allowed.
- 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.

EngageOne™ Communicate specific security controls

This section describes the security controls specific to EngageOne™ Communicate.

Data handling

Data handling applies to both the data uploaded by users for use in communications and the analytics data captured by EngageOne™ 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.
- Authorized EngageOne™ staff, when carrying out routine operational procedures, may require access to client data. These staff are authorized by management and require specific administrator privileges. Note that the EngageOne™ Software makes no use of the data.

Program for identification of vulnerabilities

EngageOne™ Software uses a range of industry leading tools to carry out composition analysis, SAST and vulnerability scanning.

All changes are subject to peer code review prior to deployment to production.

Findings for vulnerabilities that have been identified are prioritised by risk and remediated in line with EngageOne™'s security standards.

Secure design and development

Static application security scans

EngageOne™ Software performs static code analysis on proprietary source code. Vulnerabilities are remediated in line with EngageOne™'s standard.

Open source

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 in line with EngageOne™'s standard.

External penetration testing

EngageOne commissions a third-party to perform an annual penetration test. The tests try to discover any security weaknesses in the EngageOne™ Communicate that would be useful to a malicious actor trying to gain access to the application or disrupt services. This is run on a replica of the production environment. The findings are analyzed and fixed in line with EngageOne™'s standard.

The results of the test are dependent on individual client requirements, as not all services are the same. The penetration test report is not shared, but a letter of attestation can be provided on request.

Security patch availability

AWS is responsible for patching the resources used by EngageOne™ 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 EngageOne™ Communicate code base and development environment.

Access control for EngageOne™ Communicate

Note: This describes how users access the EngageOne™ Communicate application. For details of how EngageOne™ Software staff access the backend system, see **Logical access controls** on page 13.

- 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).

EngageOne Communicate uses Role Based Access Control to ensure that user access is managed using the principle of least privilege. Roles are administered within EngageOne Communicate.

Access controls on components

The roles configured for software components in EngageOne™ Communicate Software follow the principle of least privilege.

Encryption

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

Data at rest

The database (including the replicas made for backup purposes) is 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 and other data sources. These passwords are encrypted at field level using KMS custom keys.

Communication security

EngageOne™ provisions infrastructure using segregated networks and firewalls. This is configured to deny traffic by default. An allow list is applied that only permits authorised protocols and ports to exchange data across network boundaries.

Intrusion Detection/Intrusion Prevention

EngageOne™ utilizes **AWS GuardDuty** to provide continuous threat detection.

Logging and monitoring

Privileged access activity and security events are logged securely via AWS CloudTrail. Security events are analyzed to identify suspected and detected breaches.

Data center secuirity

EngageOne™ Communicate is hosted on AWS. AWS maintains certification to the standards shown in **https://aws.amazon.com/compliance/iso-certified/** for the scope of their hosting.

Change management

Changes to production systems follow a change control process in which changes are documented and authorised by management. All changes have a roll back plan to be exercised if the change did not get deployed as intended.

Amazon Web Services (AWS)

EngageOne™ 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™ 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**.

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

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 EngageOne™ 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 uses 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. EngageOne™ Communicate regularly reviews 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 EngageOne™ Communicate, and ensuring that there is no disruption to the service provided to clients. This is automatically handled through AWS Lambda.

> **Note:** EngageOne™ is responsible for applying patches and security updates to the EngageOne™ Communicate code base and development environment.

Business continuity and disaster recovery tests

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

Anti-virus software

Anti-virus software is installed on employee machines that are used to connect to AWS infrastructure.

Logs

- Logs are stored 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 is restricted only to users who require it.
- The logs are read only.

Databases

Database management

Data is segregated by tenant.

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.

Notices

1700 District Ave Ste 300
Burlington, MA 01803-5231
USA

www.precisely.com