Time To Reply

Security and Privacy Document

TIMETOREPLY.COM

General Information

Time To Reply is a cloud-based email analytics tool that shows businesses how long it takes their staff to respond to emails, the volumes of email which they are dealing with and a whole range of productivity and workload related metrics

The system works by ingesting email header information and processing this information to produce email reply time, productivity and workload management reports..

Time To Reply Limited is ISO 27001 certified. ISO/IEC 27001 is an information security standard, part of the ISO/IEC 27000 family of standards, of which the last version was published in 2013, with a few minor updates since then. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee. ISO 27001 is comparable to the United States SOC 2 certification.

Time To Reply is an approved Google App having undergone an independent security audit by Bishopfox.com (one of three Google nominated cyber security auditing companies). The official testing letter can be viewed here: https://timetoreply.com/wp-content/uploads/2020/06/Timetoreply-Security-Assessment-2020-Testing-Letter-20200310-SIGNED.pdf

Comparative	SOC 2	ISO 27001
Governing Body	American Institute of Certified Public Accountants (AICPA)	ANSI-ASQ National Accreditation Board (ANAB)
Origination	USA	UK
Assessor Requirements	Certified Public Accountant (CPA)	Qualified Security Assessor (QSA)
Structure	Principles and Criteria	Information Security Framework
Scope	The Services Provided to End Users; Includes Infrastructure, Software, Data, People & Procedures Relevant to those Services	The Information Security Management System (ISMS)
Focus	Controls to meet Trust Services Criteria based on design (Type 1) and operation (Type 2)	Policy and Processes to establish, implement, maintain and improve an ISMS based on design only
Assurance Coverage	Security; Optionally includes Availability, Privacy, Confidentiality & Processing Integrity	Security Only
Assurance Approach	Flexible; The Service Organisation (you) decides on the attestation audits to report on control design (Type 1) and operating effectiveness (Type 2) for a chosen date or period of time. This is usually influenced by the end user requesting the SOC 2 report(s)	Pre-defined; An initial certification is followed by a 3-year period of surveillance audits to maintain the certification
Period	Point in time or period of time	Point in time only
Deliverable	A Report including the System Description, controls to meet the Trust Services Criteria, tests performed by the auditor (Type 2 only) and the auditor and service organisation attestations.	A 1-2-page certification document confirming the organisation has met the requirements for certification.
Practitioner Opinions	SOC 2 provides a higher level of assurance by confirming the operating effectiveness of controls over a period of time.	ISO 27001 follows best practice, in contrast to SOC 2 which follows good practice.
	SOC 2 is more relevant to customers as its scope is focused on the systems and services provided to those customers.	ISO 27001 certification is harder to achieve than a SOC 2 Report.
	There's a higher level of quality in the SOC review process as it requires a CPA certified firm completing the assessment.	
	The flexibility with SOC 2 Scope, timing and approach can limit the assurance provided to customers.	

ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific and detailed requirements which need to be met. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.

To view Time To Reply Limited's ISO 27001 certificate, follow this link:
https://timetoreply.com/time-to-reply-iso27001-2013/

For detailed information on our risk and information security policies please view:
ISMS INFORMATION SECURITY MANUAL
https://timetoreply.com/001-information-security-manual/

To view our Data Protection Policy please view:
DATA PROTECTION POLICY
https://timetoreply.com/data-protection-policy-mss-dp-doc-11-1/

How Time To Reply works at the data level

Time To Reply works with o365, Gmail/GSuite, IMAP, MS Exchange and Mimecast. Depending on which one of these options is chosen, Time To Reply works differently in terms of how it ingests the data, the procedure required to add a mailbox, and how it connects to those mailbox(es). Each option is explained in this document.

Once the data has been ingested, the data resides on Time to Reply's Amazon Web Services (AWS) servers. The data is stored in a database that is not accessible via the public internet. Data is encrypted and the keys are stored in a separate database. Data that is transferred between Time to Reply and 3rd parties such as the Gmail API, o365 API, Mimecast API or Nylas API is done so over SSL.

Time To Reply only views and stores the header information of emails. Time To Reply does not view, or store the body or attachments of any email.

The email header information includes the following:

- TO, FROM, CC
- Subject line
- Timestamps
- Message ID, Conversation ID used to link conversations
- Other non-sensitive META information

o365

In order to ingest email from an o365 mailbox Time to Reply connects via the MS Graph API using OAuth 2.0 protocol (https://graph.microsoft.com).

To add a mailbox, the user simply enters an Agent's name and email address, and then clicks "Add". Note: no password is required.

An email will be sent to the email address that has been added, and which includes an "activation" link. The owner of the email address would be required to click the activation link, follow the steps to grant permission to Time to Reply, and Time to Reply's software begins tracking their email performance.

An alternative option is to use Time To Reply's o365 Bulk Add option. This allows the user to authenticate once with an o365 admin user's credentials, "tick" the mailboxes they would like to track, and then add them to Time To Reply without each mailbox needing to authenticate one-by-one.

The scopes timetoreply requests for adding mailboxes one-by-one are:

offline_access User.Read Mail.ReadBasic (for paid o365 accounts)

Or

offline_access User.Read Mail.Read for "free Microsoft" accounts

For o365 Bulk-Add (adding multiple mailboxes in one go) Permissions

timetoreply™ asks for: offline_access User.ReadBasic.All Directory.Read.All Mail.ReadBasic.All

Permission reference:
https://developer.microsoft.com/en-us/graph/docs/concepts/permissions_reference

User.read.all: Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.

Directory.read.all: Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.

Mail.ReadBasic: Allows the app to read email in user mailboxes. Allows the app to read email in the signed-in user's mailbox, except for body, bodyPreview, uniqueBody, attachments, extensions, and any extended properties. Does not include permissions to search messages.

o365 Individual Add Permissions

timetoreply™ requires: Offline_Access, User.Read, Mail.ReadBasic

Gmail / GSuite

In order to ingest email from a Gmail/Gsuite mailbox Time to Reply connects via the Gmail REST API using OAuth 2.0 protocol (https://developers.google.com/gmail/api/guides/).

To add a mailbox, the user simply enters the Agent's name and email address and then clicks "Add". Note: no password is required.

An email will be sent to the email address that has been added, and which includes an "activation" link. The owner of the email address would be required to click the activation link, follow the steps to grant permission to Time to Reply, and Time to Reply's software begins tracking their email performance.

The scope that Time To Reply uses from the Gmail API is:

https://www.googleapis.com/auth/gmail.metadata

Read resources metadata including labels, history records, and email message headers, but not the message body or attachments.

https://developers.google.com/gmail/api/auth/scopes

IMAP

In order to ingest email from an IMAP mailbox, Time to Reply connects to the mailbox in the same way as Outlook / Mac Mail does.

To add a mailbox, Time to Reply requires a username and password, a mail server address and a port number. The password is encrypted and stored separately from the encryption key.

Microsoft (MS) Exchange

In order to connect to MS Exchange mailboxes (self hosted or cloud hosted) Time to Reply uses a 3rd party service called Nylas. Nylas is an API service that allows services such as Time To Reply to access MS Exchange mailboxes securely. Their security document can be found here: https://www.nylas.com/security/.

To add an MS Exchange mailbox, a user would need to enter their mailbox username, password and mail server address. These credentials are entered into the Nylas system and are stored by Nylas and not by Time To Reply. Time To Reply has no access to these credentials which are securely stored within the Nylas secure environment.

Once the mailboxes have been added, Time to Reply polls the MS Exchange mailboxes and analyses the email header information.

Mimecast

In order to ingest email header information from Mimecast, Time to Reply connects to Mimecast via their API.

This connection option is currently in invite-only beta. Please contact support@timetoreply.com for more information.

Security Overview

Enterprise-grade security and privacy controls are at the heart of the Time To Reply's infrastructure and cloud platform. Time To Reply strives to earn customer trust by enforcing world-class security practices and standards. We keep customer data both private and secure through a multi-layered physical and network-level security hierarchy. This document details all of these platform security procedures and processes. For direct inquiries, please contact support@timetoreply.com

Time To Reply is in no way involved in the email flow and has no effect on the successful or unsuccessful delivery of emails. User's email will continue to perform as normal, and independently of Time To Reply.

Transparency

Time To Reply adheres to a high level of operational excellence. Time To Reply has multiple interlocking policies for incident response, audits, and privacy. We believe security practices should be transparent to customers, and these measures are outlined below.

Incident Response Policy: As part of our basic service to all customers, all Severity Level 1 and Business Critical incidents are closely monitored and responded to 24/7, 365 days a year. Our dedicated Infrastructure Security teams are constantly monitoring both our infrastructure, as well as alerts from upstream vendors, throughout all our Operation Centers. We use notification and alert systems to immediately identify and manage risks and threats. Time To Reply network status and incidence reports are posted on the live site and on the dashboard should we experience any Severity Level 1 and Business Critical incidents

Privacy Policy: The Time To Reply Privacy policy is publically accessible at https://timetoreply.com/privacy-policy and strictly adhered to by all Time To Reply agents and employees. All Time To Reply employees undergo a rigorous background check, and are given

job-specific scoped access to our private VPN and backend infrastructure. No root credentials for backend infrastructure are ever assigned. Only Time To Reply employees that require customer data access as a necessary part of their job function are permitted access to encrypted customer data, and only upon manager approval. These groups include our customer support, development, and infrastructure security teams. All Time To Reply employees are trained on our policies, and notified of ongoing updates.

Audit Policy: Time To Reply uses https://portswigger.net/burp to scan our systems for security vulnerabilities. All access to production clusters is logged and audited regularly. The production cluster is accessible only to Time To Reply operational staff and engineers, whose primary responsibility is the construction and maintenance of the Time To Reply software system. We also perform regular security audits of our own code, third-party libraries, and our infrastructure automation. We update any software dependencies we have, so as to remain up to date with all the latest security patches at all times.

Encryption and Access Control

Time To Reply utilizes multiple application-level security mechanisms and features to ensure customer data safety. Each account's data set is isolated with multi-level permission checks. All API calls require OAuth2 authentication tokens only granted by Microsoft, Google or Nylas, and user data is encrypted.

OAuth: Time To Reply ensures user information and identity protection through our adherence to the OAuth protocol. User Authentication to email back-ends (i.e. Gmail, Microsoft Exchange) is completed via OAuth2 where possible, and encrypted password-based Auth otherwise. OAuth2 is the top industry-standard secure authentication protocol that provides developers with individual revocable tokens per e-mail account.

SSL: Time To Reply uses TLS 1.2 to encrypt bidirectional session traffic between our application and our end users' browser.

Customer Data Backups: Time To Reply does not keep backups of customer data. In the event of a loss of data Time To Reply will re-ingest your account data directly from your mail server. It is the customers' responsibility to backup their own mail server data. As long as the data is on their mail server Time to Reply will be able to restore users' email analytics data on Time To Reply.

Role-Based Access: Time To Reply has procedures and controls in place to appropriately limit access to customer data and mitigate the risk of insider threats. Access is granted on a least-privilege basis and all requests require management approval. All access is logged and regularly audited to ensure policies are followed. Customer data may be accessed in the event

that a customer account enters a failure state that requires accessing email data for debugging purposes. This data is not accessed for debugging unless an error cannot be resolved without doing so; all private data is excluded from system logs.

Network Transport and Storage

Time To Reply implements best practices for maintaining service-wide network security. We deploy the latest technology to provide uninterrupted service and guard against attack. Internal sync infrastructure is isolated from the public Internet within separate VPCs, blocking all inbound connections and persistence and storage layers are encrypted and secured behind VPN and firewalls.

Network Firewalls: Time To Reply adheres to industry standard practices for securing and maintaining our infrastructure, with additional protection being afforded by our firewalls. Each system uses firewalls to restrict access from external networks and between systems internally. To mitigate both internal and external risk, access is restricted to only the ports and protocols required for specific business needs.

Denial-of-Service (DOS) Prevention: Time To Reply implements best practices for preventing DoS attacks and uses Cloudflare to assist in preventing DoS attacks: https://www.cloudflare.com/ddos/

Distributed Denial-of-Service (DDOS) Prevention: Time To Reply data centers are hosted at AWS, and AWS uses a variety of proprietary DDoS mitigation techniques to guard against the risk of attacks. In addition, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity and to ensure network availability and Time To Reply makes use of Cloudflare for additional protection: https://www.cloudflare.com/ddos/

Clustered Infrastructure: Automated systems deploy new code to Time To Reply clusters in real time, to ensure smooth transitions between software updates with no downtime.

TLS Encryption: All web traffic between the user's mail server and Time To Reply is encrypted using TLS (Transport Layer Security) to protect customer data. The only exception is if the user specifically chooses not to make use of this by connecting to IMAP without encryption. Time to Reply's systems enforce TLS communication channels over public networks, and only support certificates signed by well-known CAs. The TLS protocol provides data encryption and authentication between customer mail server and Time To Reply servers and prevents third parties from gaining illegitimate access to information.

Infrastructure and Physical Security

All Time To Reply physical infrastructure and data centers are housed in state-of-the-art secure facilities with industry standard access controls and physical security measures.

Time To Reply is hosted at Amazon Web Services (AWS) data centers, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001, and PCI DSS Level 1.

SSAE 16, or more formally, Statement on Standards for Attestation Engagements No.16, is key guidance for reporting on internal controls for service organizations. SSAE 16 is used for reporting on the Service Organization Control (SOC) framework, which consists of SOC 1, SOC 2 and SOC 3. SOC 1 is focused toward an organization's internal controls over financial reporting, while SOC 2 and SOC 3 cover reporting for the security, availability, processing integrity, confidentiality and privacy for service organizations, including cloud and data center providers.

AWS is certified to ISO 27001, which describes a systematic approach to managing sensitive information so that it remains secure. ISO 27001 covers a risk management process that encompasses people, processes, and IT systems. AWS is also Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS), enabling customers to run applications on AWS's PCI-compliant infrastructure for storing, processing, and transmitting credit card information in the cloud.

Additional AWS physical security measures include:

24x7 Surveillance: At each AWS hosting site, Time To Reply servers are secured at all times by trained security guards, and access is authorized strictly on a least privileged basis. The data centers use state-of-the-art electronic surveillance to monitor any suspicious activity.

Security Logs: AWS CloudTrail provides logs of all user activity to the Time To Reply servers. Time To Reply employees can monitor and track what actions were performed on each of the Time To Reply resources, and by whom.

SSH Access: Time To Reply have no access using username and password, and can only access the server through SSH by using a security key. Any other SSH access is disabled.

Multiple Redundancy Zones: AWS spans multiple geographic regions and Availability Zones, which allow Time To Reply servers to remain resilient in the event of most failure modes, including natural disasters or system failures. In addition, each AWS data center has independent power grids, as well as redundant power, HVAC and fire suppression systems. The AWS data centers use state-of-the-art practices for fault tolerance at each level of the system infrastructure, including Internet connectivity, power and cooling.