CallTrackingMetrics

Security Overview

Introduction

Thousands of companies around the world rely on CallTrackingMetrics' cloud communications platform to exchange millions of calls and messages.

Providing reliable reporting and communication channels is only the first step. CallTrackingMetrics services must also follow the latest security best practices and comply with strict privacy regulations and corporate policies. The information contained in this document is intended to provide transparency on CallTrackingMetrics' security processes.

The framework for CallTrackingMetrics' security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of our Customer Data. CallTrackingMetrics' Security and Privacy Program follows a framework based on the AICPA Trust Services Categories and Criteria (SOC2) guidance. It includes programs covering: Policies and Procedures, Asset Management, Access Management, Physical Security, Operations Security, Communications Security, Business Continuity Disaster Recovery Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response.

Security Certifications and Attestations

CallTrackingMetrics holds the following security-related certifications and attestations:

SOC 2 Type 1: Security, Confidentiality, Availability (Type 2 In Progress)

Governance Strategy

Security is managed at the highest levels of the company, with the CallTrackingMetrics Security Team meeting regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by this Team at least annually and are made available to all CallTrackingMetrics employees for their reference via the company intranet.

These policies and procedures are in place to guide employees in information security administration processes, including, but not limited to acceptable usage, access provisioning, password management, change management, incident response, physical access procedures, confidentiality, data retention and classification.

A strong top-down security culture at CallTrackingMetrics governs the security charter and key goals are defined and communicated to all stakeholders across the organization.

CallTrackingMetrics uses a risk management approach to select and develop these control activities. After relevant risks are identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the overall objectives of the organization.

Hosting Architecture and Data Segregation

CallTrackingMetrics Services are hosted on Amazon Web Services (“AWS”) in the United States of America and the European Union and protected by the security and environmental controls of Amazon. The production environment within AWS where the CallTrackingMetrics Services and Customer Data are hosted are logically isolated in a Virtual Private Cloud (VPC). Customer Data stored within AWS is encrypted at all times. AWS does not have access to unencrypted Customer Data. More information about AWS security is available at the AWS Cloud Security and Shared Responsibility Model webpages.

For AWS SOC Reports, please see SOC Compliance FAQs.

Production and non-production networks (i.e. staging, test, development) are segregated. All network access to production hosts is restricted using firewalls and other access controls to only allow authorized services to interact with the production environments. CallTrackingMetrics separates Customer Data using logical identifiers. Customer Data is tagged with a unique customer identifier that is assigned to segregate Customer Data ownership.

People Security

All candidates must pass background checks by a third party before being offered a position. These checks include SSN trace, criminal county search, multi-state instant criminal search, National Sex Offenders Public Registry, professional references, and education verification.

At least once per year, CallTrackingMetrics employees must attend an annual security training which covers CallTrackingMetrics security policies, security best practices, and privacy principles. CallTrackingMetrics’ dedicated Security Team also performs phishing awareness campaigns and communicates emerging threats to employees. The Security Team provides continuous communication on emerging threats and communicates with the company regularly.

Confidentiality

CallTrackingMetrics has controls in place to maintain the confidentiality of Customer Data in accordance with our Terms of Service, Privacy Policy and Data Protection Addendum. All CallTrackingMetrics employees and contract personnel are bound by internal policies regarding maintaining the confidentiality of Customer Data and are contractually obligated to comply with these obligations.

Change Management

CallTrackingMetrics has a formal change management process it follows to administer changes to the production environment for the Services, including any changes to its underlying software, applications, and systems. Each change is carefully reviewed and evaluated in a test environment before being deployed into the production environment for the Services. All changes, including the evaluation of the changes in a test environment, are documented. A rigorous assessment is carried out for all high-risk changes to evaluate their impact on the overall security of the Services. Deployment approval for high-risk changes is required from the correct organizational stakeholders. Plans and procedures are also implemented in the event a deployed change needs to be rolled back to preserve the security of the Services.

Encryption

CallTrackingMetrics uses AES-256 encrypted storage for data at rest within the cloud environment and Customer Data is encrypted when in transit between Customer's software application and the Services using TLS v1.2 or greater.

Vulnerability Management

CallTrackingMetrics maintains controls and policies to mitigate the risk of security vulnerabilities that balances risk and the business/operational requirements. CallTrackingMetrics uses a third-party tool to conduct vulnerability scans regularly to assess vulnerabilities in CallTrackingMetrics' cloud infrastructure and corporate systems. Critical software patches are evaluated, tested, and applied proactively. Operating system patches are applied through using automation tools and deployed to all nodes in the CallTrackingMetrics cluster over a predefined schedule.

Penetration Testing

CallTrackingMetrics performs penetration tests and engages independent third-party entities to conduct application-level penetration tests. Security threats and vulnerabilities that are detected are prioritized, triaged, and remediated promptly.

Access Controls

To minimize the risk of data exposure, CallTrackingMetrics follows the principles of least privilege through a Team-based-access-control model when provisioning system access. CallTrackingMetrics personnel are authorized to access Customer Data based on their job function, role, and responsibilities, and such access requires approval. Access rights to production environments that are not time-based are reviewed at least semi-annually.

An employee's access to Customer Data is promptly removed upon termination of their employment. In order to access the production environment, an authorized user must have a unique username and password and multi-factor authentication enabled. Before an engineer is granted access to the production environment, access must be approved by management and the engineer is required to complete internal training for such access including training on the relevant Team's systems.

CallTrackingMetrics logs high risk actions and changes in the production environment. CallTrackingMetrics leverages automation to identify any deviation from internal technical standards that could indicate anomalous/unauthorized activity to raise an alert within minutes of a configuration change.

Third Party Security

Third-parties used by CallTrackingMetrics are assessed before onboarding to validate that prospective third parties meet CallTrackingMetrics security requirements. CallTrackingMetrics periodically reviews each vendor in light of CallTrackingMetrics security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal or regulatory requirements. CallTrackingMetrics ensures that data is returned and/or deleted at the end of a vendor relationship. CallTrackingMetrics enters into written agreements with all of its critical vendors which include confidentiality, privacy, and security obligations that provide an appropriate level of protection for Customer Data that these vendors may process.

Service Continuity

Service can be failed over to another region of the third-party cloud hosting provider if required. Separately, the CallTrackingMetrics application hosts are configured in clustered configurations in multiple availability zones to mitigate against single points of failure and provide high availability. These high availability/disaster recovery (HA/DR) technologies, together with full database backup, database redundancy and archiving processes, ensure key systems are available and mitigate against the risk of data loss.
Backup systems for critical applications are regularly tested to ensure there is adequate capacity to store relevant information and that the ability to restore critical data is in place. CallTrackingMetrics performs daily backups of Customer Data which is hosted on AWS's data center infrastructure. Customer Data that is backed up is retained redundantly across multiple availability zones and encrypted in transit and at rest using the Advanced Encryption Standard.

Business continuity and disaster recovery plans are in place and reviewed and tested at least annually to ensure readiness in the event of a breach or emergency to reduce financial, operational, and reputational risk. CallTrackingMetrics' implemented contingency plan reduces the risk of CallTrackingMetrics being unable to resume normal operations after a disaster or emergency.

Active monitoring and regular reviews of logs have been implemented to proactively identify issues and problems and reduce the risk of negative consequences to the organization.

Incident Management

CallTrackingMetrics maintains an incident response program in accordance with NIST 800-61. The program defines conditions under which security incidents are classified and triaged. The Security Team assesses the threat of all relevant vulnerabilities or security incidents and establishes remediation and mitigation actions for all events. Security logs are maintained for 180 days. Access to these logs is limited to the Security Team.

CallTrackingMetrics will promptly investigate a Security Incident upon discovery. To the extent permitted by applicable law, CallTrackingMetrics will notify Customer of a Security Incident in accordance with our Data Protection Addendum. Security Incident notifications will be provided to Customer via email to the email address designated by Customer in its account.

Questions?

For further details and steps to secure your CallTrackingMetrics account, check out our knowledge base which provides additional guidance for customers needing to be HIPAA, GDPR, CCPA and PCI compliant.

Visit our Knowledge Base