Security Whitepaper

Introduction

C2FO delivers a scalable application with high availability and dependability. Protecting the confidentiality, integrity and availability of our customer's data is of the utmost importance to C2FO, as is maintaining customer trust and confidence. This document is intended to summarize C2FO's standards compliance, security framework and operational practices.

C2FO Compliance

SOC Compliance

C2FO has implemented effective controls for all required SOC 1 and SOC 2 criteria. An independent audit is conducted annually to ensure continued compliance. The most recent SOC 3 report is publicly available here on our website. The most recent SOC 1 and SOC 2 reports are available upon request.

Penetration Testing

Internal and external penetration tests are conducted annually by an independent security organization. Any vulnerabilities found are documented and immediately remediated. Post mortem analysis is performed to identify root cause and implement future controls.

C2FO Customer Data

Encryption

All customer data is encrypted in transit and at rest using one or a combination of the following algorithms and/or protocols:

- AES-265
- SHA-256
- 3DES
- Blowfish
- TLS
- PGP
- AWS KMS
- Google KMS

Content

C2FO only requires a summarized list of accounts payable. The summary is broken up into six files:

- Award
- Control
- Division
- Invoice
- Organization
- User

Details for the content and format of these files can be made available upon request.

Transmission

C2FO provides a number of secure options for the transmission of customer data, all of which encrypt data in transit.

- SFTP
- AS2

Storage

All customer data is logically separated and stored encrypted in AWS. C2FO employs security methods which prevent customers from accessing anything but their own data.

Amazon Web Services (AWS) Compliance and Infrastructure

C2FO utilizes AWS for hosting its systems and services. This section is intended to summarize the security and high availability features and infrastructure AWS provides.

Compliance

C2FO reviews AWS's compliance reports annually. To date, AWS is compliant with the following standards:

- SSAE16 / ISAE3402 (formerly SAS70)
  - SOC 1
  - SOC 2
  - SOC 3
- FISMA
- DIACAP

- FedRAMP
- DOD CSM Levels 1-5
- PCIDSS Level 1
- EU Model Clauses
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- ITAR
- FIPS 140-2
- MLPS Level 3
- MTCS
- CJIS
- CSA
- FERPA
- HIPAA
- MPAA

Physical Security

AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Redundancy

AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. Data centers are built in clusters in various global regions. All data centers are online and serving traffic; no data center is “cold.” In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Fire Detection and Suppression

Automatic fire detection and suppression equipment are installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Generators are used to provide back-up power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. AWS data centers are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

System Monitoring

AWS monitors all support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Google Cloud Platform (GCP) Compliance and Infrastructure

C2FO utilizes GCP for hosting its systems and services. This section is intended to summarize the security and high availability features and infrastructure GCP provides.

Compliance

C2FO reviews GCP's compliance reports annually. To date, GCP is compliant with the following standards:

- SSAE16 / ISAE 3402 Type II

    - SOC 1
    - SOC 2
    - SOC 3
- ISO 27001
- ISO 27017
- ISO 27018
- FedRamp ATO for Google App Engine
- PCI DSS v3.1
- CSA STAR
- HIPAA
- MPAA
- EU-US Privacy Shield Framework

Physical Security

Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. GCP data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Only approved employees with specific roles may enter. Less than one percent of Google associates will ever set foot in a Google data center.

Logical Security

Google logically isolates each customer's Cloud Platform data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Google associate access is monitored and audited by dedicated security, privacy, and internal audit teams.

Redundancy

Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are automatically and instantly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps customers protect themselves from data loss. Cloud Platform

resources can be created and deployed across multiple regions and zones. Allowing customers to build resilient and highly available systems.

Power, HVAC, Fire Suppression & Detection

Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.

Hardware Tracking & Disposal

Google meticulously tracks the location and status of all equipment within its data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired.

Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical \destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility.

System Monitoring

Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across Google's global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.

C2FO High Availability Strategy

The objective of this section is to highlight just some of the steps C2FO has taken to deliver high system availability. Our systems are designed and engineered with the goal of minimizing or eliminating critical points of failure. This means that no single component failure will disable the entire system or even large parts of the system for any appreciable amount of time. Even the unlikely event of simultaneous multiple component failures should not disable a large portion of our systems.

Redundant Facilities

At the heart of C2FO's approach to high availability and business continuity are redundant facilities. All of our systems and data are replicated to secure facilities in separate geographic areas.

Telephone Infrastructure

Our primary phone systems are VOIP-based and provided by a best-of-class vendor. C2FO is able to route incoming calls to any end point destination. The full system, including message backups, have redundant storage, network connections, and battery backups.

Internet and LAN Security

Enterprise level Internet services are provided at C2FO's headquarters, with redundant ISPs and dedicated fiber circuits. Services are monitored and protected by industry leading application delivery controllers. Internet security is provided by redundant firewalls and an IDS.

Database Management

C2FO deploys scalable database systems across multiple availability zones and regions. Each zone is geographically separated to avoid a single point of failure, and data replicates to all zones in real time.

Mass Storage Systems

C2FO uses mass storage data systems built in clusters, capable of dynamic or on-demand expansion. These clusters are distributed among various global regions and are designed to tolerate hardware failures while maintaining required service levels.

Backups

C2FO uses a number of IAAS provided tools for backup management. All backups are encrypted in transit and at rest. Redundant backup copies are stored across multiple availability zones and/or regions. Backup frequency and retention vary depending on the critical nature of the data and/or system.

Hardware and Infrastructure

Configuration management software is installed when new hardware is provisioned. Updates by IAAS providers are done in such a manner that, in the vast majority of cases, will not impact the customer and their service. When service may be adversely affected, IAAS providers communicate the change(s) prior to implementing.

Capacity Management

C2FO uses AWS Elastic Compute Cloud (EC2) and Google Compute Engine (GCE), which provide resizable computing capacity using server instances in state of the art data centers. EC2 and GCE make web-scale computing easier by enabling dynamic scaling with minimal friction.

Maintenance and Failure Allowance

C2FO's redundant architecture allows shutting down parts of systems for maintenance or replacement with little or no impact on our required capacity at a given time.

Our system allows for rapid expansion of system capacity should the need arise. Internet services are burstable, meaning unexpected spikes in bandwidth utilization are handled with no intervention.

C2FO Security Policy & Procedure Framework

The purpose of this section is to provide a brief overview of C2FO's security framework. Only key policies and procedures are covered in this section. All policies, not just those summarized here, are made available to all C2FO associates.

Background Checks

C2FO screens all associates prior to employment, which includes a background investigation. Issues identified during background checks are resolved prior to employment and prior to provisioning

access to C2FO systems. In addition, HR processes and stores all associates' personal and confidential information such as background investigations findings in accordance with the C2FO Information Security Policy.

Security Awareness Training

All C2FO associates are required to complete an online information security awareness training course within the first 5 days of employment, and annually thereafter. Additional training is provided, and all security policies reviewed, in the new associate IT orientation which also occurs the first week of employment. All activities and results are documented and retained indefinitely.

Information Security

At the heart of our security framework is the Information Security Policy. This policy defines what we consider to be confidential and third party confidential information, how that information can be shared both internally and externally, how and where that information can be stored, and how it is labeled. These definitions inform most other security policies as they're the basis for which we determine secure solutions and audit compliance.

Information Security Charter

The Information Security Charter consists of the CTO, an executive sponsor, the head of business services, the engineering security lead, the information security program manager and a HR representative. The Charter meets quarterly and is responsible for the oversight, review and approval of all security related policies, audits, risk assessment approval and remediation, and the general approach to fostering a secure culture at C2FO. Charter meeting activities are documented in detail and retained indefinitely.

Business Continuity

C2FO has developed different business continuity and disaster recovery plans for each critical environment. Each plan is tested annually. Test results are documented, reviewed, and retained indefinitely. Any issues that arise during testing are immediately remediated. All personnel key to each plan are given multiple copies of emergency contact cards which contain all contact information for all other key personnel and vendors.

Clean Desk & Screen

C2FO associates are prohibited from keeping any confidential or third party confidential information in view at their work area. This sensitive data is required to be kept in a locked compartment or at a minimum concealed from view. When unattended, all workstations are required to be locked and

password protected. Clean desk and screen compliance is audited regularly, and results are documented and shared with management.

Access Control

C2FO follows least privileged access practices. Formal policies and procedures exist and are strictly followed for all requests and changes. Access, both internal and external, is reviewed regularly. All access requests, changes and review results are documented and retained indefinitely.

Risk Management

C2FO conducts an internal risk assessment annually to identify, prioritize and remediate any known vulnerabilities. High risks are remediated immediately upon discovery. The entire assessment process is thoroughly documented and audited annually by an independent party as part of the SOC 2 process. Findings and remediation are reviewed, discussed and approved by the C2FO Information Security Charter.

Change Management

Formal change management policies, procedures, and controls are in place to prevent unauthorized and untested system changes from being made. Such changes can lead to system downtime, processing disruptions, functional problems, data loss, and integrity issues. Code, database and infrastructure change requests follow strict workflows and are thoroughly tested and documented from initial submission to deployment.

Mobile Device Management

C2FO maintains the ability to remotely wipe all data from any associate's mobile phone or tablet containing C2FO data. Devices are screened and only allowed connectivity to C2FO services after meeting security policy standards.

System & Event Logging

Access and system event logs are captured on all resources and stored in a number of repositories. Reviewing and reporting responsibilities are clearly defined, as are schedules and escalation. All logs are retained indefinitely.

Intrusion Detection System (IDS)

C2FO leverages intrusion detection to perform real-time scans and identify threats and trends. An intrusion detection alerts an on-call resource, who responds and escalates in accordance with

internal requirements. Threats, responses, remediation, and post mortem are documented thoroughly and retained indefinitely.

Intrusion Prevention System (IPS)

An industry leading, enterprise class Intrusion Prevention System is used to protect the internal network and its users. URL filtering blocks malicious websites and files using definitions updated in real-time. Undefined files and data are detonated in an isolated environment, analyzed for threats, and submitted to a definition repository.