Security Assessments and Compliance

DATA CENTERS

CFM Roadmap's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001, ISO 27017, ISO 27018
- SOC 1/SSAE 16/ISAE 3402, SOC 2, SOC 3
- PCI DSS Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)
- SEC Rule 17a-4(f)

PCI

We use PCI compliant payment processor Stripe for encrypting and processing credit card payments. CFM Roadmap's infrastructure provider is PCI Level 1 compliant.

PHYSICAL SECURITY

CFM Roadmap utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three 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.

Amazon only provides data center access and information to employees 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 and electronic access to data centers by Amazon employees is logged and audited routinely.

Environmental Safeguards

FIRE DETECTION AND SUPPRESSION

Automatic fire detection and suppression equipment has been 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

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

CLIMATE AND TEMPERATURE CONTROL

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. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

MANAGEMENT

Data center staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Network Security

FIREWALLS

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

DDOS MITIGATION

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

SPOOFING AND SNIFFING PROTECTIONS

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. CFM Roadmap utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

PORT SCANNING

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

• Data Security

DATA IN TRANSIT

- All data transmission between your computer and our servers is encrypted, using industry-standard HTTPS protocol.
- Our HTTPS implementation is rated A+ by independent Qualys SSL Labs.
- Our SSL certificate uses 2048-bit asymmetric and 256-bit symmetric encryption.
- We use HTTP Strict Transport Security (HSTS) to ensure only secure connections can be used for our website. Our website is accepted by and built in to Google Chrome, IE 11, Edge, and Firefox for this purpose.
- Our servers take advantage of Perfect Forward Secrecy (FPS) to protect data transmission for modern web browsers. With forward secrecy, all past communication confidentiality is maintained even when a long-term secret key is compromised.

DATA AT REST

All your personally identifiable information — including your name, email, address, and uploaded documents — is encrypted when we store it. Such data is encrypted using AES-256.

TWO-STEP VERIFICATION

Two-step verification secures your account by requiring something you possess (your mobile phone), in addition to something you know (your password), to access your account.

Once enabled, you'll need to enter a verification code from your mobile phone to log in. This protects your account from unauthorized access even when your password is compromised.

WE DO NOT SAVE YOUR CREDENTIALS

We partner with Envestnet | Yodlee to provide account aggregation. All of your banking credentials are managed by Envestnet | Yodlee, and we do not store your credentials. We communicate with Yodlee via an encrypted data link.

Envestnet | Yodlee is a leading data aggregation and data analytics platform powering dynamic, cloud-based innovation for digital financial services. More than 1,000 companies, including 11 of the 20 largest U.S. banks and hundreds of Internet services companies, subscribe to the Envestnet | Yodlee platform to power personalized financial apps and services for millions of consumers.

For additional information see: Yodlee's commitment to its clients and their customers.

NO ONE CAN MOVE YOUR MONEY

CFM Roadmap has read-only access to your financial accounts through Yodlee. No one (not even you) can move any money in, out or between your accounts via CFM Roadmap.

System Security

SYSTEM CONFIGURATION

System configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments. Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

SYSTEM AUTHENTICATION

Operating system access is limited to CFM Roadmap staff and requires username and key authentication. Operating systems do not allow password authentication to prevent password brute force attacks, theft, and sharing.

Vulnerability Management

Our vulnerability management process is designed to remediate risks without customer interaction or impact. CFM Roadmap is notified of vulnerabilities through internal and external assessments, system patch monitoring, and third party mailing lists and services. Each vulnerability is reviewed to determine if it is applicable to CFM Roadmap's environment, ranked based on risk, and assigned to the appropriate team for resolution.

New systems are deployed with the latest updates, security fixes, and CFM Roadmap configurations and existing systems are decommissioned. This process allows CFM Roadmap to keep the environment up-to-date.

VULNERABILITY REPORTING

CFM Roadmap takes security very seriously, and investigates all reported vulnerabilities. If you would like to report a vulnerability or have a security concern regarding CFM Roadmap services, please email . If your message contains sensitive information, please use our PGP key.

Please provide full details of the suspected vulnerability so the CFM Roadmap security team may validate and reproduce the issue.

Backups

All of your data is backed up daily. CFM Roadmap maintains at least 30 days of backup data at any given time.

In addition, we continuously take snapshots of the database. CFM Roadmap can restore data to any point in time between the earliest backup and typically within 5 minutes of the current time.

Disaster Recovery

CFM Roadmap replicates customer data to at least two different locations at any given time to protect against failure or local disaster.

The CFM Roadmap platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. Our platform maintains redundancy to prevent single points of failure, is able to replace failed components, and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. CFM Roadmap reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes.

Access to Customer Data

CFM Roadmap staff does not access or interact with customer data as part of normal operations. There may be cases where CFM Roadmap is requested to interact with customer data at the request of the customer for support purposes or where required by law. CFM Roadmap may also inspect customer data to debug and troubleshoot platform issues.