Cultivate Security and Privacy

Cultivate takes the security and privacy of your data very seriously, with robust policies, controls, and systems in place to keep your information safe and secure.

People Security

All Cultivate employees are required to understand and follow strict internal policies and standards. All employees are trained on security topics including but not limited to device security, preventing spyware/malware, physical security, data privacy, account management, and incident reporting.

Application Security

The Cultivate development team follows security best practices. All code is version controlled and goes through peer review and continuous integration tests to screen for potential security issues. Changes to the production environment are logged and the development team is notified of each release.

Authentication

Cultivate users login with their Google or Office 365 accounts using OAuth 2.0, an industry standard for authorizing secure access to external apps. Cultivate does not receive or store user passwords at any time. Users may revoke Cultivate's access at any time and also are able to request their data be deleted.

Network Security

Encryption in transit

All data in transit between users, Cultivate, and email/messaging services is encrypted using 256-bit SSL/TLS. These protocols are revised as new threats and vulnerabilities are identified.

Network Isolation

Cultivate divides its systems into separate networks using logically isolated Virtual Private Clouds in Amazon Web Services data centers. Systems supporting testing and development activities are hosted in a separate network from systems supporting Cultivate's production services. Customer data only exists and is only permitted to exist in Cultivate's production network. Network access to Cultivate's production environment is restricted. Only network protocols essential for delivery of Cultivate's service to its users are open at Cultivate's perimeter. All network access between production hosts is restricted using firewalls to only allow authorized services to interact in the production network.

Physical Security

Data center security

Cultivate's infrastructure is built on top of Amazon Web Services, and is housed in data centers operated by Amazon. Amazon has strict policies for physical security, including 24-hour video surveillance and strict access restrictions which are described in detail here: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Office security

All employee devices must meet our security standards. These standards require all computers to have strong passwords, encrypt data on disk, run anti-virus software, and lock automatically when idle. No data is stored on employee computers or servers in the office.

Data Security

Data We Collect

Upon authorization by each individual user, Cultivate collects both metadata and content of messages and events in their connected email, messaging, and calendar accounts. The content of events and messages is retained for one year from their dates, but metadata including the people involved and length of the message may be retained indefinitely. Additionally, we may store the output of classification algorithms run on individual messages indefinitely.

Data Sharing

We do not share the content of any user's messages with any party, including the user's employers, except as required by law. Your employer will have access to reports based on metadata, computed statistics, and classifications aggregated over many messages, but the content of any individual message will not be exposed.

Data Access

To the extent possible, Cultivate automates access to customer data and strictly limits viewing by humans. Only Cultivate's Chief Technology Officer and Chief Data Scientist may request permission to access customer data for essential job functions for a limited amount of time in a secure environment. All requests to access customer data must be reviewed and approved by the executive team and must have a clear technical justification.

Encryption at rest

All data at rest in Cultivate's production network is encrypted using 256-bit Advanced Encryption Standard (AES). Message content is further encrypted in our database such that the plaintext never exists on Cultivate database servers at any point in time. Cultivate uses the AWS Key Management Service (KMS) to manage encryption keys. Keys are never stored on disk and retained only in memory while in use. Encryption keys are rotated regularly.

Server hardening

Production servers are hardened, with the minimally required set of services allowed to run. A custom based server image which has been reviewed for security is used to run all production services.

Vulnerability Management

Cultivate uses third party services to run automated vulnerability tests on the production environment. Engineers are always on call to immediately address any issues.

Penetration testing

Cultivate undergoes independent black and gray box security penetration tests by third-party security firms. The findings are reviewed, prioritized, and tracked to resolution, including third-party verification of resolution.

Compliance

Cultivate is hosted in Amazon Web Services (AWS) data centers, which are certified to meet compliance requirements of SOC2 and ISO27001. Details can be found at https://aws.amazon.com/compliance/.