forethought

Agatha Security Whitepaper

Confidential

Overview

Forethought Technologies, Inc (“Forethought”). is a Silicon Valley software company founded by a team of Dropbox, Palantir, and Autonomy alumni in 2017. Our mission is to enable everyone to become a genius at their jobs.

Our flagship product is Agatha™, an answer engine for the enterprise. Agatha provides the following services:

- Unified indexing of corporate knowledge bases (including Box, Google Drive, Confluence, Sharepoint, Zendesk, Slack, and more)
- Natural Language Search + Question Answering over indexed documents
- Extensions to use Agatha inside existing workflows and tools (including Slack, Zendesk, and Google Chrome)

Agatha accelerates decision making processes and access to information for any line-of-business worker.

Architecture

Agatha is built on Amazon Web Services, Inc. (“AWS”). Forethought has implemented suggested best security practices from AWS and industry standard practices and continues to advance practices to ensure the confidentiality, integrity and, availability of customer data. Information about security and privacy-related audits and certifications performed by AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Website and the AWS Compliance Website.

Web Application Attacks

Agatha leverages the AWS platform protection against various kinds of application attacks. In addition Forethought utilizes AWS Web Application Firewall to protect against common and advanced web exploits that could affect Agatha’s availability and security. Services, protocols, and ports are restricted to just allowed services to run the service.

Intrusion Detection

Forethought reviews logs for security and performance related events. The team will monitor the services for unauthorized intrusions and other malicious activities leveraging industry tools.

Vulnerability Scans

Frequent vulnerability scans are performed. The discovery of any available security issue is logged in a vulnerability management process and remediated as deemed appropriate based on a risk assessment of the vulnerability.

Security Logs

Logs from all systems which provide service to Agatha are sent to a centralized logging service to enable security reviews and analysis for security events such intrusions and threats.

Incident Management

Forethought maintains security incident management policies and procedures. In addition AWS will be escalate to Forethought without undue delay of any unauthorized disclosure once AWS becomes aware to the extent permitted by law.

Physical Security

Production data centers used for Agatha have access system controls in place. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor access screening, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure. Further information about physical security provided by AWS is available in the AWS Compliance site.

Reliability and Backup

All data in Agatha are automatically replicated on a near real-time basis at the database layer and are backed up regularly on secure, encrypted, and redundant storage. Data in scope is models and metadata indices.

Disaster Recovery

Forethought operates Agatha in the AWS Oregon region and maintains reserved instances in the AWS N. Virginia region as a backup for the failure of Oregon. Forethought currently has business continuity and disaster recovery plans with the following target recovery objectives:

- Restoration of service within 12 hours (Recovery Time Objective)
- Maximum customer data loss of 4 hours (Recovery Point Objective)

Forethought's platform, AWS, utilizes disaster recovery facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centers were to be rendered unavailable. AWS has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to a secondary data center utilizing developed operational and disaster recovery procedures and documentation.

Viruses / Malware Protection

AWS implements practices and software to limit the risk of exposure to software viruses, malware and known indicators of compromise. In addition Forethought uses latest Amazon Machines Images (AMIs) which are hardened against industry standards. The entire system is constructed in an isolated environment and is not a general-purpose computer with new software periodical loaded that may introduce malicious code.

Data Encryption

All data in transit is encrypted using TLS.

Deletion of Customer Data

Upon termination of a customer account for any reason (such as account termination, nonpayment, or customer deletion of the account), Customer Data will be deleted in 1 week and all records purged after 30 days. This process is subject to applicable legal requirements. Customer data include document content and associated metadata.