ALLOCADIA

TRUST AT ALLOCADIA

Product Security Overview

At Allocadia, we take the processing of our customer's data assets very seriously. This is why we have built a comprehensive information security and privacy management program, designed to defend our systems and the data assets we process.

Our security practices were designed to defend the marketing plan using the same calibre of security measures that banks use to defend cash, assets, people and systems.

Security is a big part of our customer commitment. Many of the world's largest businesses have put their trust in Allocadia, and we hope yours will, too.

Product Security

At Allocadia, safeguarding customer data assets is the most important thing we do. Our security, privacy, and resiliency assurance programs are comprehensive, mature, and responsive, and designed to exceed the requirements of our global enterprise customers. From our CISO to our leadership team to each individual employee, everyone at Allocadia is committed to the security and confidentiality of your data assets.

Application Security

User Authentication

Access to the Allocadia application requires that all users authenticate themselves using the business email address (provided to them by their organization) and a secret password known only to the user. For organizations with their own identity provider, users access the Allocadia application from their SSO dashboard via a SAML 2 integration (see below).

Identity Federation through SAML

The Allocadia application supports identity federation through SAML2, providing organizations with credential centralization management capabilities through an Identity Provider under the customer's control. For organizations desiring maximum control over authentication security, Allocadia recommends SAML integration with the organization's own IdP.

Password Policy

The Allocadia application prevents users from creating weak passwords by enforcing a strong password policy for all application accounts. Any passwords set by the user must contain three of the four-character classes (lowercase, uppercase, numbers, and symbols) and must have a minimum length of eight characters. Limited customization of these complexity parameters is available within the application to allow customers the option to align complexity enforcement across their toolsets. Passwords are never stored in plain text. Instead, a bcrypt salted hash is stored in the Allocadia database. Organizations that choose to integrate with their own identity provider can enforce stronger controls, including multi-factor authentication.

Secure Data Transfer

All upstream and downstream data transfer between the user's machine and the application servers and services is done over an encrypted connection signified by the "https://" URL. The Allocadia application encryption is based on a 2048-bit SSL certificate and 256-bit encryption with only TLS v1.2+ protocols allowed with the "MEDIUM" and "HIGH" class of cipher suites (anonymous DH ciphers disabled). If a user tries to visit a non-encrypted ("http://") URL, they are redirected to the "https://" equivalent to force the encrypted connection at all times.

Session Handling

The Allocadia application is configured by default to keep the user's sessions private and secure. Once a user successfully authenticates to the Allocadia application, a session is established on the server. If no activity that requires a round-trip to the server occurs within 60 minutes, the user session expires. After such expiration, no further actions can be performed and the user will be redirected to the login page when they next attempt to perform an action. In addition to the session time-out, sessions are invalidated when a user closes their web browser, or if they explicitly log out of the application.

API Access

The Allocadia application has an Application Programming Interface (API) that is disabled by default and can only be enabled by Allocadia administrators under the customer's written authority in service of a documented and approved integration project driven and owned by the customer organization. Once enabled, each API request must contain valid credentials; any API request sent without valid credentials is discarded.

Allocadia Application Cookie Management

Cookies used by the Allocadia application:

- Secure Cookies: The Secure attribute is meant to keep cookie communication limited to encrypted transmission, directing browsers to use cookies only via secure and encrypted connections.
- HttpOnly Cookies: The HttpOnly attribute directs browsers not to expose cookies through channels other than HTTPS requests.

Authorization

The Allocadia application was designed with role-based access controls with prescribed privilege levels for users to access marketing plans in part or in whole. These rules ensure that only explicitly assigned users have access to customer data assets. The authorization rules are centered around budgets and the users who have different levels of access privilege to them, i.e., users only have access to data which has been explicitly granted by the customer. Any actions taken inside the Allocadia application are automatically checked against existing access

controls which defend the data assets; if the user's account or role does not have access privileges, the data is unavailable until the user is granted such privileges by the customer.

Protection Against Web Application Vulnerabilities

The Allocadia application is protected by active in-line security technologies which programmatically defend against web application and processing stack vulnerabilities and defects. All code is assessed against SANS 25 and OWASP 10.

Audit Trail for Application Actions

Every event in the stack generates an event log as data assets are processed and/or their state is modified. An audit log is kept for all major actions performed by users within the Allocadia application. For each action, the audit log contains the user or service which performed the action, the process which generated the event log, and a time stamp synced to the logging service. Passwords are not logged. The audit log is only accessible to Allocadia administrators; no programmatic access is available, nor are internal operations logs shipped outside the secure environment.

Quality Assurance

Allocadia's development and devops staff are regularly trained in the assembly, shipping, and governance of secure software processing stacks. In addition, to ensure regressions do not appear, a set of automated software test suites are maintained and run by the Allocadia's Dev QA team. This test suite includes both positive tests (e.g., a user should be able to access this budget) and negative tests (e.g., a user should not be able to access this budget) and is run continuously with new code changes and commits. A three-step testing process is executed against all builds prior to production promotion: (i) a security QA analysis performed by a peer; (ii) a SAST scan with no issues rated "medium" or higher; and (iii) a stack vulnerability posture assessment performed by the internal security team of the daily build. The Allocadia application source code is held in a secured private Git source code repository. Only the members of the Allocadia development team have permission to retrieve and submit changes to the source code. All access to Git is encrypted, access-controlled, and subject to regular internal audit.

Network Security

Data Centers

The Allocadia application is hosted within Amazon Web Services (AWS). AWS is a secure and reliable Infrastructure-as-a-Service hosting platform. Allocadia customers benefit from the world-class security measures that AWS employs at its data centers, ranging from the physical security of the facilities to its network, hardware, host operating systems, and virtualization services. AWS maintains dozens of current security and assurance certifications for a variety of global and national security frameworks.

Firewall & Production Access Control

The hosting environment is fronted with a load balancer and network firewall configured in deny-all mode by default. The only inbound ports open to the Internet are TCP 80 and 443 for http and https communication with the web server, respectively. All requests to TCP 80 are redirected programmatically to TCP 443; unencrypted sessions are never allowed. The firewall and WAF rules are reviewed regularly and updated as threats and risks evolve.

Remote access to the Allocadia application processing environment can only be accomplished via an SSH controlled by four-factor authentication controls. SSH runs on a non-standard port to further obfuscate itself and blocks access from everywhere other than approved and secure Allocadia corporate locations. Password-based authentication is disabled, requiring multi-factor authentication.

Encryption & Key Management Program

Allocadia is committed to ensuring secrecy, privacy, and security through the managed use of encryption technologies for data in transport and at rest. Weak cipher suites and ciphers with known cryptographic vulnerabilities are prohibited, with all key sizes enforced at a minimum of 2048 bits. Signature algorithms must be SHA256 or stronger (or equivalent strength hashing algorithm). Keys, certificates, and other encrypting artefacts are managed under the formal Key Management Process, with all access to keys and cryptographic artefacts logged and alerted against.

Web Application Firewall

Allocadia deploys a web application firewall in front of the Allocadia application which protects the web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. The WAF's ruleset aligns to and reports on OWASP 10 issues based on both standard and custom rulesets. The WAF is actively monitored, with alerts going to the security operations team in real-time for analysis and action.

Production Access Control & Management

The web application server and database server application processes run under non-root, low-privilege user accounts rather than the "root" account. The production database is run within the encrypted AWS RDS, adding additional security

layers while abstracting access through security groups and the IAM service, minimizing attack surface and authentication service presentation. Authentication into the production environment requires a jumphost IP-locked to the Allocadia HQ external IP, an active VPN account, a unique SSH host cert, an active and valid MFA token, and a valid AWS admin account.

System Security Visibility & Reporting

Allocadia deploys and manages a SIEM and log aggregation and analysis platform to monitor the production environment for deviations from baseline behavior and detect security risks before they can activate and propagate. “High” and “Critical” alerts are reviewed and actioned immediately, while non-CVE “Medium” alerts are reviewed during the weekly security stand up meeting.

Standard Server Image

Allocadia uses a standard immutable server image in the hosting environment. The image is based on Amazon Linux and includes a strong security configuration by default. In addition, standard industry best practices are employed to harden this server image, including, but not limited to, the following:

- Only the minimum required software packages are installed.
- Password-based authentication is disabled, requiring key-based authentication with passphrases.
- Web server and database server processes run under non-root, low-privilege accounts.
- File permissions are restricted for files/folders containing database data files, log files and any other files with sensitive data.

Patch Management

Allocadia updates its server images to apply the latest security and hotfixes for the operating system and application software. Patching is scheduled by issue criticality, with “Critical”, “High”, and “Medium” patches seeing fixes within industry-standard mitigation times. Occasionally a reboot is required, which is done during the scheduled maintenance window.

Platform Resiliency

Data Center Locations

Allocadia delivers the Allocadia application from AWS’ highly secure and resilient network, hardware, and processing infrastructure. Allocadia maintains both production and warm standby processing environments in each processing jurisdiction (Ireland/Frankfurt and NorCal/Virginia) in the event one region were to become unavailable. These standby environments are provisioned in separate availability zones from the production environments to ensure recoverability and continuity of service.

System Monitoring

Allocadia utilizes both internal and external monitoring solutions to check the health of its systems. When monitoring agents identify an anomalous event, appropriate security team members are notified in real-time via email, secure corporate chat, and SMS notifications.

Backup

Allocadia performs a full database backup every 30 minutes.

S3 file storage service for a minimum of three months. Daily backups are held for a minimum of one year. Backups can be retrieved and restored by Allocadia administrators when required.

Business Resiliency

Allocadia has a comprehensive business resiliency program, covering operational incident response, security incident response, disaster recovery, and business continuity. Plans are tested semi-annually, with full review and update cycles occurring annually. Allocadia has set the following objectives specifically for restoring the Allocadia application for customers in the event of a disaster:

- Recovery time objective (RTO): 8 hours
- Recovery point objective (RPO): 1 hour

© Copyright 2021, Allocadia Inc. All rights reserved. Confidential and Proprietary.