ALTVIA PRODUCT SUITE SECURITY OVERVIEW

OVERVIEW

The Altvia product suite is fully cloud-based and built upon widely trusted cloud-based Internet providers. Our products operate within a mixture of the Salesforce and Amazon AWS ecosystems and integrate with vetted third party systems as needed that include HelloSign, PostMark, Sendgrid and Twilio. Our operational policies and procedures to manage the product suite within those environments provides a highly resilient, reliable and secure product line.

WEB APPLICATION SECURITY

Our products employ numerous mechanisms to ensure security for users and data, including:

- All user access is secured by SSL/TLS and insecure connections are not permitted
- User authentication mechanisms are secured to help prevent brute force attacks, timing attacks, session hijacking and other vulnerabilities
- Secure password handling and password reset procedures, as well as up-to-date best practices for password hashing are employed
- Mitigations for web security vulnerabilities such as XSS, CSRF, SQL injection and other items such as those described by OWASP are enforced
- Third party penetration testing is used to verify overall web application security

SECURE DEVELOPMENT PRACTICE

Security in our products is maintained as new features are added through several practices:

- Automated Testing: Our products have a large automated testing suite, including coverage for security, authentication and authorization features
- Peer-Review: All application changes are reviewed by multiple team members before deployment. All changes are reviewed with security considerations in mind
- Quality Assurance: Application changes are reviewed and checked for errors by separate personnel in a staging/QA environment before deployment
- Security Analysis Tools: We utilize static security analysis tools that automatically look for security vulnerabilities (such as XSS, CSRF, SQL injection and other items such as those described by OWASP)

ADMINISTRATIVE PROCEDURES

Access to our AWS server infrastructure is highly restricted. The servers communicate with each other over a private network, with firewalls that prevent all traffic other than users from using our applications. Administrative access to these servers is only available via SSH by the minimum necessary Altvia staff connecting through a logging security gateway service. Members of the Altvia team monitor for emerging security threats through the CVE database, CERT and security lists for relevant infrastructure projects. Patches or other mitigations for security issues are applied in a timely fashion.

ARCHITECTURE AND DATA SEGREGATION

Our products leverage the Salesforce.com platform as well as AWS-based systems for storage of customer data and documents. Sendgrid (a sub-processor) and Postmark (a sub-processor) are leveraged for email message delivery and mailing statistics.

ALTVIA PRODUCT SUITE SECURITY OVERVIEW

DATA SECURITY

- Data Transmission: All data in transit is encrypted using SSL/TLS.
- Data Storage:
  - AWS: AWS file storage of customer documents uses Amazon's S3 storage service. The files are encrypted with AES256 at rest.
  - Salesforce.com: Optional Shield Platform Encryption can be used to encrypt documents stored in Salesforce as well as specific fields within structured data using AES256.
  - Postmark: Message activity/metadata/content is stored encrypted with 2048-bit RSA.
- Data Retention:
  - Our Products: Retain customer data in Salesforce and AWS infrastructure indefinitely unless deleted by customer
  - Sendgrid (Altvia Correspond Marketing Edition): Retains email message activity/metadata (such as opens and clicks) for 30 days. Stores customer's aggregated sending stats and suppression lists (bounces, unsubscribes) and spam reports (which may contain content) indefinitely, and stores minimal random content samples for 61 days
  - Postmark (ShareSecure and Altvia Correspond Investor Edition): Retains email message activity/content for 45 days. Bounced message content is retained up to a year, and bounced message activity/metadata is retained indefinitely.

INFRASTRUCTURE

Our AWS hosted applications use redundant application and database servers to ensure availability. Web traffic is routed to multiple application servers by load balancers. The application databases are continuously replicated to warm spares in geographically separate locations. This redundancy allows for minimal maintenance downtime and quick recovery in the event of server failure.

Our AWS hosted application and database servers are maintained in secure data centers with:

- SSAE 16 Type II and/or ISO 27001 certifications
- 24/7/365 hour on-site security
- Redundant and optimized transit and peering connections
- Key card and biometric access controls

AUDIT AND SECURITY STANDARDS

- Salesforce.com: ISO 27001/27017/27018. SOC1, SOC2, and SOC3 Audits
- AWS: ISO 9001/27001/27017/27018. SOC1, SOC2 and SOC3 Audits
- Sendgrid: SOC2 Type II Attestation
- Postmark: SOC2 Type I Attestation

ALTVIA PRODUCT SUITE SECURITY OVERVIEW

DISASTER RECOVERY AND BACKUP

- Salesforce.com: Redundant, geographically separate data centers. Automated data backup options from Salesforce are available as well.
- AWS: Redundant, geographically separate data centers. We have a manual disaster recovery process for our AWS-hosted applications which can typically be performed in under two hours. We have real-time replication of our databases across geographies, as well as hourly backups that are replicated across regions and cloud vendors. We also have real-time replication of documents across both geographies and cloud vendors, including incremental snapshots for varying time periods. This provides geographic diversity and data corruption protection as well. Our recovery process involves activating and scaling up our warm failover infrastructure, switching to our alternative document storage locations (if needed), and verification of the system prior to restoring service. We also utilize redundant application servers behind load balancers to protect against loss of individual servers.
- Sendgrid: Redundant, geographically separate data centers.
- Postmark: Redundant, geographically separate data centers.

MORE DETAILED INFORMATION

- Salesforce.com: https://trust.salesforce.com/en/security
- AWS: https://aws.amazon.com/security/
- Sendgrid: https://sendgrid.com/policies/security/
- Postmark: https://postmarkapp.com/why/security