Security at Aptly

Whitepaper

December 2018

Introduction

Aptly takes information security very seriously. We have invested a great deal of time, effort, and resources into ensuring that only authorized users can use the Aptly application, and that our users' information is secure.

Organizational Security

How do you assess risk?

We use a risk-based approach to information security, following the NIST standard in Special Publication 800-30, "Guide for Conducting Risk Assessments" to annually assess all possible risks to our information. The results are then reviewed by management and a corrective action plan is prepared, if necessary.

How do you screen employees?

All our employees are vetted before hire, including reference checks with former managers, and only those with a recognized business need have access to customer data. All employees receive training on security and privacy topics on a regular basis and are advised to report any potential problem to our Security Officer.

Physical Security

How do you physically secure your data?

Aptly does not maintain any of its own physical datacenters, nor is any production data or customer data stored on local media. Instead, all production data is stored and processed in a virtual private cloud (VPC) hosted by Amazon Web Services (AWS), which is Aptly's exclusive compute environment (see below under "Network Security" for more details). Customer data (the types of which are described below under the heading "Data Security") is hosted and processed by our cloud-based database and analytics providers, which, themselves, use public cloud infrastructure providers such as AWS, Google Cloud Platform (GCP), and Microsoft Azure to host their environments.

Network Security

How do you enforce network security?

All environments are hosted in a Virtual Private Cloud in Amazon Web Services, containing separate public and private subnets. No inbound internet traffic is allowed to the private subnets and all application servers only reside in private subnets without public IP addresses. Only Amazon managed and maintained load balancers have ingress access to the application servers. See Figure 1, below.

How are data transfers secured?

All internal data is transferred within our private Virtual Private Cloud, and such data never reaches the public internet. All remote access to our internal environments occurs over VPN.

All external data transfers, whether between the browser and Aptly or between Aptly and our technical partners such as Google, Microsoft, Box and Dropbox, are encrypted in transit with TLS. Once external data is transferred to Aptly it continues to be encrypted at rest using AES-256.

Are all updates to firewall rules reviewed before being deployed?

All firewall rule changes (security group changes) are reviewed by our security team before being deployed.

Do you have a process in place for timely updates of security patches?

Aptly's physical infrastructure is hosted and managed with Amazon's secure data centers and utilize Amazon Web Service (AWS) technology. Aptly consists of Platform services build and run on top of Amazon's Elastic Container service and Amazon Web Services. Aptly utilizes Amazon EC2 virtual machine and Docker isolation mechanisms. Each application instance is run in its own Docker container on an Amazon EC2 virtual machine. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II) PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

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 replace to up-to-date systems. For databases that host customer data, our managed services providers apply timely patches - which we verify and review with them. Databases are secured by standard system and authorization policies. Access to databases is restricted to authorized personnel only, for purposes of administration and support.

Data Security

What type of data does Aptly access, collect, store or transmit?

Type of information	Description
Access tokens	Aptly stores third party access tokens (e.g. Google, Microsoft) in order to access these services on behalf of users.

Name and email address	Aptly collects a user's first and last names and email address.
Browser, device and cookie	Aptly receives and records information on our server logs from your browser or device, which may include your IP address, "cookie" information, the type of browser and/or device you're using to access our Services, and the page or feature you requested.
Message content	Aptly does not store email content after the email has been sent. While a user is writing an email, the content of the draft email message is stored on our servers. Once the message is sent, we transfer the content back to the user's Gmail or Office365 account where it is stored on Google or Microsoft servers.
Contacts	Aptly stores user's contacts so that we can propose them when users are drafting emails.
Calendar	Aptly enables users to share their available times in an email. After a recipient chooses a time, we schedule the meeting on the user's Google calendar.

Is data encrypted at rest?

All data is encrypted at rest with AES-256.

Are databases backed up?

Yes.

How often?

Backups are performed nightly and tested every 14 days.

Is access to the data controlled and restricted?

Access to customer data is restricted based on role: only authorized engineering and customer success team members have access to data. Access is reviewed periodically and follows the principle of least-privilege. Access is revoked immediately upon employee termination. The database is accessible only from our Amazon Virtual Private Cloud. Access to our Virtual Private Cloud is strictly controlled and requires VPN access in addition to a secondary network access control.

What is the password policy for systems and infrastructure that is used to host customer data?

To access customer data, employees must first connect to the VPC requiring password + certificate + two-factor authentication. All passwords and access keys allowing access to client data are rotated every 3 months. Employees are required to use a secure Password Manager for all passwords allowing access to customer data.

How are access requests and approvals to internal Aptly systems tracked?

Access requests and approvals are tracked in our internal project management systems. Only the Security Officers have permissions to modify Identity and Access Management in AWS. All changes to users, roles and policies are monitored via AWS and audited monthly.

Does Aptly use a central cryptographic key management system?

Aptly uses a secure key management system for storing access keys to data warehouses. Only admins and security officers can manage cryptographic keys.

Data retention

After the end of the engagement, how long is the data held by Aptly?

Data is deleted within 30 days or upon request.

Can data be removed at customer's request and per customer's policies?

Yes. Data is automatically removed from the system when past the negotiated retention period. Data can also be optionally removed at any time per customer request.

Application Security

How is authentication managed?

All user authentication to the Aptly application is handled by secure servers. Two factor authentication will be an optional enhancement (Q1 2019) which maybe be optionally enabled. There is a detailed log of all actions available for review if needed.

Whenever made available by the third-party API, Aptly uses OAuth to connect to third-party systems that integrate with our products. OAuth credentials are easily manageable and revocable by the customer. When OAuth is not available for third-party systems, Aptly defaults to Basic Authentication with an API Key (or API Key + Secret).

Is HTTPS enforced?

Yes, and if a user reaches our website via HTTP we redirect them to HTTPS.

Do you perform vulnerability scans?

Yes, we partner with Truvantis to perform regular vulnerability scans of our platform.

Incident response

Are regular backups of data on all systems performed?

We have automated backups that make snapshots of our databases from 1 to 3 times daily.

What notification and escalation processes exist in case of a security event?

We will notify customers about any confirmed security or privacy breach as soon as possible. We provide assessment and mitigation reports within:

- 24 hours for a critical events.
- 2 business days for non-critical events.

Conclusion

Through limiting our exposure, relying on the security expertise of Google, Microsoft and Amazon, and keeping our production data strictly off-limits from local use, we reduce the risk of an accidental or deliberate breach. Our security program seeks to continually improve our risk management, whether through administrative, physical, or technical means, to give our customers the confidence they need to share data.