

Cloud Data Security

Monitor and Protect Data in the Cloud with Axway API Gateway



Axway API Gateway can monitor, secure and control API traffic to and from the cloud, so you can take control of your own data security.

For a variety of reasons, including convenience, better collaboration, and faster data movement, business users are uploading growing volumes of sensitive sales, customer and product data to consumer-grade cloud-based services — a practice that sets off alarm bells for potential violations of corporate data security and retention policies, as well as data privacy and residency regulations.

Typically, organizations are at the mercy of the service provider when it comes to operational procedures and security safeguards to protect the data at rest, in transit, and in backup. But it doesn't have to be that way. Instead of relying on questionable SAS-70 certifications or the operational discipline of the provider, Axway API Gateway empowers your organization to take control of data security in the cloud in three easy steps.

Step 1: Know what data is leaving and where it is going

The first step in taking control of cloud data security is to gain situational awareness: What data is leaving the enterprise and where is its destination in the cloud? While Data Loss Prevention (DLP) technologies do a fine job monitoring documents, including HTTP traffic, they cannot fully protect API traffic.

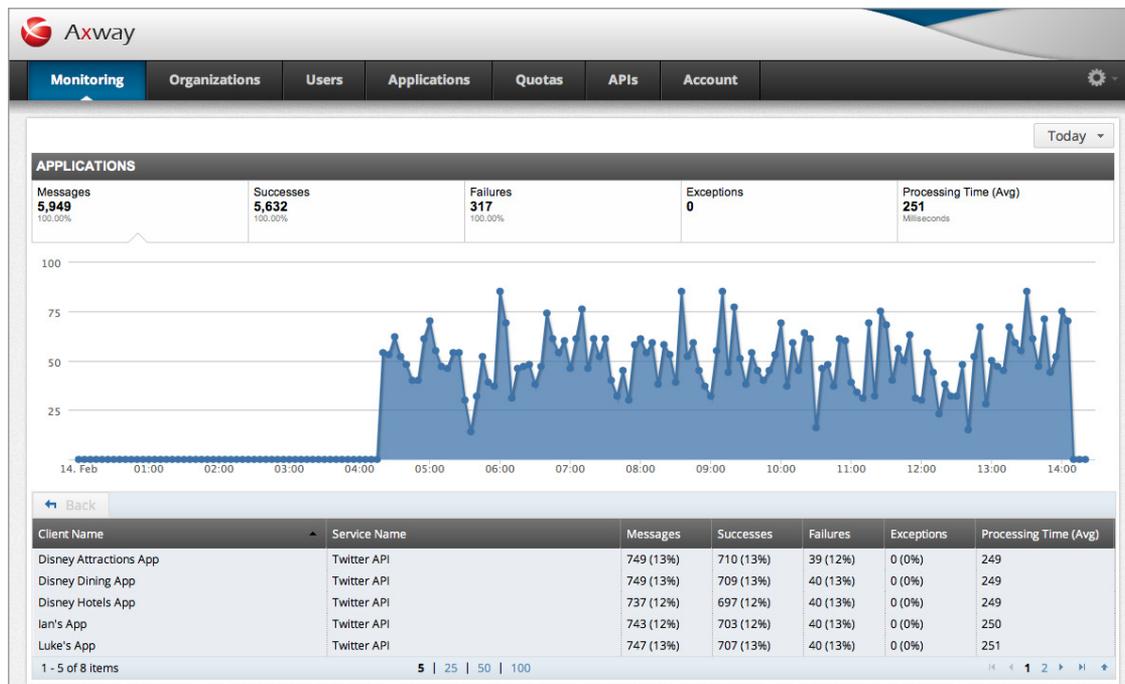
Axway API Gateway provides full data security monitoring for API traffic, covering a broad range of standard and proprietary protocols. You can use it to monitor for sensitive data not just in documents, but also in places where sensitive data may be embedded as identifiers and attributes, such as headers, query strings and resource names.

Axway API Gateway can be deployed in-line of cloud-bound traffic for both monitoring and protection, or strictly as a traffic sniffer for monitoring and alerting only.

Axway API Gateway is a next-generation technology that enables enterprises to standardize the API development and delivery capabilities required to provide business services via cloud, mobile and partner channels. Encapsulating application gateway, cloud service broker and identity middleware functionality in a unified platform, Axway API Gateway provides an agile API environment that leverages existing back-end applications, services and data to help speed time-to-market for new business services.

Axway API Management Solution Pack is a dedicated API management solution that works with Axway API Gateway to simplify all aspects of publishing, promoting and managing APIs in a secure, scalable environment.





Monitor Cloud and mobile traffic and protect data sent to Cloud services and mobile devices

Other Axway API Gateway Solutions include:

- API and SOA Security
- API Identity and Access Federation
- Application Services Governance
- Bring Your Own Device (BYOD)
- Cloud API and Service Brokering
- Cloud Identity Service
- Cloud Single Sign-On
- Fine-Grained Authorization
- Mobile API
- SharePoint Gateway

Step 2: Secure data flowing to the cloud

After gaining situational awareness, the next step is to take measures to prevent non-compliant data from moving to the cloud. Axway API Gateway can function as a cloud data security gateway that enforces privacy and residency policies by blocking, routing, removing, masking, encrypting, or tokenizing any data flowing to the cloud.

Axway API Gateway also secures the communication channel to the cloud, acting as the SSL termination point, managing API keys and certificates and performing all encryption tasks.

Step 3: Control access from cloud-based services

Cloud integration is often bi-directional, such as a CRM integration between Siebel and Salesforce.com. While data leaving the organization can create compliance issues, data coming into the organization can be problematic as well. For example, if a cloud-based service sends credit card numbers into an on-premise CRM system that does not expect to host such data, it can create PCI DSS compliance issues for the organization.

In addition to enforcing authentication and authorization policies for cloud-based clients such as API key-based policies, Axway API Gateway can also monitor data flow and API calls to and from cloud-based services to control incoming access.

For More Information, visit www.axway.com

Copyright © Axway 2013. All rights reserved.

