Solution Brief

Access Management for Mobile, Cloud and Partner APIs

Access Management for APIs

API Economy

The 'API Economy' is more than the latest buzz-phrase. It is the foundation of a new way for businesses to acquire customers and generate revenue, with lower acquisition and transactional costs than have ever been possible. The API Economy drives how modern web and mobile applications are designed, and how Internet commerce will work for the foreseeable future.

The technology behind the API Economy is simple, but powerful. Businesses make data and services available over the Internet by using standard web technologies, and through application programming interfaces, or APIs. Customers and partners use APIs in their own applications and services depending on the needs of the business, with or without cost.

Agility and Security in the API Economy

Exposing data and services over the Internet poses enormous security risks, and poses a number of questions: Who is accessing your data? Are they accessing it legitimately? Are hackers taking advantage of publically available interfaces to gain access to data and systems that should be secure? Maintaining security by controlling access to your public APIs is the price of admission into the API Economy.

Architecting for Agility and Security

It is difficult to know the best way to structure and control access to your API, and it is almost certain that you will go through several iterations before you discover what is best for you and your customers. If you want to maintain security and remain agile in the wake of changing requirements, your application design should incorporate three architectural concepts:

- Separate the API structure from the underlying service.
- Separate API security from the underlying service.
- Manage security with policy, not code.

Separating functional concerns in this way creates a system that is agile and adapts to changes in requirements.

Attribute Based Access Controls

Attribute Based Access Control (ABAC) is the most suitable access control model for modern environments, because user and resource attributes are used to define access policies. This abstraction means that policies can be written without any specific knowledge about the users within the system or the resources being protected.

By combining ViewDS Access Sentinel and the Axway API Gateway, organizations are able to manage their APIs, optimize access control, meet regulatory and industry compliance mandates and gain the required security levels all within an easily implemented solution.

Fine Grained API Security

Multi-platform and multi-channel Security

To be successful, organizations need to provide services across multiple platforms and channels. Mobile API's and application support are essential in order to capture some markets, whilst web services and secure file transfer solutions are typically required for partners and customers.

These diverse needs require a single API management and access control platform that can accommodate all traffic protocols centrally, from a single set of security policies.

API Security

API security breaches can cause brand damage, revenue loss, and compliance penalties. To ensure security and allow future extensibility, API security must be implemented at all levels. Authorization policies must be fine grained and highly contextual, as this will allow you to make access decisions based on a wide variety of information:

- Subject attempting access
    - Location
    - Device characteristics
    - Any attributes associated with the subject
- Resource being accessed
    - Service details, such as the web service endpoint being access
    - Content within requests and responses
    - Any attributes associated with the resource
- Environmental
    - Time of day / Day of week

Integrated with Identity Management

Identity management (IDM) systems provide a wealth of identity information that is required for API authorization decisions. API security can be achieved by:

- Leveraging attributes from IDM systems to be used for API access control
- Permitting additional attributes to be maintained as part of the authorization solution and used in conjunction with the IDM attributes.
- Ensuring API access controls do not impose an excessive load on IDM systems
- Ensuring API access controls only access the attributes that are required

Performance and Availability

Your API management and access control platform must be high performance and highly available. Your API services cannot be affected by the unavailability or poor performance of dependent systems. To achieve this there must be a tight coupling between the API management and security services, along with the localization of required IDM attributes.

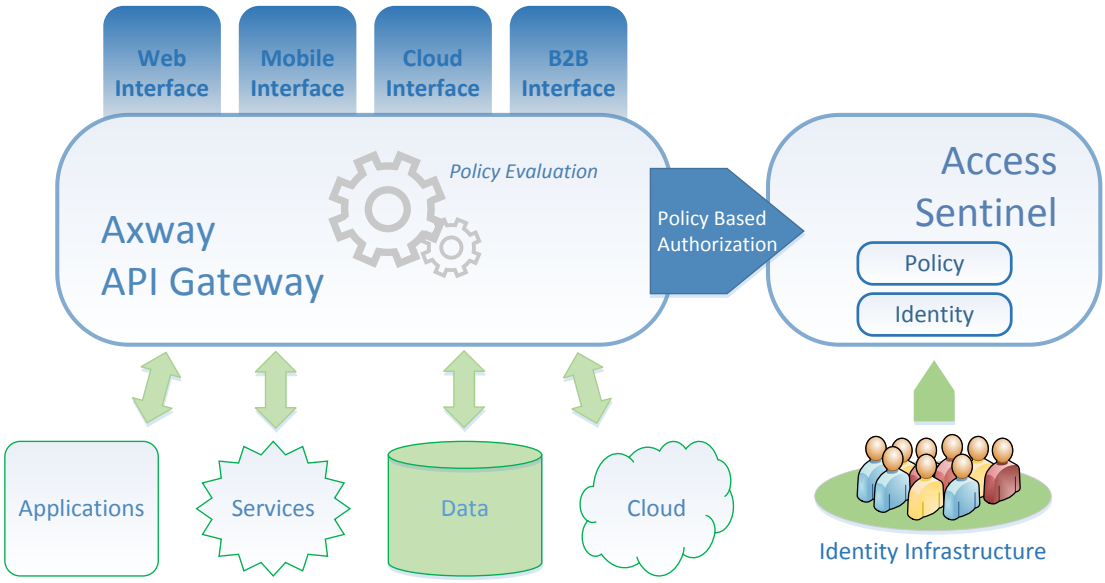
Axway + ViewDS: Fine Grained API Management

The combination of the Axway API Gateway and ViewDS Access Sentinel authorization server addresses all of these issues. It provides a scalable and flexible access control security architecture for regulated and mandated environments such as federal, financial services and healthcare industries.

The Axway API Gateway provides multi-platform service protection, message encryption and decryption, and user authentication features. This together with ViewDS's Access Sentinel, providing fine-grained attribute based access control, delivers a powerful policy-based common solution.

End users benefit from the fast performance of the combined solution, achieving thousands of authorization requests per second, which can be optionally scaled to handle authorizations from hundreds of millions of users.

ViewDS Access Sentinel natively integrates with identity management infrastructure to leverage existing attribute information. Rather than accessing information at runtime, the required attributes are synchronized into Access Sentinel. This results in a high performance solution that isn't dependent upon the availability or performance of external systems in order to operate.



About ViewDS

ViewDS Identity Solutions is a specialist provider of identity and access management software offering a suite of solutions for directory search, identity management and authorization services.

ViewDS Identity Solutions is headquartered in Melbourne, Australia with offices in Australia and the USA, and channel partners across the globe.