Fine-Grained Authorization

Ensure Legacy APIs are Secure and Compliant with Axway API Gateway

Axway API Gateway enables role-based, fine-grained authorization for legacy APIs to prevent exposure of sensitive data and ensure compliance.

Without role- or attribute-based authorization, many APIs from legacy applications do not have the access controls necessary to satisfy security-policy and regulatory-compliance requirements.

To secure APIs, Axway API Gateway enforces fine-grained authorization policies that prevent exposure of sensitive data such as personal identifiable information (PII) and protected health information (PHI).

Enforce fine-grained authorization policies

Whether a policy engine is based on eXtensible Access Control Mark-up Language (XACML) or proprietary schemes, it requires a policy enforcement point (PEP) at runtime to make the policies actionable. While fine-grained authorization/entitlement management products such as Oracle Entitlements Server, Axiomatics Policy Server, and Quest One Authorization Server offer great flexibility to define and administer fine-grained authorization policies, they provide few PEP options, which is why most implementations rely on custom-coded PEPs inside the applications.

Axway API Gateway offers out-of-the-box PEP integrations with leading policy engines to enforce access policies and redact data returned by APIs.

Control access to APIs based on roles, attributes and context

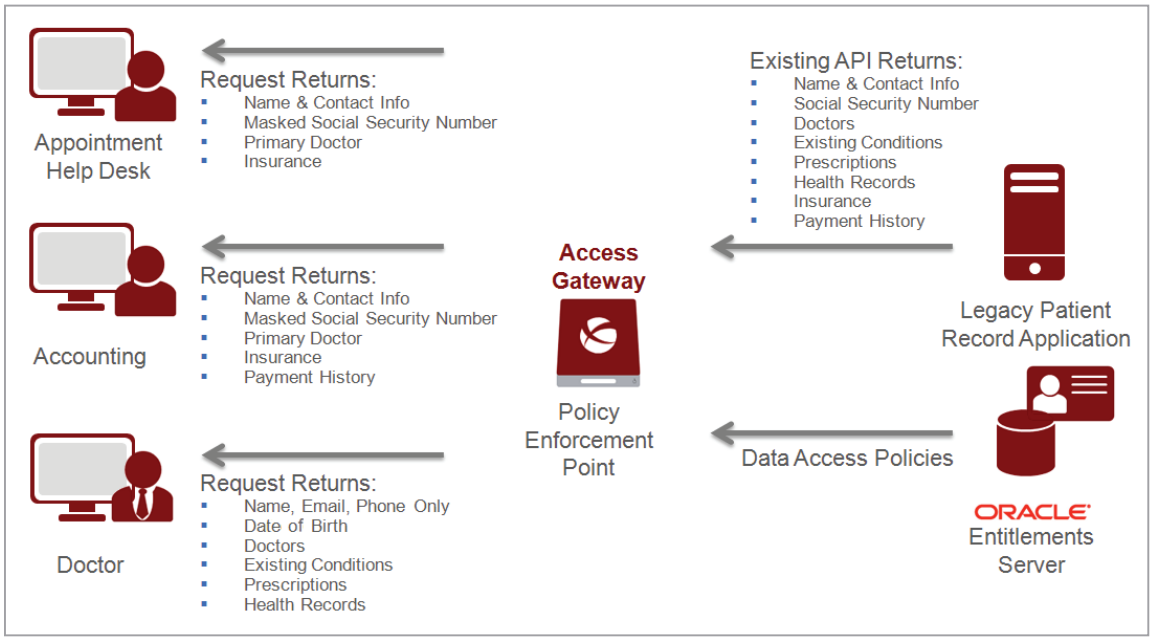
API access control policies are often more complex than simple static decisions because they depend on attributes and context that changes over time (such as user role, type of application, security domain of the API client, and time of day).

Axway API Gateway extracts and retrieves the attributes the policy server requires to make an authorization decision. These attributes can be about the client, the application, the user, or the network, and they can be extracted from the request, its payload, or another system such as LDAP. After providing the policy engine with the

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.

axway
business. in motion.



Example of fine-grained access control added to legacy back-end systems in a healthcare environment

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 Data Security
- Cloud Identity Service
- Cloud Single Sign-On
- Mobile API
- SharePoint Gateway

required input to make an authorization decision, Axway API Gateway enforces the decision by granting or blocking access to the whole or parts of the API.

Redact API data to meet security and compliance mandates

Legacy applications and their APIs typically don't have the ability to adjust output based on input parameters such as roles and attributes. When the same data set is always returned by the API, the result is often excessive data exposure beyond what is allowed by security and compliance policies.

Axway API Gateway helps ensure that legacy APIs and applications meet privacy requirements by removing, reducing, masking or encrypting any data element in the API response in real time based on authorization policies.

For More Information, visit www.axway.com