As organizations expose more enterprise APIs and SOA services that handle sensitive data and business-critical functions, security and access control have become must-have capabilities. Protecting the business means protecting against the kind of attacks and security breaches that can result in brand damage, loss of revenue and compliance penalties.

With Axway API Gateway and the Axway API Management Solution Pack, organizations can protect APIs (including REST-style APIs) and SOA services at all levels: interface, access, and data. Comprehensive API security and out-of-the-box identity management integrations deflect attacks against, control access to, and secure the data transmitted by APIs and SOA services. Complete auditing, monitoring, logging and reporting capabilities also help enterprises meet the most stringent compliance mandates.

**Protect APIs against both enemy and friendly fire**

Cloud and mobile computing have greatly increased the usage of APIs not only in terms of traffic volume, but also in terms of the number of different API clients in use, some of which are poorly engineered. A popular but misbehaving client repeatedly sending requests can cause as much damage as a malicious distributed denial-of-service attack.

Serving as the policy enforcement point (PEP) that authenticates, authorizes and audits API access, Axway API Gateway protects APIs from malicious attacks as well as potential “friendly fire” by monitoring API call volume and client behaviors. Clients that exhibit disruptive behaviors, such as denial-of service attacks or cross-site scripting, can be blocked or throttled.

**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, it 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.
Enforce message-level security across all API and SOA web service traffic

Unlike network and web application firewalls, Axway API Gateway detects and prevents message-level threats across all API and SOA traffic, including cloud, web, mobile and B2B channels.

- Messages are scanned at the protocol header, SOAP header, XML and attachment levels.
- REST API methods (GET, PUT, DELETE, POST, etc.) can be selectively restricted to ensure that inappropriate method usage is detected and blocked.
- Payloads and attachments are scanned for harmful content, JSON/REST schema validation and enforcement of schema usage policies.
- Out-of-the-box integration with CLAM AV, McAfee, and Sophos detects and prevents common attacks against APIs, including:
  - Denial of service attacks
  - Command injection attacks
  - Malicious code and viruses
  - Sniffing
  - Spoofing, tampering, and impersonation
  - Data harvesting
  - Privilege escalation
  - Reconnaissance

Secure REST APIs with enterprise-strength protection and integrations

Especially suitable for mobile applications, REST (Representational State Transfer)-style (“RESTful”) APIs are quickly gaining popularity among developers and architects. While REST is lightweight and easy to implement, it is a pattern and not a standard, which has made it more difficult to secure in enterprise environments. For example, most REST APIs are accessible only by authorized clients. Axway API Gateway authenticates and authorizes REST API requests, making it just as easy to implement enterprise-strength protection and integration for REST APIs as it is for SOAP and other APIs.

Use OAuth and SAML for identity federation

Consumer users often prefer to use their existing credentials from Google, Facebook, Twitter or other third-party identity providers to log in to an application. This capability is usually implemented using the OAuth standard, and more specifically the three-legged OAuth pattern. Axway API Gateway provides comprehensive OAuth support to help API developers incorporate OAuth client, resource server, and authorization-server capabilities into REST APIs.
SAML (Security Assertion Mark-up Language) is more popular with enterprise federation scenarios. Axway API Gateway supports OAuth, SAML, XACML, X.509, Kerberos, OpenID and other popular authentication and authorization standards.

**Protect SOA services with access control and identity management**

While SOA web services are supported by a comprehensive set of security standards (SAML, WS-Security, WS-Trust, WS-Federation, WS-I and WS-Secured Conversation) the task of implementing them “by the book” is daunting for developers. This leaves most SOA services without sufficient access control.

Axway API Gateway provides out-of-the-box access control capabilities for SOA services, including authentication, authorization, audit, trust relationship management and identity federation. These capabilities are in addition to the basic security capabilities such as transport security, encryption and signing.

**Other Axway API Gateway Solutions include:**
- 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
- Fine-Grained Authorization
- Mobile API
- SharePoint Gateway