axway

Best Practices for Digital

9 WAYS TO SECURE AND ENHANCE YOUR ARCHITECTURE

01
Be creative and inventive without putting data at risk
API access control and policy rules let you be transparent without compromising corporate security and regulatory compliance.

02
Give developers access to common services for seamless cloud integration
Implement a consistent API-centric integration layer for cloud-to-ground data exchange, and ensure that existing identity services are extended to new cloud applications.

03
Know how data and services are being accessed from everywhere
Use your API platform as a central point for governing the flow of data to and from the cloud and mobile apps, between business applications, with partners, and across customer-facing services.

04
Prepare for the dreaded IT or security audit
Use application and API management platforms to maintain irrefutable and actionable information about how your IT services interact with on-premise, cloud and mobile apps and services.

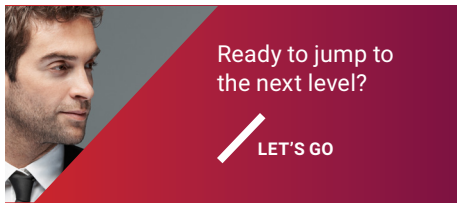
05
Protect all APIs — even internal APIs — against hijack and attack
Add security measures to safeguard the API service control layer and block common web API (REST and SOAP) attacks.

06
Guarantee service-levels for both internal and external customers
Allow business and technical users to measure, monitor and act on changes in performance or demand.

07
Think of security as a window, not a wall
With the right security in place, you can open up data to mobile access, cloud integration and partner collaboration. Use identity management infrastructure along with API-specific identity patterns (OAuth, for instance) to provide safe access to APIs.

08
Separate service exposure from policy enforcement
Give API developers a suite of standard and reusable policy rules that can be easily applied to microservices that represent the specific needs of a given application.

09
Protect back-end services from unusual traffic patterns
Set limits and expectations for API services and their consumers to manage scale and traffic expectations, and protect back-end services from malicious activity.



axway.com/digitize

AXWAY_CK_9_WAYS_SECURE_DIGITAL_ARCHITECTURE_EN_020917