ORACLE API GATEWAY

Centralized And Secure Cloud Connectivity

Oracle API Gateway is a standards-based, policy-driven, standalone software security solution that enables organizations to securely and rapidly adopt Cloud, Mobile and SOA Services by bridging the gaps and managing the interactions between all relevant systems.

KEY FEATURES

- ***API Security***: Threat Protection for XML, SOAP, REST and JSON, Identity and Access Control, API Key authentication, Data level privacy and integrity, Content Payload inspection, Compliance.
- ***Centralized Cloud Connectivity:*** Proxy and Manage interactions with Cloud Services. Restrict, throttle and manage web services and REST APIs.
- ***API Management for Mobile and Cloud:*** Connect mobile devices to enterprises. Map between data formats such as XML and JSON.
- ***Centrally Protect and Manage API Keys***
- ***Virtualize and Route Cloud traffic***
- ***Audit and monitor Cloud usage***

KEY BENEFITS

- ***SSO and Access Control for Cloud Applications***
- ***Regain visibility and demonstrate compliance with activity monitoring and security intelligence***
- ***Protect and manage internal and external users, data, applications as they move to and from the cloud***

STANDARDS SUPPORTED

- ***Web Services Protocols***: SOAP 1.1 & 1.2, SwA, MTOM, Plain XML (POX), REST, Web 2.0 (Ajax, JSON), UDDI, WSDL
- ***Transport Protocols***: TCP, HTTP 1.0 & 1.1, JMS, MQ, FTP, SFTP, SMTP, POP.
- ***Security and Policy Model***: SSL, XML Encryption, XML Signature, WS-Security (SAML, Kerberos, Username, X.509 token profiles), WS-Policy, WS-SecurityPolicy, WS-Trust, WS-SecureConversation, WS-Addressing, WS-RM, XACML, XKMS, PKCS#1, PKCS#7, PKCS#12, S/MIME., OAuth

Introduction

Cloud computing is transforming the way enterprises think about Information Technology. Adoption of a cloud based approach and model – results in greater operational efficiencies and lower costs than many traditional IT deployments. However, as with any new technology, security is often a major inhibitor to adoption. A cloud service consumer or subscriber based computing model is associated with concerns over visibility into these services, less control over security policies, new threats facing shared deployment environments and complexity of demonstrating compliance.

Oracle API Gateway acts as a control point for managing how internal users and application assets are exposed to outside cloud offerings and reduces cloud related security risks. It allows enterprises to leverage their existing Identity and Access Management investments by extending authentication authorization and risk policies to mobile, cloud and enterprise applications – without changing backend applications.

In Cloud environments, Oracle API Gateway allows to:

Integrate Cloud Services and On-premise Services

- Proxy and Manage interactions with Cloud Services.
- Restrict, throttle and manage web services and REST APIs.
- SSO for Web Services

Extend Enterprise Security to Mobile and Cloud Applications

- Secure and Manage APIs (support for OAuth, REST API security and JSON)
- Centrally protect and manage API Authentication Keys
- SSO for Web Services and REST APIs
- Extend authentication, authorization, and risk policies to mobile, cloud, and enterprise applications – without changing backend applications
- Securely bring advanced mobile computing into the enterprise by leveraging integrations with Oracle and non-Oracle IAM solutions.

Audit and Monitor Cloud Usage

- Monitoring and reporting on cloud usage
- Monitor service quality and audit SLA agreements

Enforce Data Security Policies

- Scan messages and data payloads against security and privacy policies
- Block, redact, remove or encrypt data

Oracle API Gateway – Cloud Use case Scenarios

Feature Highlights	
Access Security: Simplifying identity and access management in cloud environments	• API Key authentication • SSO for Internet APIs • Validate HTTP parameters, REST query/POST parameters, JSON data structures, XML schemas etc. • Protect against cross-site scripting (XSS) and DoS attacks • Authentication and SSO for cloud services • Authorization leveraging Enterprise Fine Grained Authorization engine.
Data Security: Securing access to sensitive information in shared environments	• Inspection of inbound and outbound cloud traffic on the wire. • Enforce data security policy to remove, mask or encrypt sensitive data. • Scan inbound requests to prevent message level attacks • Any to any identity token conversions
Audit and Monitoring: Visibility and insight into cloud activity and threats	• Monitor, measure and report cloud usage and SLAs • User, client, data and transaction level logging • Detect rogue usage of non-approved cloud services • Service monitoring and alerting
Integration: Centralized cloud connectivity	• Integrate cloud services to on-premise services • Protocol translation and data bridging • Request routing, throttling and response caching

Contact Us

For more information about Oracle API Gateway, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Oracle is committed to developing practices and products that help protect the environment

SOFTWARE. HARDWARE. COMPLETE.

ORACLE