API Security & Management Suite

The Industry's Leading Products for Enterprise-Scale API Security & Management

Securely Expose APIs to Partners, Developers, Mobile Apps & Cloud Services

The CA Layer 7 API Security & Management
Suite offers products for:

API Security & Management Suite
Expose information assets for reuse across Web, mobile and cloud, while maintaining the highest data security and IT efficiency standards

Developer Access
Empower internal and external developers to leverage your APIs

Mobile Access
Securely connect the enterprise with mobile apps and smart devices

Partner Access
Share information and services across organizational boundaries

Cloud Access
Remove barriers to adoption of SaaS applications and cloud infrastructure

**Learn More About the
CA Layer 7 API Security &
Management Suite**

- **Phone** +1-8
- A̋+

Introduction
Increasingly, enterprises are opening their data and applications to partners, developers, mobile apps and cloud services. APIs provide a standardized way to open up information assets across the Web, mobile devices, Service Oriented Architecture (SOA) and the cloud.

However, to make API information sharing safe reliable and cost-effective, enterprises must deal with critical security, performance management and data adaptation challenges. CA Layer 7's API Security & Management Suite makes it simple for enterprises to address these challenges.

The API Security & Management Suite combines advanced functionality for backend integration, mobile optimization, cloud orchestration and developer management. It is unique in its ability to address the full breadth of enterprise API Management challenges.

CA Layer 7 API Gateways
CA Layer 7's family of API Gateways offers unmatched flexibility, performance and security. Available as hardware appliances or virtual machines, for deployment on-premise or in the cloud, they represent the best solution for securely exposing enterprise data and services.

CA Layer 7 API Gateways include:

- **API Proxy**
  Deploy the core functionality needed for enterprise-scale API security and management

- **CloudConnect Gateway**
  Connect securely and seamlessly with SaaS applications and other cloud-based services

- **SOA Gateway**
  Centralize governance of services integrated across the extended enterprise

- **Mobile Access Gateway**
  Securely and efficiently open enterprise information assets to mobile devices and apps

The Complete Solution for Enterprise API Management
The API Security & Management Suite includes a range of complementary products that are delivered pre-integrated with CA Layer 7's API Gateways, including:

- **API Portal**
  Engage, onboard and educate internal and third-party developers via a branded online interface, to facilitate the creation of applications that leverage enterprise APIs

- **API Service Manager**
  Manage the API lifecycle from development, to test, to production

- **OAuth Toolkit**
  Control access to API-based resources using OAuth 2.0 and OpenID Connect

- **Security Token Service**
  Simplify identity federation and Single Sign-On (SSO) using OAuth and SAML

Key Features

API Gateways

API Proxy	• Implement enterprise-grade threat protection and access control for APIs • Simplify the process of API composition, orchestration and lifecycle/performance management • Track API performance and generate an audit trail of all service interactions
CloudConnect Gateway	• Create SSO for SaaS applications and other cloud services • Securely integrate cloud services with on-premise IT systems • Track usage of cloud services to ensure compliance with regulatory requirements
SOA Gateway	• Enable secure SOA integration, partner connectivity and cross-departmental information sharing • Compose, edit, customize and enforce SOA Governance policies from a single, central location • Manage complex SOA architectures that span enterprise datacenters and the cloud
Mobile Access Gateway	• Enforce access control, firewalling and data security for mobile apps that access enterprise resources • Adapt and optimize complex enterprise services for bandwidth-light mobile use cases • Securely integrate enterprise apps with the cloud, social networks and mobile notification services

API Portal

Developer Onboarding	• Support for both individual developers and larger partner organizations • Ability to define registrations as being automatically accepted or subject to approval • Support for both self-signup and managed enrollment
Developer Resources	• Discussion and support forums, integrated messaging etc. • API documentation, API explorer, API status, application reports etc.
Reporting & Analytics	• API reports that track and meter API usage, successes versus errors, latency etc. • Application reports that show latency, usage, successes versus errors etc.
Content Management	• Ability to define the look, feel, brand and content of the Portal • Support for both staging and production environments, as well as a content approval/publication/ rollback processes, streamlining change management

API Service Manager

API Migration	• Ability to automate the migration of API policies between environments (from dev to test, east to west etc.) with full dependency resolution, thereby decreasing migration risk • Support for automatic API versioning, including rollback to any previous version
Operational Metrics	• Configurable, out-of-the-box reports provide insight into API performance, making it possible to meter and track API/method usage for per-user billing, capacity planning, SLA compliance etc. • Real-time monitoring dashboard provides insight into API Gateway and network performance
Change Management	• Ability to create changes to API policies and push them out to all Gateways in the enterprise

OAuth Toolkit

Specifications	• Supports OAuth 1.0a, OAuth 2.0 and OpenID Connect • Provides sample OAuth implementations that can be configured to specific needs

Security Token Service

Specifications	• All Gateways include a built-in STS that can issue and validate OAuth and SAML access tokens, optionally with HMAC or RSA signature methods and SHA-1, SHA-256 or SHA-512 encryption