DATA SHEET

CA API Gateway

At a Glance

APIs are becoming ubiquitous as enterprises increasingly need to open up to mobile devices, cloud-based services, partners and third-party developers. The CA API Gateway provides a single solution that can accommodate internal API initiatives, enabling businesses to consume data in new ways—driving innovation, customer satisfaction, and increased efficiencies. The CA API Gateway combines policy management with runtime policy enforcement, delivering a central policy enforcement point between the business and the end-user—no matter where they are located.

Key Benefits/Results

- Security: Centrally manage and secure corporate assets
- Control: Prioritize traffic to help ensure APIs remain available and responsive
- Adaptation and Composition: Create APIs that contain subsets/supersets of API functionality
- Translation: Translate between legacy and new applications and data

Key Features

- Security: Passed rigorous vulnerability tests, and integrates with any popular IAM system with support forOAuth, SAML and RADIUS.
- Performance and Scale: Clustered architecture allows linear scalability across multiple Gateways, with automatic failover. Includes application level throttling and prioritization.
- Manageability: Handles migrations across dev/test/production with global management tools, and integrates with enterprise BI, analytics, and reporting tools.
- Flexibility: Multiple form factors/ deployment models with support for a wide range of platforms, including Docker, AWS and Azure. Provides protocol bridging across legacy and new systems, and includes content-based routing.
- Extensibility: Plug-in framework to add new transports and identity providers, and deep integration with enterprise management and BI products.

Business Challenges

As the enterprise looks to embrace cloud and mobile, they are faced with some serious business challenges, starting with the key issue – how do they maintain control over corporate apps and data once these leave the business? Additional challenges include:

Opening on-premise data and applications to third parties. Opening on-premise data and applications to third parties via APIs raises a range of serious security concerns. Additionally, API publishing creates challenges around ensuring scalability and manageability as adoption grows and adapting data for consumption by a range of constituents.

Protocol orchestration. As businesses migrate to the open enterprise model, there is a need to connect disparate data/applications across a multitude of environments—legacy to cloud to mobile. The ability to connect these different solutions, their identity management, their protocols, and their data into a seamless solution is crucial.

Manageability. One of the biggest challenges that businesses face is how to manage a framework that consists of legacy solutions and open solutions—across data centers and the cloud. Further, any new solution must integrate with corporate reporting/analytics/BI tools inside the enterprise.

Solution Overview

The CA API Gateway enables enterprises to selectively open their data and applications to both internal and 3rd-party developers, integrating with existing IAM solutions for a plug and play solution. The CA API Gateway deploys in a variety of form factors, easily scales, and can be deployed in a failover environment for high availability. The gateway can be configured to be PCI-DSS compliant, and includes a built-in PKI engine, FIPS 140-2 level encryption, a robust RBAC system, and SAML support.

The CA API Gateway includes protocol bridging, providing full translation between a variety of protocols—from legacy to REST and JSON—providing the bridge from legacy to mobile, cloud, and social.

Finally, the CA API Gateway not only plugs into existing management solutions, it can easily be managed across data centers and the cloud, and provides dynamic policy management to maintain efficient response times.

	Feature	API Gateway Essentials	API Gateway Enterprise	Mobile API Gateway
API Mangement	Manage API lifecycle and migrate policies between environments	✓	✓	✓
	SLA adherence via traffic throttling, prioritization and routing	✓	✓	✓
	Customizable API composition and virtualization	✓	✓	✓
	RESTful interfaces for policy migration and gateway management	✓	✓	✓
	Troubleshooting tools for debugging and versioning	✓	✓	✓
Security	FIPS 140-2 compliant and CommonCriteria Certification	✓	✓	✓
	Threat detection and message content filtering	✓	✓	✓
	Manage access using industry standards	✓	✓	✓
	Integration with third-party IAM systems and customizable execution branching	✓	✓	✓
Policy Development and Editing	Policy development, debugging and troubleshooting tools	✓	✓	✓
	Reusable policy statements and customizable policy execution branching	✓	✓	✓
	Administration-based service and operation policies	✓	✓	✓
	Policy lifecycle management across dev, test, staging and production	✓	✓	✓
Enterprise Scale Management	Single, real-time view of all gateways across the enterprise and cloud	✓	✓	✓
	Centralized migration of policies between environments, setting, and geographies	✓	✓	✓
	Configurable reports provide insight into gateway operations and SLA	✓	✓	✓
	Ability to centrally back up configuration files and policies	✓	✓	✓
Integration	SaaS federation	✓	✓	✓
	SSO integration with enterprise and cloud services	✓	✓	✓
	Connect to, query and retrieve data from enterprise resources such as DBMSs and Microsoft® SharePoint®	✓	✓	✓
	SAML integration		✓	✓
	Amazon AWS AMI integration		✓	
SOA	Simple Orchestration		✓	✓
	WS-* support		✓	✓
	XACML		✓	✓
	MOM mediation		✓	✓
Auth & Comms	WebSocket		✓	✓
	XMPP		✓	✓
	OAuth and OpenID Connect	✓	✓	✓
Mobile	Android/iOS push notifications			✓
	Mobile SDK for mutual SSL and SSO			✓
	Cross-device session sharing (QRC, BLE and NFC)			✓
	Geolocation (client or network originated)			✓
	Samsung KNOX for APIs (attestation, container management, Integrity validation, on-device SSO)			✓
Supported Standards	XML, JSON, Swagger, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, RADIUS, SAML, XACML, OAuth 1.0a/2.0, JWT, PKCS, Kerberos, X.509 Certificates, FIPS 140-2, XML Signature, XML Encryption, SSL/ TLS, SNMP, SMTP, POP3, IMAP4, HTTP(S), JMS, MQ Series, Tibco EMS, Raw TCP, FTP(S), WS-Security, WS-Trust, WS-Federation, WS-SecureExchange, WSIL, WS-I, WS-Addressing, WS-Policy, WSSecureConversation, WS-MetadataExchange, WS-SecurityPolicy, WS- PolicyAttachment, WS-I BSP, UDDI, WSRR, MTOM, IPv6, WCF			

The CA Technologies Advantage

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**

Our strategic partner: eBlueprint

With over 14 years of experience, eBlueprint provides companies – no matter what their size, industry or location – with end-to-end technology solutions that optimize their IT investments. Central to eBlueprint's success is partnering with industry leaders like CA; which enables them to deliver best-of-breed technology that is specific to customers' individual requirements and budgets. **www.eblueprint.com.au**.

For more information, please visit **ca.com/api**

CS200-206243_0616