An Architect’s Guide for Extending Your ESB/SOA Environment to Mobile, Cloud and IoT:

Connecting the Enterprise to the New Digital World with API Management
The Integration Landscape Today

Every enterprise has a wide variety of IT requirements where integration is needed. The rapid proliferation and adoption of cloud and mobile technologies has accentuated the financial impact of these needs. In response, the integration space has matured to include feature-rich stacks from enterprise integration vendors that provide full, multi-layer platforms in the form of an Enterprise Service Bus (ESB) or SOA suite. But with these very broad capabilities comes complexity—multi-layer stacks can be difficult and costly to install, debug, administer and secure. In fact, this has created something of a backlash in the development community for simpler tools and frameworks—for example, using Spring and Node.js for development initiatives with lighter-weight server-side implementations not requiring a full-fledged app server. The same reasons that drive developers to prefer a lighter-weight Java container apply at the integration engine level as well. There is a real demand for lighter-weight integration solutions, especially in cases where an enterprise is focused on simple and secure integration that may span SOA, mobile API, B2B, SaaS and cloud, without being part of a large initiative implementing an ESB or SOA. People still need to connect systems together, even when the problem at hand doesn’t justify a complex multi-layered integration platform.

However, the benefits of ESB patterns are still relevant to nearly all integration projects—standards-based usage of XML for canonical and intermediate data types, rich protocol connectivity and adapter support, configuration-based policies, etc. What is really needed is a lighter-weight integration technology that is modern enough to support these capabilities yet provides a simpler experience for installation, development and operational management. In addition, the multi-layer approaches common to integration stacks often leave security to a separate component, layer or device. While this can be an issue for internal integration projects, it becomes a real liability when integrating with Web API patterns and standards like REST and JSON. As a result, including security and identity control natively in the integration layer is even more critical than ever.

Finally, the nature of exposing services externally as well as integrating with services outside an organizational firewall means that the integration, service bus and security needs will often require technology to be placed in the DMZ. This is an area where deploying a large software stack is the last thing an enterprise wants to do—there is a very rigorous set of requirements that any enterprise has regarding what can go into the DMZ. This is where appliances (including both software appliances based on virtualization platforms and physical appliances with bundled hardware and software) become especially critical. An enterprise should avoid deploying software into the DMZ at all costs and a hardened security appliance is widely accepted as the best approach. Aside from this absolute requirement, an appliance form factor for integration technology also provides a superior installation experience and unparalleled performance when compared to a traditional ESB approach to integration.
Extend SOA/ESB with API Management

To address these requirements, CA API Management solutions allow you to integrate simply across SOA, API, cloud and Internet of Things (IoT). The CA API Gateway appliance provides a broad set of integration capabilities, including native security and XML Gateway functionality and identity federation using both SAML and OAuth. Relevant features include:

- Support for the message formats and connectivity protocols used by most modern applications, as well as an ability to transform message formats from legacy applications by mediating to more modern standards
- Real-time, dynamic routing to any of these protocols, based on message content, message context or transaction metadata
- Sophisticated access control mechanisms that can leverage request content and existing identity stores to provide policy-based authentication, authorization and single sign-on using SAML and OAuth-style federation
- Data privacy and integrity operations based on Public Key Infrastructure (PKI) standards
- Comprehensive threat protection and content filtering
- Orchestration and exposure of existing assets as fully-managed APIs or micro-services for easy consumption by mobile apps
- Support for integration standards and methodologies for cloud and mobile connectivity
- Flexibility of deployment form factor (hardware, virtual machine, software appliances) and location (intranet, DMZ, cloud)
- High performance and easy scalability for elastic environments
- Simplified deployment, lifecycle and operational management

This makes CA API Gateway a market-leading integration appliance—providing a simple, secure platform for integrating applications without the baggage of a complex, multi-layer solution, resulting in a powerful yet lightweight alternative to a traditional ESB.
Protocol Mediation

One of the main hallmarks of an ESB is support for message format transformations and protocol mediation. This is generally accomplished through application-specific adapters, which then need to be wired together, often by generating and modifying code and metadata. That underlying code, the application server it runs on and the ESB layer then need to be deployed, managed, versioned and maintained. A CA API Gateway appliance, on the other hand, has built-in support for message transformations from legacy, B2B and industry-specific formats to standards-based XML included with the appliance, with no such application server dependencies. These include COBOL copybook, 14 flavors of EDI, HIPAA and user-defined custom formats. In addition, adaptation of SOA services using WSDL and SOAP to newer interfaces using REST, JSON and OData allows broad exposure of applications, without the need to modify existing code.

Support for various messaging (MQ, JMS, EMS, AMQP, WebSockets, XMPP), file (FTP, FTPS, SFTP), B2B (AS2), email (SMTP, POP3, IMAP), data sources (SQL and NoSQL) and operational (SNMP, syslog) standards is built in for mediation between protocols without the need for additional coding or maintenance. This allows usage of existing infrastructure, without modification of current operational practices. The combination of these common protocols with standard HTTP-based APIs exposed by the vast majority of packaged applications and SaaS providers means that CA Technologies enables companies to connect to nearly anything. In cases requiring a custom protocol or non-standard legacy format, CA Technologies provides an SDK for adding a new data handler or transport protocol.

For maximum flexibility, messages can also be dynamically routed to an endpoint, using any supported protocol, based on a variety of decision factors. These include the message source (user, application, organization), message content (transaction total, account number, operation), transaction metadata (service, operation, protocol header value) or operational metric (day of week, time of day, transaction count). For example, a SOAP-wrapped XML banking transaction from a particular customer can be transformed to a flat-file format, routed to the appropriate network segment and delivered to a queue intended for a mainframe application—this provides simple, secure modernization of legacy applications.

Beyond Mediation: The Growing Security Imperative

When enterprises expose their applications to partners, mobile users, Cloud apps or even other internal systems, security must be of the utmost concern—at CA Technologies, security is a first-class citizen, whether the integration is around the world or between two internal applications. Security begins with the appliance itself, which has received the most stringent security certifications in its field, including Common Criteria, PCI DSS compliance and FIPS 140-2 certifications. Government agencies and private enterprises can be assured by vulnerability testing for Secure Technical Implementation Guide (STIG) compliance, integration with at least six DoD security/monitoring working groups and support for the latest encryption technologies such as Elliptic Curve Cryptography.
Specific functionality around access control, data privacy, data integrity and threat protection is also built on this secure platform. A powerful, flexible access control system ensures that only allowed users/systems gain access to data exposed by these interfaces. CA API Management integration appliances support a wide range of credential types and can authenticate and authorize these credentials using all major identity and access management product suites. Whether it’s a WS-Security UsernameToken being validated by CA Single Sign-On or an SSL certificate subject being looked up in Microsoft Active Directory, security tokens are verified in an appropriate manner for the application in question. CA API Gateway appliances are ready for today’s latest access control standards, such as OAuth and OpenID Connect, for flexible connectivity to cloud, mobile, or web-based interfaces, while leveraging existing IAM investment. In addition, a built-in WS-Trust Security Token Service (STS) can federate identities between disparate identity domains using standards-based protocols and tokens such as SAML.

Once an application call or service invocation has been authenticated and authorized, data privacy and integrity must be ensured. This begins with transport layer security using SSL/TLS and IP filtering and continues up the stack, with encryption and digital signature implementations designed to protect data, using PKI standards. CA API Gateway supports W3C XML encryption and signatures, as well as WS-Security for SOAP-based messages. These are complemented by related WS-* standards for describing (WS-Policy), routing (WS-Addressing) and communicating (WS-SecureConversation) using PKI for distributed trust. This is an area where an appliance approach can offer significant advantages over the traditional ESB for integration because with a traditional approach, adding security to services can have a very large negative impact on performance. Don’t be fooled by vendor performance benchmarks for unsecured services if your production services will need to be secured.

Opening application interfaces to a broader audience also brings with it a wide range of new threats. CA API Management appliances address these threats with a combination of positive and negative security models. A positive security model strictly specifies expected input criteria and forbids entry to any requests not meeting those expectations. CA API Management appliances are application-aware and can reject any requests without the appropriate pre-defined protocol headers, credentials, schemas, namespaces and even content. Negative security models rely on common attack vectors to create filters for vulnerabilities such as SQL injection, cross-site scripting, parser attacks and message format attacks. CA API Management appliances have built-in filters for over 30 types of attack that could accidentally or deliberately compromise enterprise systems. Attachments can be analyzed, stripped, rejected or sent to an external virus scanner for additional processing.

A combination of the integration and security features discussed here is what makes integration appliances a true solution for modern architectures that include external systems such as mobile and cloud deployments. The message formats, protocols and security tokens needed for these use cases can easily be incorporated into any policy. This allows an enterprise to safely extend the perimeter of the datacenter to include partners, hybrid clouds, public cloud service offerings and mobile applications.
Simplifying Implementation Inside the Enterprise or the Cloud

To simplify the installation, deployment and management process, CA API Gateway supports multiple form factors and deployment options. Within the intranet and in the DMZ, an appliance form factor provides a data center drop-in option for bundled deployment. Virtual appliances based on common platforms (including VMware and Xen) can be deployed on existing hardware for on-premises or private cloud deployments. The appliance form factor relieves enterprises of the support and maintenance headache of a multi-layer ESB solution. CA Technologies also provides instances on popular cloud platforms, including Amazon EC2, for hybrid and public cloud deployments. These cloud-resident appliances allow for duplication of internal applications in the cloud, for traffic bursting or capital expenditure reduction. Lastly, CA API Management is available as a software deployment for embedding with other systems.

Wherever they are deployed, CA API Management appliances provide a high-performance, scalable platform for securely connecting applications. Both hardware and virtual appliances are tuned for maximum performance and scale linearly with the addition of new instances to support increased application traffic. They can be clustered, managed and monitored across deployments spanning internal data centers and external cloud infrastructures, for seamless, hybrid cloud use cases. Policies can be migrated between dev/test/staging/production deployments, with environment-specific parameters surfaced for editing. Previous policies are automatically stored and versioned and can be retrieved and enabled at any point, in any environment. The appliances integrate with existing operational management systems, and business-level usage reports can be generated around any standard metadata or custom user-defined data points.

The Case for CA API Management

CA API Management appliances are prepared to meet the specific integration needs of the modern enterprise, tying together existing infrastructure products to gain end-to-end connectivity and operational consistency. They provide out-of-the-box support for proprietary IDM, SSO, XACML and Federation services from Microsoft, Oracle, Novell, IBM, CA, VMware, Sun, Axiomatics, Ping Identity and many more. Service definitions can be retrieved from or published to existing registries and repositories such as HP Systinet, SoftwareAG CentraSite, IBM WSRR or any UDDIv3 compliant platform. In addition, deeper integration allows CA API Management appliances to be included as a part of service policy lifecycle management, including automated deployments, approval workflows etc. Cryptographic (such as SSL) and XML operations are accelerated out of the box and can be supplemented with specific hardware options. For additional security around storage of cryptographic material, CA API Management appliances support both onboard and external Hardware Security Modules (HSMs). Operational visibility is provided via standards such as syslog, SNMP and WSDM, as well as specific integrations with runtime dashboards such as CA Application Performance Management. For end-to-end visibility of identities and threats across partners, customers, mobile users, cloud services and on-premises applications, the appliance integrates with SIEM platforms, IP firewalls and operational intelligence engines.
The CA API Management appliance feature set combines the robustness of a traditional SOA/ESB network integration appliance with the simplicity and ease of use of a much lighter-weight solution. The vast majority of customer needs can be met by core out-of-the-box functionality and custom requirements are easily added through the provided SDKs. Integration policies are defined using a rich, user-friendly GUI that blends declarative assertions (“Require WS-Security UsernameToken,” “Route to JMS endpoint,” “Validate XML/JSON Schema”) with workflow constructs for fan-in/fan-out, looping, conditional and other processing patterns. Orchestration of multiple internal or external calls, support for microservices architectures and creation of new value-added APIs allow powerful mash-ups and a lightweight alternative to traditional BPEL engines. Any data, including cloud-resident metadata, external service responses, identity attributes or access control decisions can be cached and re-used to decrease the latency impact of network callouts on subsequent requests. Even elastic management of physical and virtual infrastructure using command line and cloud management APIs is available in the CA API Management appliance—everything necessary to integrate simply for SOA, API and cloud.

Conclusions

As integration technologies have matured and key standards have emerged, SOA/ESB approaches have provided very functionally rich solutions, but at a cost. However, it is now possible to get a simple and secure integration appliance that enables a modern integration architecture, but with a lightweight footprint and user experience. CA API Management offers the market-leading integration appliance for simple, high-performance integration, with a rich functional footprint and security baked in.

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

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.