Make your security moves wisely
THE LEADER IN WEB SERVICES & SOA SECURITY
**Leading the Way to Enterprise SOAs**

It seems just yesterday that web applications redefined commerce and community by creating new value and new growth opportunity from the outside into the enterprise. Service-Oriented Architectures (SOAs) are creating similar transformational impacts on the way companies do business -- this time from the inside out. Customer orders can originate from on-line shopping carts, flow to a global order management center, which in turn triggers events such as distribution, shipping, payment, and inventory replenishment.

However, loosely coupled SOAs increase business and IT risk. Unauthorized data disclosure, credential capture, and data theft are a few examples of the growing threats that trail SOA deployments. In turn, enterprises are being compelled to stopgap or revisit their security strategies to preserve the protection and security of business processes and applications.

Forum Enterprise SOA Security Solutions address performance, security, scalability, and management challenges faced by government and commercial organizations, ensuring data continuity and defense against a new generation of threats.

**A Seamless Security Architecture**

Security must be integral to SOAs. Enterprise SOA security must address message-level security requirements that transcend the transport and the application. By inspecting and securing the content of XML messages, SOA security should guarantee the confidentiality, authentication, integrity, authorization and non-repudiation of machine-to-machine interactions using standards such as WS-Security, SAML, WS-Secure Conversation, WS-Trust, and WS-Policy. Enterprise SOA security must also offer mechanisms that ensure XML-related vulnerabilities are contained and new threats are avoided.

**Forum Enterprise SOA security solutions are a life cycle approach to protecting Web services and SOAs using an adaptive approach to creating trustworthy and protected business applications.**
Threat Protection:
The process of quantitative and qualitative risk assessment for information security begins by:
1) identifying the assets,
2) their dependencies, and
3) any associated vulnerabilities, be they accidental or malicious.

Forum solutions include capabilities that focus on information threat protection and offer specific remedies for known vulnerabilities, continuing updates for assessments and remediation efforts for impending (or unknown) threats.

Trust Management:
In an open and distributed computing environment where information is shared among numerous entities (whose level of trust varies), organizations must determine appropriate access for each entity (user, person, machine or software agent), even when that entity cannot be known in advance. Granting privileges to a user, based on his or her digital identity and determining the user’s degree of trustworthiness, are part and parcel of information trust management.

Information Assurance:
To be useful, information must be available and the degree of this availability impacts its risk level. Because connectivity makes information available, it also exposes information to risks both outside and inside an organization’s control. Forum information assurance solutions offer business continuity, availability, and reliability using measures that protect and defend information and information systems using detection and reaction capabilities.

Enterprise SOA Security Considerations

Web Services and XML Security Standards:
Adoption of Open specifications of the World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS) for the enforcement of confidentiality and integrity of Web services

XML Threat Prevention:
Deep inspection, validation, monitoring and filtering of Web services and XML transactions. Actively defending and avoiding against pattern and signature-recognizable XML vectored attacks, intrusions and malicious software

Security Policy Management:
Management and the governance of rules must be derived from business, organizational and enterprise requirements. Centralized Policy Decision Points (PDP) as well as distributed policy Enforcement Points (PEP) need to be deployed

Authentication:
Verifying proof of an asserted identity, authentication should be facilitated and resolved using transport (e.g. SSL X.509 Certificates) as well as message-based protocols (e.g. SAML/WS-Security Assertions)

Identity Mapping:
Transforming and brokering an identity that exists in one domain to an identity within another domain

Authorization:
Resolving a policy based on access control decision

Secure Web Services Exchange:
Ensuring trusted exchange of multiple SOAP messages and the security policies that govern the formats and tokens of those messages

Credential Conversion:
Provides mapping of one type of credential to another such as an X.509 Certificate to a Kerberos/WS Security token

Trust Delegation:
Bridging the differences between mechanisms associated with authentication, assertions, and entitlements to enable a federated trust model

Audit:
Tracking, monitoring, and reporting of security related events

Privacy:
Policy driven enforcement of personally identifiable information using both transport (e.g. SSL Session encryption) as well message-based protocols (e.g. XML-Encryption)

Safe and Secure Cryptography:
Private keys and passwords once comprised void the trust model that depends on them. A secure SOA must offer a robust and tamper resistant storage of private keys, passwords, and algorithms

Vulnerability Management and Risk Assessment:
Organizations should actively look at flaws and weaknesses in SOA design and implementation to preempt potential threats.
Web Services Firewall with data level authentication, XML intrusion prevention and interoperability enforcement protects enterprises against XML viruses, denial of Web service attacks and unauthorized data access. Forum XWall ensures applications are appropriately accessible and continuously available by enforcing policies that check data integrity and control access to exposed enterprise Web services.

Web Services Diagnostics is a quality assurance solution that tests Web services for security susceptibilities, functional accuracy, and performance requirements. Forum XRay can systematically and cost-effectively detect and eliminate design-centric as well as attack-centric vulnerabilities prior to application deployment.

Vulnerability Containment Service is an early warning system for known and impending XML-related vulnerabilities. Forum Vulcon is an on-line subscription service that automatically delivers threat intelligence reports, antivirus updates, as well as software and policy revisions.

Forum Gateway enables trusted information sharing using XML data and Web services across disparate security domains and complex business processes. Forum Sentry allows enterprises to achieve a higher return on investment by implementing secure service-oriented architectures and event-driven applications.

XML Accelerator is a network device that offloads XML processing such as parsing, Schema Validation, XPath and XSLT at wire speed performance. Forum Vantage™ ensures that consistent network and application behavior will lower the investments required at the datacenter to support new XML-aware applications.
Forum solutions are unique because they rely on an adaptive approach to security, fitting your current application and network requirements and not vice-versa. Because security is not a one-size fits all proposition, you must begin by analyzing your specific risks, then determine the security features you really need.

### Security Management

<table>
<thead>
<tr>
<th>Security Challenges</th>
<th>Authorization</th>
<th>Discovery, Description, &amp; Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEGRITY &amp; PRIVACY</td>
<td>Trust Management</td>
<td>Dynamic Web Services</td>
</tr>
<tr>
<td>Strong authentication</td>
<td>Information Assurance</td>
<td>Collaboration &amp; Orchestration</td>
</tr>
<tr>
<td>Federated security</td>
<td>Federation</td>
<td>Federation</td>
</tr>
<tr>
<td>Federated security</td>
<td>Automation</td>
<td>Admisison Control</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure integrity of messages</td>
<td>Filter for malicious content</td>
</tr>
<tr>
<td>Ensure business interoperability</td>
<td>Ensure business interoperability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Features</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Management</td>
<td>Discovery, Description, &amp; Integration</td>
</tr>
<tr>
<td>FTPS</td>
<td>Dynamic Web Services</td>
</tr>
<tr>
<td>WS-ReliableMessaging</td>
<td>Federation</td>
</tr>
<tr>
<td>Strong authentication</td>
<td>Automation</td>
</tr>
<tr>
<td>Federated security</td>
<td>Security Challenges</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Levels</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small / Simple</td>
<td>Trust Management</td>
</tr>
<tr>
<td>Medium / Advanced</td>
<td>Authorization</td>
</tr>
<tr>
<td>Large / Sophisticated</td>
<td>Discovery, Description, &amp; Integration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standards</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML 1.0</td>
<td>XML Schema</td>
</tr>
<tr>
<td>SOAP 1.1/1.2</td>
<td>XML Encryption</td>
</tr>
<tr>
<td>WS-I Basic Profiles</td>
<td>WS-Policy</td>
</tr>
<tr>
<td>XML Antivirus</td>
<td>WS-Trust</td>
</tr>
<tr>
<td>WS-Addressing</td>
<td>WS-Security</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>SAML</td>
</tr>
<tr>
<td>X.509 Certificates</td>
<td>WS-RP</td>
</tr>
</tbody>
</table>

---

**Forum Enterprise SOA Security: Adapting to the Needs of the Enterprise**

Forum solutions are unique because they rely on an adaptive approach to security, fitting your current application and network requirements and not vice-versa. Because security is not a one-size fits all proposition, you must begin by analyzing your specific risks, then determine the security features you really need.
Forum Government Solutions

Forum Systems is committed to state and federal governments by offering products that meet infrastructure requirements, government mandates as well as compliance criteria and certifications.

Forum Systems is listed on an approved GSA Schedule and is able to sell its solutions directly to the government market. Forum’s inclusion as a GSA Schedule Vendor allows government customers to obtain special and approved pricing and license terms from a trusted vendor. Forum also has strong relationships with key System Integrators (SIs), and Government Solutions providers that have expertise in and established partnerships with government organizations.

Forum Sentry™ 1504G Gateway is the first and only Web Services Security solution in the market to provide both JITC DoD PKI certification and Federal Information Processing Standard (FIPS) 140-2 Level II validation, delivering comprehensive information assurance for XML, Web Services, and SOA.

- FIPS (Federal Information Processing Standard) is a US Government certification program that prescribes detailed security requirements for cryptographic-based systems when used within US Federal agencies.

- Common Criteria EAL 4+ Certification is a set of internationally recognized guidelines that provide a consistent standard for evaluation security products, validated jointly by the National Information Assurance Partnership (NIAP) and the COACT, Inc. Common Criteria Test Lab (CCTL).

Forum Education Services

Forum Education Services empower organizations with the skills, tools, and processes to succeed along their SOA roadmap.

Training programs are designed to address the unique challenges around Enterprise SOA deployments and are customized to the pace of each organization covering topics such as:

- Web Services Security
- Enterprise Identity Management
- Policy, Governance, and Compliance
- XML Acceleration
- Risk Reduction

Forum Solutions are designed to meet the following Federal Standards and Certifications:

Infrastructure Requirements
- JITC DoD PKI
- FIPS 140-2 Level III Key Management
- Common Criteria EAL 4+
- e-Government Authentication
- Federal Enterprise Architecture
- Check Point OPSEC Certification

Mandates and Strategies
- Home Land Security
- Information Assurance
- eGov initiative
- Improving Efficiency

Compliance and Directives
- CNSS Policy N# 15
- NSTISSP #11
- NCES (Net-Centric Enterprise Services)
- DITSCAP
- EGA (E-Government Act)
Forum Fortified Program

Enterprises are looking to protect the entire breadth and depth of the application and network stack to enable integrated and consolidated XML security, processing, and networking. Forum Systems products are available as embeddable technologies through the Forum Fortified™ Program for OEM, hardware/software systems integrators, and channel partners.

BOSTON:
95 Sawyer Road, Suite 110, Waltham, MA 02453

SALT LAKE CITY:
45 West 10000 South, Suite 415, Sandy, UT 84070

www.forumsystems.com

Putting together the security, acceleration, and management pieces for the world’s most demanding enterprises