



# SecureSpan™ XML Data Screen

Guard against the growing threat of cyber attacks

The SecureSpan XML Data Screen offers:

## Policy-based Protection

Minimize maintenance costs by enforcing common data screening requirements for all application services in policy instead of code.

## Secure Services According to Risk

Reduce overhead by screening all incoming data and processing, rejecting or passing through messages appropriately, according to the risk they present.

To learn more about Layer 7 and how it can address your organization's SOA and Web services needs, call 1-800-681-9377 (toll free within North America) or +1.604.681.9377

**Intercept problematic messages before they reach your services.**

## Threat Prevention

Message-based XML, REST, AJAX and other Web 2.0 traffic presents new vectors of attack for malicious hackers – vectors that cannot be thwarted by traditional means. Existing security measures like network firewalls can't protect against message-borne threats since they lack the ability to inspect XML-based messages, validate XML structures or detect anomalous XML content. Similarly, network-based VPNs (whether SSL or IPSec) can't preserve a message's integrity and privacy as it gets passed across multiple service hops in an SOA transaction. Moreover, VPNs can't provide a message level audit trail or non-repudiation across an SOA transaction.

The SecureSpan XML Data Screen is specifically designed to protect XML, Web services and Web 2.0 applications from damage, downtime or improper information. Whether deployed in the enterprise or in the cloud, the Data Screen can cleanse XML data streams of threats, vulnerabilities and unauthorized content for all common XML message formats, including POX (Plain Old XML), SOAP, REST and AJAX.

Acting as a content filter, the XML Data Screen can be configured to scan, expurgate or transform malicious or malformed data, classified or unwanted "dirty" words, and AJAX generated scripts. Policies can be defined to remove, block or transform illegal data or entire messages. Traffic to specific endpoints can be restricted or throttled based on user defined traffic limits, data formats, or REST-based URLs. HTTP headers and form data can be validated, transformed or removed as required. The XML Data Screen also protects applications from XML Denial of Service (XDoS) and other parser-based exploits, assuring the continuous availability of service endpoints.

## Services Protection

The first step in protecting mission-critical application services is to ensure that all incoming messages are screened for potential threats not only to the downstream service, but to the protection infrastructure itself. Some of these threats may be the result of poorly designed or poorly implemented client-side code, while others may be malicious. In either case, organizations require the flexibility to identify and react to common threats on a message-by-message basis.

Some common threats addressed by the XML Data Screen include:

- Parameter Tampering
- Coercive Parsing
- WSDL Scanning
- External Entity Attacks
- Replay Attacks
- Recursive or Oversized Payloads
- Schema Poisoning
- Routing Detours
- SQL or XQuery Injection
- XML Morphing

| Key Features  |   |
|---|---|
| Threat Protection   |   |
| Filter XML content for Web 2.0 and SOA  | <ul style="list-style-type: none"> <li>Configurable validation and filtering of HTTP headers, parameters and form data</li> <li>Detection of classified word, “dirty” words, or arbitrary signatures with subsequent scrubbing, rejection or redaction of messages</li> </ul>   |
| Prevent XML attack and intrusion  | <ul style="list-style-type: none"> <li>Infrastructural protection against XML parsing, XDoS and OS attacks</li> <li>Application protection against XML content tampering and viruses in SOAP attachments</li> <li>Protection against SQL and malicious scripting language injection attacks</li> <li>Configurable throughput restrictions based on requestor or destination prevents downstream XDoS</li> </ul> |
| Secure REST and AJAX  | <ul style="list-style-type: none"> <li>Support for XML, SOAP, POX, AJAX, REST and other XML-based services</li> <li>Configurable scrubbing or rejection of AJAX or other messages with embedded scripts or privileged commands</li> </ul>   |
| Validate data structures  | <ul style="list-style-type: none"> <li>Content detection within XML data structure or across entire message</li> </ul>  |
| Set traffic limits  | <ul style="list-style-type: none"> <li>Allow/reject messages based on time of day, day of week and IP address</li> </ul>  |
| XML Acceleration  |   |
| Accelerated XML message processing offload  | <ul style="list-style-type: none"> <li>High speed message transformations based on internal or external XSLT</li> <li>High speed message validation against predefined external schema</li> <li>High speed message searching, element detection and content comparisons</li> </ul>  |
| Optional hardware-based acceleration  | <ul style="list-style-type: none"> <li>ASIC-based hardware accelerator can be optionally used to maximize message throughput and minimize processing latency</li> </ul>   |
| Enterprise-scale Management   |   |
| Operations Console  | <ul style="list-style-type: none"> <li>A single, real time view of all Gateways across the enterprise and cloud showing audits, events and key metrics</li> </ul>   |
| Policy Migration  | <ul style="list-style-type: none"> <li>Centrally move policies between environments (development, testing, staging, production, etc), settings (enterprise, cloud, etc) or geographies, automatically resolving discrepancies such as SSG licenses, IP addresses, IT resources (i.e., LDAPs may be named differently), etc</li> </ul>   |
| Services Reporting  | <ul style="list-style-type: none"> <li>Configurable, out-of-the-box reports provide insight into SSG operations, service-level performance, and service user experience</li> </ul>  |
| Remote Patching   | <ul style="list-style-type: none"> <li>Selectively update any software installed on Gateways, including system files and operating system</li> </ul>  |
| Disaster Recovery   | <ul style="list-style-type: none"> <li>Centrally back up SSG config files and policies from one or more Gateways/clusters, and remotely restore, enabling full disaster recovery</li> </ul>   |
| Management API  | <ul style="list-style-type: none"> <li>Remote management APIs allow customers to hook their existing, third-party management tools into the SSG, simplifying asset management</li> </ul>  |
| Supported Standards   |   |
| XML 1.0, SOAP 1.2, REST, AJAX, XPath 1.0, XSLT 1.0, WSDL 1.1, XML Schema, LDAP 3.0, SAML 1.1/2.0, PKCS #10, X.509 v3 Certificates, FIPS 140-2, Kerberos, W3C XML Signature 1.0, W3C XML Encryption 1.0, SSL/TLS 1.1 / 3.0, SNMP, SMTP, POP3, IMAP4, HTTP/HTTPS, JMS 1.0, MQ Series, Tibco EMS, FTP, WS-Security 1.1, WS-Trust 1.0, WS-Federation, WS-Addressing, WSSecureConversation, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, WS-PolicyAttachment, WS-SecureExchange, WSIL, WS-I, WS-I BSP, UDDI 3.0, XACML 2.0, MTOM |   |

To learn more about how Layer 7 can address your needs, call us today at +1 800.681.9377 (toll free within North America) or +1.604.681.9377 or visit us at [www.layer7tech.com](http://www.layer7tech.com).