zapthink white paper

SECURING & MANAGING XML & WEB SERVICES IN THE ENTERPRISE

Jason Bloomberg and Ron Schmelzer, Senior Analysts, ZapThink LLC

Abstract

There are two related forces that are transforming information technology today: the rapid growth of XML traffic on the network, and the widespread adoption of Web Services as a way of reducing the cost of integration and moving traditional enterprise architectures to flexible, Service-oriented architectures. Enterprises must plan ahead if they want to be able to manage the XML and Web Services on their networks. Even more importantly, enterprises must take care to provide uninterrupted security for their IT environments. In the face of these changes, XML and Web Services introduce new security concerns for the IT manager, and new technology tools, including XML firewalls, offer the missing pieces of security that today's enterprises need.

New Problems for the Network

The amount of XML traffic on the network is set to explode.

There is a sea change occurring in today's information technology environment. XML is becoming the lingua franca of information on the network, and Web Services herald a new, open standards-based approach to getting computers to talk with each other. As a result, the amount of XML traffic on the network is set to explode. These changes promise to enable IT to deliver substantially greater value to the businesses that rely on information than the closed, proprietary technologies that came before. However, with these positive changes come new risks and problems, as well. It is essential for today's enterprise to understand both the benefits that XML and Web Services can bring to the business, but also understand the changes that IT organizations must make to accommodate new approaches to computing and the risks associated with those approaches.

This report details the changes to today's IT environment that XML and Web Services introduce, and then discusses the new XML management and security tools coming to market that address the problems that these changes present. In particular, this report covers:

- The business drivers in the industry. What are the specific problems that face IT departments as a result of the burgeoning use of XML in the enterprise?
- What technologies and tools are coming to market that address these issues?
- How should an enterprise decide what solutions they need, and when?

Business drivers for XML management and security tools

The increasing use of XML in the enterprise presents a number of business drivers that are spurring the adoption new XML-aware tools and technologies. As this report discusses in detail below, these drivers include:

- The need to manage the increased volume of XML network traffic
- The need to continue to provide security across the network
- The desire to establish a consistent XML usage policy across the enterprise
- The need to increase flexibility and agility within the enterprise, by increasing the value of the XML and Web Services on the network.

As XML traffic increases on the network, enterprises will need specialized applications to achieve the desired economies of scale.

Managing increased volume of XML traffic on the network

One of the major drivers for the adoption of XML management and security tools is that as XML traffic increases on the network, enterprises will need specialized

applications to achieve the desired economies of scale. In distributed systems, there are fundamentally two types of entities: those that are providing functionality (servers or service providers), and those that are requesting functionality (clients or service requesters). In a traditional system, service requesters send messages directly to providers, which respond with the results of the requested operation. While this client/server approach works in limited volume environments, the direct request-response model does not scale well.

Traditional firewalls are not able to distinguish when XML traffic is malicious or unauthorized.

Continuing to provide security across the network

Traditional firewalls are *packet-based*: they understand the traffic that hits their ports in terms of the origin and destination of the packets, rather than the content of the messages contained in the packets. Some firewalls have some visibility into the content of the traffic they encounter in order to filter viruses and other harmful content, but these filters work simply by looking for recognizable patterns of bytes that indicate malicious content. Content in XML form, however, contains structure and meaning. XML traffic to or from Web Services can also contain instructions for internal systems within the enterprise. Traditional firewalls, however, are not able to distinguish when such traffic is malicious or unauthorized.

Enforcing corporate XML policies and normalizing XML implementations

Enterprises also need XML management and security tools that can also allow users to implement XML and Web Services solutions without having to frequently modify those applications to comply with various corporate XML policies. These policies may affect the security, management, performance, and vocabulary features of the XML documents. For example, an enterprise may stipulate that all XML messages bound for outside the network must be compressed, digitally signed, and compliant with ebXML specifications.

Increasing flexibility and agility within the enterprise

As XML becomes an increasingly important part of the corporate IT fabric, IT administrators, managers, and CIOs will be able to wring more value out of their XML traffic. For example, they may want more in-depth reporting and auditing of XML traffic, message-tracing facilities, billing and metering functions, and other functionality that will increase the flexibility of the IT organization, leading to an enterprise where the technology responds quickly and efficiently to changes in the business environment—what we call the agile enterprise.

The growth of XML

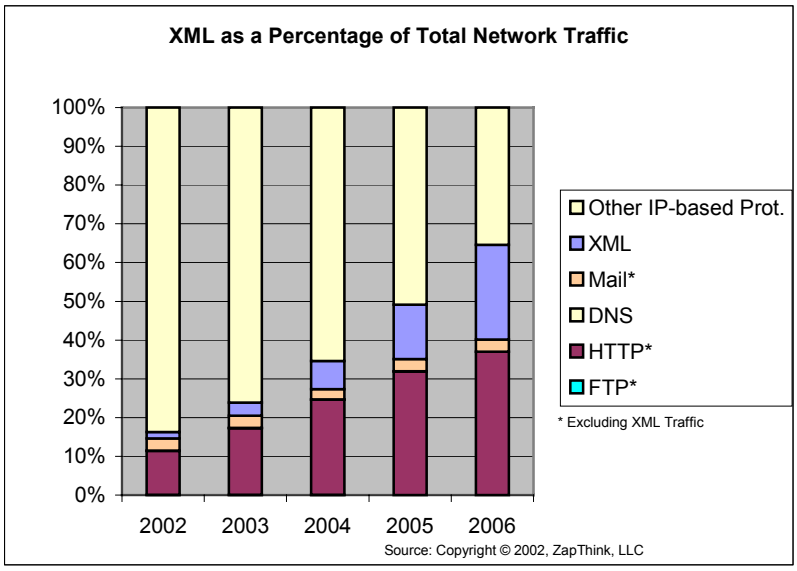
XML has already become established within the enterprise as a fundamental tool for addressing a wide range of problems: document creation and management, Web content management, simplification of integration, B2B communication, and more. Web Services, in particular, are gaining rapid acceptance within the enterprise, which also contributes to the increasing use of XML. As a result, ZapThink expects XML traffic on the corporate network to greatly increase over the next few years. Currently, ZapThink estimates that XML represents less than 2% of all network traffic on the network in 2002. However, we expect this percentage to increase to just under 25% of all LAN network traffic by 2006. The following chart and diagram show the expansion of network traffic over the next few years.

Table 1: Percentage utilization of Network Traffic by format

Protocol	2002	2003	2004	2005	2006
FTP	0.06%	0.06%	0.04%	0.03%	0.02%
HTTP	11.33%	17.06%	24.17%	31.42%	36.57%
DNS	0.08%	0.07%	0.06%	0.04%	0.03%
Mail	3.16%	3.81%	4.32%	4.49%	5.18%
XML	1.60%	3.34%	7.09%	13.83%	24.15%
Other†	83.73%	75.64%	64.30%	50.17%	35.04%

Source: Copyright © 2002 ZapThink, LLC

Figure 1: Growth of XML as Percentage of Network Traffic†



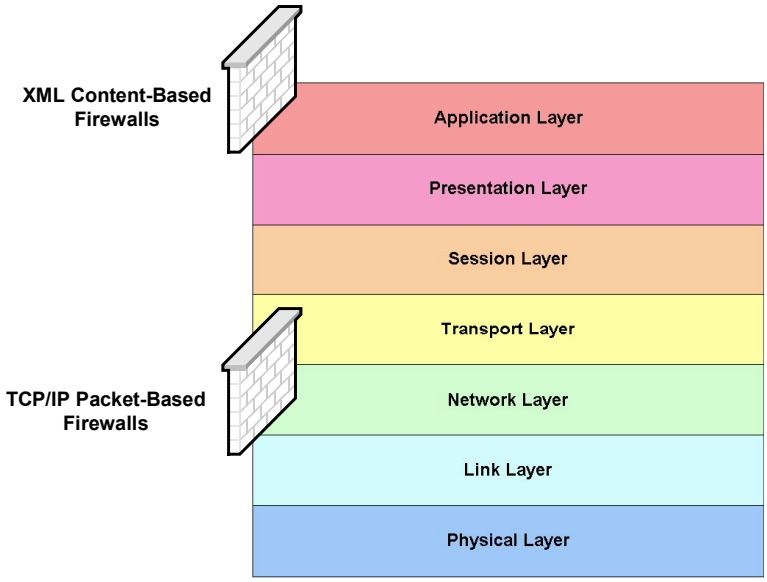
(†Other IP-based protocols includes instant messaging, file and print sharing protocols, IP-based RPC protocols, P2P formats, and proprietary messaging formats).

This explosive growth of XML on the network is the primary technical driver for the adoption of XML management and security solutions across the enterprise.

Why current network protocol-based solutions are not adequate to handle XML traffic

To understand why XML is such a problem for existing security and management technologies on the market, it is important to understand how network protocol-based solutions work. All network technology relies on the Open Systems Interconnection (OSI) Networking Model, as shown in figure 2:

Figure 2: The OSI Networking Model



A wide variety of hardware products participate on the lower levels of the OSI stack. These devices include routers, switches, gateways, bridges, hubs, and firewalls of all types. However, all of the core protocols for Internet applications, including HTTP, SMTP, FTP, and telnet, operate in the application layer at the top. What layer of the stack, therefore, do the emerging XML and Web Services protocols such as SOAP, WSDL, and UDDI operate? This question is difficult to answer since these specifications are primarily *content-oriented,* rather than *protocol-oriented*. While a case can be made that SOAP is a message format, the OSI model is inadequate to describe the nature of most XML formats. While the OSI model is still a mechanism to assist in the understanding of traditional networking products, new *content-aware* networking products must transcend the limited OSI model and focus not on the message packet or envelope, but rather on the content of the message itself.

New content-aware networking products must transcend the limited OSI model and focus on the content of the message itself.

In order to process high volumes of XML content on the network, hardware and software devices must able to understand not only network protocols, therefore, but also the XML-based content traveling on these protocols. Current TCP/IP-based firewall and router solutions that operate in the middle of the OSI stack are typically put to use in a corporate network by presenting just a single point of access to the outside world, thus hiding the real structure of the corporate network from intruders. These firewalls work by blocking access to all network traffic, except ones that run on certain TCP ports such as web traffic (HTTP port 80 and HTTPS port 443) and email traffic (SMTP port 25). Firewalls can also ban all network access by hosts at certain IP addresses or based on certain usage characteristics. These firewalls operate by either static packet filtering (making simple deny or allow choices depending on the network address of the packet) which is cheap and fast, or Dynamic Packet Filtering/Stateful Inspection, which makes its decisions based on all the data in the packet.

However, the TCP/IP port model is too simplistic for dealing with XML-based content and Web Services traffic in particular. While Stateful Inspection based systems to some extent monitor packet traffic, most Web Services run over standard network ports such as HTTP and HTTPS. However, TCP/IP-based firewalls are programmed to permit or deny all traffic through these ports, and XML/Web Services traffic might be undesirable at the content-level, unlike

standard HTTP traffic. As such, firewalls will need to become aware not only of the network ports and IP addresses, but also of the content itself that is traveling across the network. In this regard, current firewall, router, proxy, and switch solutions are inadequate. Instead of being simply network and IP-aware, these solutions must be *content-aware*. More specifically, they need to be XML-aware. They need to be able to inspect and understand XML traffic as it flows across the network and perform some sort of activity on the traffic, as the appropriate policies dictate.

The XML processing challenge

As the use and proliferation of XML and Web Services spreads throughout the corporate IT environment, so too will the demands on optimizing the performance of processing and handling the XML data and applying enterprise-wide XML policies. In addition, XML is creating new exposures—security, performance, and otherwise—that corporate IT environments must appropriately deal with. In particular:

- *XML is inefficient* – XML messages consume significantly more bandwidth than other protocols and message formats. This verbosity is primarily due to the fact that XML is a text-based, human-readable language. A SOAP message will be substantially larger than a corresponding binary-format remote procedure call.
- *XML transformation is processor intensive*– XML messages that are destined for a presentation format such as HTML, WAP, or some another XML format must be transformed using XSL or similar methods. In particular, Web sites that are based on XML will require XSL transformation on the fly, increasing parsing and processing loads on servers.
- *XML is insecure* – Due to XML's human readable nature, it is particularly vulnerable to security compromises. As a result, any XML message, including SOAP messages, must be enhanced with security features including encryption, digital signatures, authentication mechanisms, and privacy controls. These features will further add to an XML message's bulkiness.
- *Most networking devices do not understand XML formats* – XML by itself is just a document format and not a messaging protocol. SOAP, ebXML, and other specifications add routing and other messaging capabilities to the format. Intermediaries must understand these messaging formats and therefore must be able to parse, process, and understand the specific routing requirements of different XML vocabularies.

XML security and the shift to Service-oriented computing

The shift from focusing on packet level network security to application level security that is aware of the content of messages is one of the many changes facing an enterprise as it implements Web Services. There are many levels of change facing IT in the enterprise, and each type of change has security implications associated with it. In addition to the need for firewalls to be application and content aware, there are changes at the system level as closed, proprietary systems give way to open, loosely coupled systems. Closed systems are relatively straightforward to secure; an administrator need only set up the users and their privileges, and the work is mostly complete.

Securing open, loosely coupled systems requires a much more sophisticated security approach, involving multiple administrators that support distributed users. Different systems now have different policies and possibly different

security mechanisms. As a result, administrators must manage security much more actively than was necessary in the closed model.

Traditional distributed computing security was modeled by *islands of security*, which describe systems and users on isolated networks or subnetworks. The network acted as an island, with its own perimeter security, but users within the network were considered to be trusted. This "trusted vs. untrusted" dichotomy breaks down in a Service-oriented model, because users can access Services located on systems across one or more enterprises. The concept of trusted groups no longer has meaning; instead, enterprises must institute policies that apply to their entire enterprise network (including participants invited from outside), and administer that security in a tiered, or hierarchical fashion. Departments or other organizational groups may then have their own administrators, but those administrators may in turn be administered by a more senior admin at a higher level within the enterprise.

Enterprises must institute security policies that apply to their entire enterprise network (including participants invited from outside), and administer that security in a tiered, or hierarchical fashion.

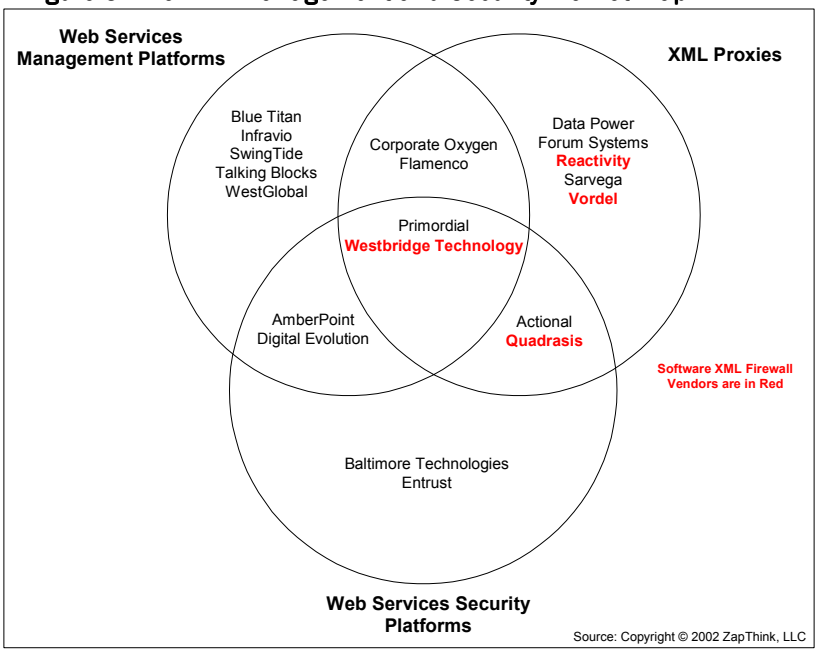
An Emerging Market of Solutions

All of these market forces and business drivers—the growth of XML traffic, the need for content-aware network technologies, and a deeper level of security across the enterprise—have led to many new tools and technologies on the market that vendors have designed to handle the new class of XML management and security problems. As a result, there is a substantial amount of confusion in the marketplace, as many vendors toss their hats into the ring, each with their own marketing message and product positioning. To help make sense of this situation, this report sorts the prominent vendors in the XML management and security space into three basic categories:

- *Web Services Management Platforms* – products that focus on helping enterprises manage Web Services and other XML traffic on production networks.
- *XML Proxies* – products that act as XML intermediaries, taking active roles on the network to provide content-aware security, routing, or transformation capabilities.
- *Web Services Security Platforms* – products that focus on securing corporate networks, both by securing the XML and Web Services traffic on the network, as well as using the power of Web Services to enhance enterprisewide IT security.

Part of the confusion surrounding these categories is that many vendors offer solutions that fall into two or more of these categories. Figure three illustrates these three categories, showing the overlaps among each category as well as prominent vendors in each of the categores. The report explains each of these categories following the figure.

Figure 3: The XML Management and Security Market Map



Web Services Management Platforms

The concept of a *platform* is a set of technologies that underlie a variety of applications and services and provide several basic services to those applications and services. Web Services management platforms typically share many of the following features:

- *Business activity monitoring and business-level management* – enabling business managers to review information about business processes, for example, the number of orders or shipments, and take actions based on that information.
- *Operations monitoring* – enabling operations personnel to monitor system-level activity such as performance, throughput, and availability of Web Services. Operations monitoring includes Quality of Service monitoring and service level agreement (SLA) monitoring.
- *Live upgrades and version control* – enabling non-intrusive updates to production systems by enabling the toggling between test and production environments, exception handling, data mapping and transformation, and developer control of systems.
- *Service request prioritization and dynamic routing* – the ability to act as a "traffic cop" for network traffic, routing and prioritizing traffic based upon established policies.
- *Auditing and logging capabilities* – the automatic recording of relevant activities and events across systems.

Enterprises should consider a Web Services management platform when they plan to have several mission-critical Web Services in production. Typically, enterprises will also want security management capabilities as well, and thus many companies will opt for solutions that manage security as part of the management platform.

Web Services Security Platforms

A Web Services security platform focuses on securing Web Services across all tiers (data, application, and presentation) as well as all networks (internal, DMZ, and public) in the enterprise. It is important to note that Web Services security platforms both secure Web Services, as well as use Web Services technology to secure other aspects of companies' systems. Web Services security platforms typically share many of the following features:

- *A security policy engine* – coordinates security and privacy policies across multiple systems.
- *A trust server* – integrates with an enterprise's existing trust management system, managing keys and certificates, and serving as a registration and assertion server.
- *An access control system* – supports authorization policies based on the context of the request, authorizing both inbound requests and outbound responses. Typically enforces system-wide access control, and leverages existing authentication systems.
- *A policy engine* – a centralized repository of all security policies that apply to the company's XML and Web Services traffic, with the appropriate administrative tools.
- *Integrates with single sign-on capabilities* – for companies that have single sign-on software that enables users to log on to one system and have their credentials accepted by other systems, a Web Services security platform will integrate with and often extend the single sign-on capability.

While Web Services security platforms coordinate security across the enterprise, they are not a complete Web Services security solution, because they do not intercept XML messages. XML firewalls, which are a kind of XML proxy, serve that role.

XML Proxies

XML Proxies are applications or devices that monitor network traffic for XML content and perform some activity on that traffic as dictated by business rules. We define XML Proxy as follows:

XML Proxy: Hardware or software solutions that actively listen for XML traffic on the network and either pass it along unmodified or perform some action on the XML content.

XML Proxies are capable of examining traffic at the content level, and can optionally handle other document types such as HTML or EDI content. They must be XML-aware, but are not necessarily specific to any one XML vocabulary (such as Web Services or ebXML). We distinguish XML Proxies from other types of network intermediaries in that they are XML-aware, while others may be TCP/IP aware or HTTP aware. However, other than the fact that XML Proxies facilitate (intermediate) XML communications and are capable of processing XML documents, the role that XML Proxies fill varies depending on the activity they perform on the XML content.

XML Proxies typically offer some or all of the following functionality:

- *Message Routing* – directing XML traffic to different destinations, based on the content of the messages, existing policies, or some combination.

- *Security* – rejecting part or all of certain messages because of some security breach, for example, an unauthorized sender.
- *Performance Enhancement* – simple acceleration of the messages.
- *Message Transformation* – transforming messages, typically with the use of style sheets, for performance enhancement, consistency, or compatibility purposes.

Different Types of XML Proxies

There are two primary ways that enterprises can implement XML Proxy solutions: in dedicated hardware (XML network appliances) or in specialized software (software XML proxies). These approaches are not mutually exclusive—there are distinct scenarios in which hardware implementations are most appropriate, other scenarios where software is best, and yet others where combinations of hardware and software solutions are optimal.

Hardware XML Network Appliances

There exist a rapidly growing segment of vendors who are applying dedicated hardware technology for XML Proxy solutions. These vendors are creating specialized software and hardware combinations that can fit within traditional IT rack environments. There are a number of scenarios where XML Network Appliances are the most appropriate implementation of XML Proxy solutions:

- *Performance* –hardware solutions that accelerate encryption, parsing, and transformation operations.
- *Controlled Installation Environment* – IT personnel can preconfigure network appliance solutions so that they are ready to install.
- *Centralized installation*– allow developers to pass off device administration and maintenance responsibilities to IT administrators.

Software XML Proxies

Another key option for implementing XML Proxies is to implement software solutions that reside on servers on the network. These software solutions provide a flexible mechanism for processing XML traffic without having to purchase dedicated hardware. In addition, these solutions can leverage application servers and other Web Services execution environments, providing a greater level of integration with the XML creation environment. Software XML proxies offer:

- *Installation Flexibility* – IT personnel can install software XML proxies in a variety of ways, including on the same machine as existing application servers, on department or division-level servers, or as a separate test or pre-deployment system. Software systems leave their implementation details up to the user, allowing for different hardware choices for scalability and robustness.
- *No need to get central IT involved* – Since implementation choices are left to the user, only department or division level IT personnel must be involved in the purchase and installation process.

XML Firewalls

An important type of software XML proxy is the *XML firewall*. A firewall is a device that acts as a message intermediary, inspecting the traffic that attempts to pass, and either allows or rejects the traffic based on a range of criteria. Traditional hardware firewalls inspect traffic on the packet level, and as such cannot reject

traffic based on the structured content (for example, XML-formatted content) it contains. XML firewalls, on the other hand, are capable of understanding the content that pass through them and appropriately managing that traffic.

These firewalls typically operate by inspecting SOAP message headers. If a header has instructions for the XML firewall (which may or may not be signed), the software can make routing decisions based upon those instructions. Even for the part of the SOAP message not intended for the firewall itself, the software firewall may be able to decrypt part or all of the message and make routing or other policy decisions based upon the secure contents of the message.

XML firewalls typically offer several of the following features:

- SOAP message and other XML message inspection
- Malicious attack protection and intrusion detection
- Authentication and authentication capabilities
- Decryption and encryption capabilities
- Non-repudiation capability
- XML Schema and XPath-based rule enforcement
- Real-time monitoring and reporting, typically via a Web Services interface.

Content-aware XML firewalls can provide more value to the enterprise than traditional packet-based firewalls because they can understand and utilize detailed metadata about both the operation and the service requestor.

Furthermore, content-aware XML firewalls can provide more value to the enterprise than traditional packet-based firewalls, not only because they understand the XML content that is in the messages, but also because they can understand and utilize detailed metadata about both the operation and the service requestor. For example, XML firewalls can understand the following metadata:

- Attributes of the service requestor that it retrieves from certificates or user directories
- The role of the service requestor in the context of the current request
- The access control lists at the operational level that are relevant for the given service requestor, operation and context
- Attributes of the operation and Web Service being accessed
- Knowledge about what categories the current operation belongs in as well as the attributes of that category.

The Enterprise Adoption Roadmap for XML Management and Security Tools

The adoption of Web Services today has an internal enterprise focus. Enterprises primarily use Web Services to simplify and reduce the cost of integration inside the firewall. Some companies are exploring the use of Web Services to communicate outside the firewall, but these instances are often pilot projects, and are typically with trusted business partners and known IT organizations. The primary reason for this tentative approach to B2B use of Web Services is the concern for security at the edge of the network. Therefore, enterprises who have begun internal Web Services projects and are looking to extend the power of Web Services to trusted business partners should consider an XML firewall solution.

As enterprises increase their use of Web Services, both within the enterprise and with business partners, suppliers, and customers, they should look for more comprehensive security and management platform solutions. Such solutions won't be separate from existing IT infrastructures; instead, companies will find

such solutions to be critically necessary for managing systems and security across the enterprise, as they move toward a Service-oriented environment.

A focus on security is critical

Security solutions address risk, and risk by its very nature implies uncertainty. There are some fundamental principles of risk and security that all companies must follow:

- There is no such thing as perfect security. Perfectly secure networks and systems are an impossibility. The most secure system is one that is turned off, and even that can be compromised.
- It is likewise impossible to write a list of all the risks presenting a company. No matter how complete an attempt at such a list might be, there is always the possibility of an entirely unexpected risk.
- Security is never complete. There will always be new vulnerabilities and new modes of attack. Security is an ongoing, ever-changing process.
- There is no way to accurately quantify the risks that security addresses. Any security failure may lead to unexpected costs and other consequences. Therefore, there is no way to accurately calculate the ROI of a security solution.
- Broad estimates of business losses due to security breaches do not apply to individual companies. Any company that believes it can proactively calculate its losses due to lack of security is simply fooling itself.

One conclusion to be drawn from the principles above is that any approach to security must be heuristic, or in other words, "seat of the pants," at some level. How much security is really enough? There is no truly objective answer to this question. Each executive must make their own decisions for their companies based upon their resources, personal experience and intuition.

How, then, will companies approach XML and Web Services security? When executives consider the current risks in the enterprise, they will look for the most cost-effective solutions that afford the subjective level of security that they wish to achieve. In some cases, XML-based security technologies will be a cost effective option for existing security infrastructures.

For companies building Web Services solutions, there is a clear transition point where security becomes a critical issue: when they begin to access and/or provide Web Services outside the enterprise firewall—in other words, when they begin projects where they do not control both endpoints of every SOAP message. Companies planning on using Web Services across the firewall will necessarily have to resolve the resulting security issues first with tools like XML firewalls.

Companies planning on using Web Services across the firewall will necessarily have to resolve the resulting security issues first with tools like XML firewalls.

Summary

The rapid explosion of XML and Web Services usage in the enterprise offers challenges to companies, as well as offering tools for addressing those challenges. Companies should look first at XML firewalls for providing intelligent content-level security. As their usage of Web Services grows, some companies will want additional functionality from XML proxies, depending on their particular needs. Enterprises should also look into Web Services security and management platforms, once their usage of Web Serivces reaches critical mass: when companies take a Service-oriented approach to IT and Web Services become integral to mission-critical processes.

About ZapThink, LLC

ZapThink is an IT market intelligence firm that provides trusted advice and critical insight into XML, Web Services, and Service Orientation. We provide our target audience of IT vendors, service providers and end-users a clear roadmap for standards-based, loosely coupled distributed computing – a vision of IT meeting the needs of the agile business.

ZapThink's role is to help companies understand these IT products and services in the context of SOAs and the vision of Service Orientation. ZapThink provides market intelligence to IT vendors who offer XML and Web Services-based products to help them understand their competitive landscape and how to communicate their value proposition to their customers within the context of Service Orientation, and lay out their product roadmaps for the coming wave of Service Orientation. ZapThink also provides implementation intelligence to IT users who are seeking guidance and clarity into how to assemble the available products and services into a coherent roadmap to Service Orientation. Finally, ZapThink provides demand intelligence to IT vendors and service providers who must understand the needs of IT users as they follow the roadmap to Service Orientation.

ZapThink's senior analysts are widely regarded as the "go to analysts" for XML, Web Services, and SOAs by vendors, end-users, and the press. They are in great demand as speakers, and have presented at conferences and industry events around the world. They are among the most quoted industry analysts in the IT industry.

ZapThink was founded in October 2000 and is headquartered in Waltham, Massachusetts. Its customers include Global 1000 firms, public sector organizations around the world, and many emerging businesses. ZapThink Analysts have years of experience in IT as well as research and analysis. Its analysts have previously been with such firms as IDC and ChannelWave, and have sat on the working group committees for standards bodies such as RosettaNet, UDDI, CPExchange, ebXML, EIDX, and CompTIA.

Call, email, or visit the ZapThink Web site to learn more about how ZapThink can help you to better understand how XML and Web Services impact your business or organization.

ZAPTHINK CONTACT:

ZapThink, LLC
11 Willow Street
Suite 200
Waltham, MA 02453
Phone: +1 (781) 207 0203
Fax: +1 (786) 524 3186
info@zapthink.com