lustratus

Research

A Competitive Review of SOA Appliances

Comparing SOA appliances from Forum, IBM, Layer 7 and Vordel

Author: *Steve Craggs*

Version 1.00

October 2012

Table of Contents

Disclaimer

Whilst reasonable care and skill has been taken by Lustratus Research Limited (the company) in the preparation of this report no liability is accepted by the company (except in the case of death or personal injury caused by the company's negligence) by reason of any representation or any implied warranty condition or other term or any statutory or common law duty or otherwise howsoever arising for any direct or indirect general special or consequential damages or loss costs expenses or other claims (whether caused by the negligence of the company or otherwise) which come out of the provision of this report or its use.

All trademarks are acknowledged as the property of their respective owners.

Executive Summary

SOA appliances have matured considerably over the last few years. As they have established themselves more firmly in the SOA landscape, vendors have developed a better understanding of requirements, resulting in a level of commonality in some of the key underlying functions such as providing a secure gateway for accessing SOA services. However, technology never stays still, and recent years have seen a broadening of the SOA mission and the introduction of new use-cases to drive maximum value from corporate SOA investments. SOA services are being opened up to mobile and cloud applications as well as B2B trading partner usage, and the growing trend of exposing corporate APIs for third party application development is driving increasing levels of SOA activity.

This broadening of access makes it even more important to control and secure corporate services, and SOA appliances can play a vital role in protecting the corporate world from unauthorized usage or other forms of risk. But more than just a gateway, SOA appliances also offer a route to SOA simplification and TCO reduction by offloading and consolidating repetitive SOA activities onto purpose-built, cost-efficient and productive specialized platforms, and provide the logical point to control and manage SOA service authorization and usage.

This new assessment takes a look at the SOA appliances being offered by four leading vendors in the marketplace. In a change from the earlier Lustratus assessment in this area, only vendors offering hardware appliances are covered this time around; so-called ‘soft appliances’ just do not have the same security and TCO benefits to put them in the same class as the hardware appliance solutions. The vendors covered in this new assessment are Forum Systems, IBM, Layer 7 and Vordel. IBM and Layer 7 are survivors from the first Lustratus SOA appliances competitive assessment, while Forum Systems and Vordel have been added as other key players in the SOA appliances market.

Summarizing the content of this paper, Lustratus has come to the following conclusions:

- Forum Systems has an impressive, purpose-built hardware SOA appliance that makes an attractive SOA Gateway, but that is all it is. It is the most limited of the four in terms of overall functionality
- Layer 7 has done a lot to support the exposure of corporate APIs on top of its security strengths, although it lacks functionality in some other areas such as B2B support
- Vordel has extended its strong security and governance story into areas such as mobile usage and API exposure, but it is still best suited as a gateway rather than as part of a broader SOA deployment
- IBM has consolidated its leadership position by embracing new use-cases effectively while continuing to deliver the best opportunities for SOA simplicity and TCO reduction, especially in IBM mainframe installations

The table below rates each vendor based on the capabilities of its SOA appliance offerings in terms of security/governance, complexity/TCO reduction and ongoing value potential.

	Security and Governance	Reduction in Complexity / TCO	Value potential
Forum Systems	■■■■■■■■□□	■■■■■■■□□□	■■■■■□□□□□
IBM	■■■■■■■■■□	■■■■■■■■■□	■■■■■■■■□□
Layer 7	■■■■■■■■□□	■■■■■■■■□□	■■■■■■■■□□
Vordel	■■■■■■■■□□	■■■■■■■□□□	■■■■■■■■□□

Figure 1: Competitive summary of SOA appliance offerings

Introduction

In 2010, Lustratus produced a report entitled "A Comparative Review of SOA Appliances", assessing the merits of SOA appliances from three vendors – IBM, Layer 7 and Intel. This new version updates the IBM and Layer 7 content and adds two new vendors; Vordel and Forum Systems. Intel has been dropped from the list, because although it was useful to consider the Intel software-only offering against hardware appliance offerings at the time, companies now have a better understanding of the advantages of a dedicated appliance platform. As before, the purpose of this paper is to provide independent guidance for companies thinking about purchasing SOA appliances – dedicated servers designed to help with the challenges thrown up by adopting a service-oriented architecture. Before moving on to look at the offerings from each vendor and how they compare, it is worth spending some time reviewing the background and the current set of primary and emerging use-cases. While some of these use-cases are not specific to SOA, they all fit within the general umbrella of a services-based architecture.

Why appliances?

The appliance concept has been around for many years. At its most basic, it represents the idea of developing a purpose-built platform for a set of functions that can leverage both the specialized nature of functionality required and the dedicated nature of the assets included in the platform. Usually the platform chosen is a hardware / firmware package.

When is an appliance not an appliance?

As noted earlier, the first Lustratus report on SOA appliances included Intel as a vendor, with its 'soft appliance' concept of a software stack that was intended to be deployed on dedicated but general-purpose server platforms. The reason Lustratus has dropped Intel from this assessment is that although there are similarities, a 'soft appliance' is not in truth an appliance. Simply placing a software stack on a dedicated server leaves too many security holes and does not deliver enough TCO benefits for Lustratus to be comfortable including this approach in a review on SOA security appliances.

This leaves two other approaches to SOA appliances, both of which are covered in this report; a software stack on a general purpose platform that is then 'hardened', or a purpose-built, specialized platform. It is important to understand the distinction between these two fundamentally different models.

In the first approach, the security, connectivity, integration and optimization capabilities that make up the broad functionality of an SOA appliance are built using general purpose operating systems, databases and communications servers. The appliance package can now be built by 'hardening' the software/hardware combination. The source of the holes that make the 'soft appliance' concept inadequate, as discussed earlier, is the need for a general purpose systems software / server platform stack to fulfil a wide range of diverse needs. Flexibility and ease of access is required, allowing many functional options and easy software-based configuration, update and maintenance. In security terms, this is bad news since it opens up possibilities for error or malicious exploitation. So the 'hardening' approach involves taking measures such as blocking off various systems software and platform options, and limiting flexibility and ease of access/change. Software can be put into firmware and system options can be removed to make the appliance more secure and robust. In addition, this new hardened package now offers the opportunity to include additional hardware cards in the server for processor-intensive functions such as cryptographic acceleration, improving efficiency and performance.

However, the design point with this approach is a general purpose stack of hardware, operating system, database and communications software that fulfils the SOA appliance functionality. Closing off options and hardening the code into electronics reduces the inherent flexibility and hence the risk of system integrity being compromised, but to use an analogy it is like fighting with one hand tied behind your back.

Contrast this to the purpose-built appliance approach. In this case, the design point is to assemble a hardware/firmware stack (no software) designed from the start to be an SOA appliance and nothing else. Blocking off system software options may be fine for hardened appliances, but for example the code is still there to check if the options are enabled. Designing an SOA appliance from scratch, the option does not even need to be present since it would never be needed. Or another example; putting software into firmware may be fine, but if the appliance is not built to be tamper-evident then it is less protection than it seems. So with the purpose-built approach, the appliance can be built with maximum focus on efficiency, optimization, security and robustness for the specialized role which it is designed to play.

Of course there is a trade-off between the two different approaches. The purpose-built approach yields greater levels of robustness, security and performance optimization, but at the price of reduced flexibility; since the purpose-built appliance has been optimized specifically as a combined hardware/firmware package, that is the way it must be deployed. The general purpose platform design point sacrifices some of these characteristics in exchange for a more generic approach that could be deployed as a simple software stack or in a virtualized model, although of course there would be degradation in the level of service offered compared to the purpose-built solution.

Why SOA appliances?

Of course, appliances don't fit every need. In areas where significant amounts of custom coding are required, for instance, software may be the more appropriate choice. But appliances appeal strongly where a cost-effective workhorse is required to repeatedly execute a fixed range of functionality, or where security and governance are paramount.

SOA appliance use-cases

It is therefore no surprise that historically, one of the first uses of the SOA appliance concept was in providing security gateways. The secure nature of the appliance makes it ideal for deploying as a shield for protecting services from service consumers, either in the DMZ for external protection or in trusted zones for internal needs. In this role it also provided another very useful facility by offering a single point of management and control for all traffic coming in and going out of the enterprise. The other common use for SOA appliances was to consolidate SOA functionality onto a dedicated, pre-loaded and uniform platform, reducing support costs through simplification of the SOA topology and offloading repetitive work such as transformations, data mapping and XML parsing from the main business servers.

The use-case of SOA appliances within mainstream SOA deployments as illustrated above remains the most common, but as technology has continued to develop and the business service-oriented approach to computing has continued to gain mindshare, new use-cases have emerged for SOA appliances that expand their applicability to a broader range of needs.

One natural extension to the base SOA use-case is Business-to-Business (B2B) integration. This involves making SOA services available externally in much the same way as the basic use-case, but it brings additional challenges. For example, many industries define specific message format standards for B2B communications which will need transforming; also, B2B integration may well be at the file level rather than message level, requiring support for large payloads and FTP protocols. Beyond these execution considerations, B2B usually involves supporting trading partner profiles that can specify locations, business IDs, certification information for different locations and specific trading partner policy requirements.

Mobile computing is a more recent use-case. With the continued expansion of mobile device-based applications, more and more applications are looking to drive enterprise services as part of their functionality. But this can present a specific set of technical challenges. For example, mobile devices often use a wider range of connectivity styles and formats, such as JSON or REST. Not only is secure access required to the enterprise services, but also these protocols may well not match those expected by the corporate SOA services. As well as playing the secure gateway role, the mechanics of protocol switching are an ideal match to the capabilities of an appliance. But mobile considerations go much further than protocol bridging. Identity management is more complex, with standards such as OAuth and the challenge of having to consider not just user but device and application aspects of the requests. The root of the problem is that the lightweight operating systems used by mobile devices are necessarily less rich in security functionality. Another issue is that while it may be OK to have data reside on the client side of an SOA application, this is almost certainly not a good idea for mobile devices that could easily change hands quickly or unintentionally. All these security issues can be greatly mitigated by the use of a security gateway appliance.

In a similar vein, cloud computing also brings its own challenges around connectivity and security. While cloud is an attractive environment for some applications and services, the risk of exposing corporate data externally often leads to cloud applications having to integrate with on-premise services, with similar security and integration challenges. As in the mobile case, if the cloud environment is multi-tenanted then special care must be taken about what is left on the client side of the application and how the service consumer is authenticated.

Another related area that has gained some traction in some industries is that of API Management. For some companies, exposing their business functionality through an externally accessible API can stimulate third parties to build new client interfaces that embed these APIs, increasing the company's capabilities and reach dramatically. While this is not an area of interest to all, in the right circumstances it can be extremely valuable. In this use-case, the appliance plays the role not only of the security gateway but also as a monitor to measure and govern allocation and use of the corporate APIs and underlying services.

Functional areas

In order to support these use-cases, SOA appliances provide functionality across five broad areas. The key areas are:

- Security – protection from incoming threats, access control to ensure proper authorization, robust and tamper-proof platform to maintain integrity, enforcement of corporate security policies
- Simplicity – reduced skills and support requirements, SOA topology simplification, standard and uniform packaging, easy configuration, out-of-the-box operations, minimal maintenance/change requirements
- Price/Performance - optimized execution through purpose-built platform, specialized focus on process-intensive and repetitive activities, hardware acceleration, general business processor offload
- Connectivity – handling different connection protocols, mapping protocols between front and back ends, dealing with specific record formats, managing connection and partner profiles, providing adapters for specific applications and environments, ensuring connection availability and recovery
- Traffic management – authorizing and policing traffic content and volumes, measuring traffic usage and statistics, smoothing traffic surges and spikes, enforcing traffic policies, delivering traffic reports

Competitive assessment approach

The remainder of this paper assesses four SOA appliance vendors; Forum, IBM, Layer 7 and Vordel. The structure is laid out as follows:

1. Provide a high-level summary of functionality offered by each vendor
2. Set out some of the key decision factors driving SOA appliance investments
3. Consider and contrast each supplier's functionality in the light of these drivers

SOA Appliance Offerings

Having identified the key areas of functionality for SOA appliances, this now establishes a functional frame of reference for further review. However, it is important not to limit this framework to purely technical features. Instead, there are a number of ancillary aspects that need to be taken into account, such as how much time and effort will be required to deliver the expected benefits, how these SOA appliances are likely to affect overall total cost of ownership (TCO) and what level of flexibility the appliances offer. This section will therefore consider each SOA appliance offering in two categories; basic functionality that would be expected from any SOA appliance, and any added-value features. The table below summarizes some of the factors considered in each area.

Basic functionality	Value-Add
Security ■ Threat protection ■ Identity management ■ Secure and robust environment ■ Data privacy ■ Policy management and enforcement	Integration and Mediation ■ Transformation services ■ Intelligent routing ■ Data enrichment ■ Adapters to other environments / tools ■ B2B
Simplicity ■ Single point of control ■ Out-of-the-box functionality ■ Server consolidation ■ Deployment flexibility	Connectivity for Mobile and Cloud ■ Support for REST, JSON etc ■ Protocol and format mediation ■ Traffic flow management and control ■ Extended security
Price / Performance ■ XML/SOA processing design efficiency ■ Hardware acceleration ■ Quality of service levels ■ Traffic smoothing and throttling	API Management ■ API usage control and governance ■ Development lifecycle support ■ Monitoring and reporting ■ Protocol and format mediation
Ease of Use ■ Standards support ■ Configuration and administration tools ■ Ease of customization ■ Monitoring and reporting	Time to Value ■ SOA experience / availability of skills ■ Skills requirements ■ Pre-packaged configurations and options ■ Deployment options

Figure 2: SOA appliances functional capabilities framework

With this framework in mind, the SOA appliance solutions for each of the target vendors will now be summarized, and then their competitive positioning will be discussed. The four vendors covered, in alphabetical order, are Forum, IBM, Layer 7 and Vordel.

Forum Sentry

Background

Forum Systems was founded in 2001 and was acquired by Crosscheck Networks in 2009, where it is now operated as a wholly-owned subsidiary. It started off life with an XML Security Gateway product in 2002, offering policy-based XML security services including encryption, decryption and key management. It has since extended the functionality to cover a wider range of SOA appliance needs.

What is the Forum Sentry portfolio?

Forum Systems delivers solutions for a number of use-cases, but although it markets these solutions as individual products, the appliance itself is the same Forum Sentry XML Gateway. The packaging and marketing may differ, but the underlying technology is the same. The only difference in shipment of the Forum Sentry appliance is whether it includes the ASIC-based hardware acceleration for cryptographic functionality.

Forum Sentry products	
Forum Sentry XML Gateway Packaged / marketed as XML Gateway, Mobile Gateway, SOA Gateway, FTP Gateway and Identity Gateway	Connectivity and access control Threat protection Identity management Authorization, authentication and privacy management Policy-based security enforcement
Forum Sentry XML Gateway with ASIC Crypto Acceleration	XML Gateway + Hardware accelerated decryption and encryption
Forum Sentry Software	Software-based packaging of XML Gateway functionality for Linux, Windows and Cloud deployment

Figure 3:- Forum Sentry XML gateway products

As well as providing a purpose-built hardware appliance form factor, Forum also offers the functionality in a software package that can run on Linux, Solaris or Windows operating systems, available either for in-house or cloud usage. From the beginning, Forum adopted an Intel-based approach to its technology, although it also exploited specific cryptographic chipsets, and indeed in 2009 it was awarded a patent for some of its cryptographic technology.

Basic SOA appliance functionality

Security has historically been the prime focus for Forum Sentry. The company started out with an XML Firewall, and then expanded from there, increasing its identity management and cryptographic functionality to add value to its existing XML threat detection and security capabilities. Forum Sentry is FIPS 140-2 Level II certified.

Starting with access control, Forum Sentry offers a very granular level of authentication and authorization that can be implemented at the level of protocols, services and even messages. On the identity front it handles identity token mediation across different formats, as well as integration with external identity services such as CA Siteminder, IBM TAM, Sun JSAM, Microsoft Active Directory and others. The Forum support for standards includes support for WS-Security and X.509. Threat mitigation and protection is strong. At its heart, the Forum Sentry security gateway is an XML firewall, covering most XML and web threat types, such as SQL injection, XML Bombs and more general malware. Schema validation provides an additional level of protection. In addition, the Sentry appliance incorporates its own in-line antivirus engine for protection from specific viruses. Malicious messages are blocked and quarantined for later analysis if required. In addition, message content can be filtered through the use of XPath and regular expression support.

Forum Sentry offers centralized policy management for controlling security, access and encryption/decryption. The policy management tool is browser-based so that it can be used across deployments. For federated installations, the Sentry appliance supports policy mirroring across different instances, although it still provides centralized management of policies. Data privacy and integrity is handled through content-level message encryption and signatures. When deployed as a hardware appliance, Forum Sentry offers a tamper-proof environment with optional hardware mirroring for high availability.

The Forum Sentry technology provides optimized XML parsing and processing to increase the efficiency of XML handling. In deference to usage in environments where file transfer is to be used as the means of integration, such as in B2B scenarios, Forum Sentry also provides optimized support for handling large file payloads. However traffic flow control is fairly basic and mostly limited to front-end throttling.

As far as ease of use is concerned, Forum Sentry supports a wide range of security and connectivity standards, such as OASIS, NIST and SWIM. The main admin tool is a secure, web-based GUI. Access control can be allocated based on roles, and federated instances of Forum Sentry deployments can be managed from a single instance of the admin tool. Monitoring and reporting support includes a message capture / archive facility, general logging support, traffic statistics and integration with third party monitoring tools such as HP-OpenView, Oracle WSM and CA WSDM. Forum Sentry is available as a hardware appliance, but the functionality is also available as a software image for deployment onto other general purpose platforms or into the cloud, for example as an Amazon EC2 image. Of course, some features such as the cryptographic acceleration are not available in the software deployment option.

Value Add functionality

Forum Sentry offers a limited level of support for integration needs. Message transformation is all XSLT-based, while XPath is used to address routing needs. Data enrichment is supported through an external services interface, and in addition Sentry offers a regular expression matching facility. Sentry also provides a range of adapters to other environments; these include IBM WebSphereMQ, TIBCO EMS and Rendezvous and Sun Java Message Queue. The only support offered for B2B usage is support for FTP protocols and large payloads for file transfer.

Basic SOA appliance connectivity has been expanded to address some of the needs of other use-cases. So for example, JSON, REST and OAuth support has been added to Forum Sentry, as well as protocol and data mediation between JSON, REST, SOAP and XML environments. Service definitions can be exposed selectively to different consumers based on their identity credentials, and Forum Sentry also offers extensive cryptographic and PKI support to ensure data integrity and privacy. Forum offers a version of its Sentry hardware appliance that includes hardware-assisted cryptographic support to speed performance, as well as FIPS 140-2 compliant secure key storage and management. For support of highly loaded environments, Forum Sentry provides a range of traffic flow control facilities. Service SLAs, defined with the policy management tool, can be metered and enforced. The policy can also include payload, message size and rates limits. Traffic information can be gathered at a number of different levels; per user, per consumer or per group.

IBM DataPower

Background

In late 2005, IBM acquired DataPower, a US-based provider of appliances designed to improve security and performance of XML web services processing. DataPower was a pioneer in XML appliances, approaching the issue from the perspective of providing a purpose-built hardware appliance to drive better security and performance; as such, DataPower offerings are designed from the start to take advantage of hardware mechanisms such as application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs) and tamper-evident packaging. IBM has since expanded and evolved the DataPower portfolio of offerings to cover a broader array of SOA appliance use-cases and operates DataPower under its SOA-leading WebSphere brand.

What is the IBM DataPower SOA appliance portfolio?

IBM inherited a number of SOA appliances when it acquired DataPower, and this range has been expanded since the acquisition, demonstrating IBM's commitment to SOA appliances. With a considerable record of success over the last few years, IBM has evolved and refined its DataPower appliance portfolio to four key members:

IBM WebSphere DataPower Appliances	
WebSphere DataPower Service Gateway XG45 Also available in a Virtual Edition	Security gateway (AAA, XML threat, etc) Service level management and monitoring Intelligent load distribution & dynamic routing Lightweight integration functions (optional module) Slim 1U form
WebSphere DataPower Integration Appliance XI52 Also available in a Virtual Edition	XG45 + Full-scale integration functionality Mainframe integration and enablement High density 2U form for greater power
WebSphere DataPower Integration Blade XI50B / XI50z	XI52 available as a blade for either the IBM BladeCenter or the IBM zBX rack for IBM System z mainframes
WebSphere DataPower B2B Appliance XB62	XI52 + Partner profile management B2B messaging support (AS1, AS2, AS3, ebMS) B2B document support (EDI, XML based, Binary file transfer) B2B Transaction Viewer with replay capabilities

Figure 4:- IBM WebSphere DataPower SOA appliances

As already stated, IBM Datapower appliances are all purpose-built hardware/firmware stacks. The XG45 provides a security gateway for SOA services, including some lightweight ESB functions such as XPath routing and XSLT transformation. For broader integration needs, the XI52 expands the service gateway capabilities with full integration functionality, and is also available in blade formats for the IBM BladeCenter or the IBM zBX. For B2B usage, the XB62 adds trading-partner specific features to the integration appliance such as partner profile support and support for EDI message formats.

For specific customer scenarios such as provisioning development/test needs, IBM also provides a virtualized image of both the XG45 Service Gateway and the XI52 Integration Appliance. It is important to note, however, that this virtualization includes the whole stack of specialized DataPower operating system and appliance functionality. The idea is to make the virtualized image match the hardware appliance as closely as possible, making it easy to migrate to the hardware appliance when practical.

Basic SOA appliance functionality

The XG45 offers robust, secure XML and web services gateway functionality, and this functionality is also included in the XI52/XI50B/XI50z and XB62 appliances. The device acts as an SOA firewall, detecting XML-borne threats and attacks such as denial of service, and identifying and protecting from incoming viruses. It provides this functionality within a purpose-built appliance form factor, with hardware redundancy, clustering support and optional mirrored disk drives for high availability. The XG45 offers web and SOA service management facilities, and a comprehensive range of security features that are tightly integrated with related standards. Identity management can be done through integration with IBM Tivoli Federated Identity Manager (TFIM) or similar third party identity managers, and federation of security tokens is also supported. This support is WS-Trust and WS Federation standards compliant. The XG45 also offers Public Key Infrastructure (PKI) and FIPS 140-2 Level 3 Hardware Security Module (HSM) support for secure key storage. XML/JSON/REST/SOA services security support includes XML validation, encryption and digital signature, with security at both field and message-level. The XG45 embraces WS-Security and WS SecureConnection, and can handle Kerberos, RADIUS, LDAP, Microsoft Active Directory, XACML, SAML, LTPA and OAuth. Specifically for web services, the XG45 implements standards-based security compliant with a wide range of WS-* industry standards.

The XG45 includes policy management and enforcement controlling access, security, quality of service and mediation of SOA service requests and data references. These customizable policies can be role-based, and the XG45 can also integrate with other policy managers and service registries that support WS-SecurityPolicy and WS-Policy.

In terms of simplification, one of the strengths of the DataPower range is its breadth, with appliances available for a number of different needs such as security gateway, SOA gateway, Integration gateway and B2B gateway. The different appliance deliverables allow for more focused out-of-the-box functionality related directly to the particular appliance positioning. So for example, the B2B gateway can ship with out-of-the-box support for implementing trading partner profiles and handling industry-specific message formats. Apart from this, the single point of management control provided through the web GUI offers a comprehensive set of administrative and monitoring capabilities, such as policy tracking, service level management, logging and alerting.

IBM DataPower SOA appliances all offer hardware acceleration. XML Parsing, XSLT, XPath and other XML operations are carried out at wire speed, and a range of optimized XML processing features are also supported including XML pipeline processing, compression and caching. But the DataPower range does not focus solely on XML processing acceleration; there is hardware acceleration for cryptographic operations such as encryption / decryption, digital signatures and SSL/TLS processing.

Price/performance is further improved through the support for different levels of quality of service, implemented through the policy-based system. In the area of traffic smoothing and throttling, IBM DataPower offers powerful performance optimization through its Application Optimization feature. This enables workloads to be intelligently balanced automatically across clusters. At the front end, traffic can be throttled to prevent the system becoming flooded, but also IBM DataPower Application Optimization offers dynamic and intelligent back-end load balancing and distribution. With its ‘application-aware’ approach, target systems are dynamically discovered and real-time performance feedback is used to weight distribution, although of course there is also a facility to force affinity to a particular back-end if required. Using this optimization feature, IBM DataPower appliances can smooth traffic flow throughout the entire SOA deployment. For companies looking for high availability, the optimization feature can also be used to provide failover across a cluster of DataPower appliances, ensuring a single system failure will have no impact on production operations.

The IBM WebSphere DataPower range is well integrated with other management and monitoring environments, both IBM’s own Tivoli enterprise management framework and leading third party offerings. In addition, IBM offers the WebSphere Appliance Management Center for managing firmware deployment and maintenance across installed DataPower appliances. Audit facilities are built in, but information can also be shared with third party tools to make administration and management easier. In the security areas, administration is simplified with support for facilities such as single sign-on.

Value Add functionality

The XI52 integration gateway appliance (and its other incarnations, XI50B and XI50z) offers considerable value-add for SOA deployments, extending the advantages of a hardware appliance throughout the SOA network. In its role as a secure integration gateway, the XI52 provides a range of security, optimization and integration capabilities, whether deployed as an external gateway or between internal departments, integrating seamlessly with a general-purpose ESB engine such as WebSphere Message Broker. One particularly attractive feature of the XI52 is that, unlike most other SOA appliances, it provides offload and optimization capabilities for non-XML workloads as well as XML ones; in addition to standard XSLT-based transformations, mapping is also supported between such formats as XML, SOAP, binary and COBOL. The XI52 also offers content and context-based routing and data enrichment facilities, as well as adapters to other connectivity options such as TIBCO EMS, IMS Connect, IBM WebSphere MQ/MQFTE, FTP, SFTP and WebSphere JMS / JMS over MQ.

For SOA deployments that include WebSphere Application Server or REST-based applications, IBM provides a caching appliance, the IBM DataPower XC10. While not specifically an SOA appliance, the XC10 extends the value of the DataPower SOA appliance family by providing flexible, reliable and cost-effective elastic caching services to satisfy a range of SOA needs such as ESB-related caching or handling HTTP session management caching needs. The XC10 offers 240GB of cached storage.

The B2B use-case is supported by the DataPower XB62 appliance. This has a comprehensive range of functions for B2B needs. B2B Messaging protocols are supported such as AS1, AS2, AS3 and ebMS. Large payloads are accepted, and there is also specific integration for IBM's WebSphere MQ's managed file transfer facility. ebXML usage is also supported, where trading partner business processes are integrated through a combination of CPPA (Collaboration Partner Protocol and Agreement) and ebXML services together with IBM Process Manager. The XB62 provides support for trading partner profiles, covering variables like multiple business locations, business identifications and partner-specific certification and policy handling information. There is a B2B Viewer tool for monitoring and managing B2B communications and transfers, and if a partner has lost a particular transaction there is a resend facility so it can be repeated. Support for B2B documents formats include EDI-X12, EDIFACT, XML and Binary documents which can be transformed on the appliance to whatever format is required.

IBM DataPower appliances support multiple formats and styles, such as REST and JSON as well as SOAP and XML, and will map between them. This is important when using IBM DataPower appliances in a Mobile or Cloud integration use-case scenario. For Cloud usage, the Application Optimization feature includes a Secure Cloud Connector that provides a secure tunnel for Cloud applications that do not already support HTTPS communications. DataPower appliances also support the OAuth standard which is commonly used in the mobile environment. For the API Management use-case, IBM combines DataPower with a cloud-based service, IBM WebSphere Cast Iron Live Web API Services. The Cast Iron Live Web API Services offering satisfies the needs of three distinct roles in the world of API Management; the Application Developer Portal provides developer on-boarding and integration with social networking, the DevOps Dashboard allows the company exposing the APIs to assemble, secure and manage them, and the Business Ops Dashboard is used to publish, measure and report on the API usage, and to manage quotas. During execution of the APIs, the DataPower appliance now takes up the messages and handles the gateway security functions as the application flow passes through into on-premise systems.

While the design point of the IBM DataPower range is definitely to supply purpose-built hardware appliances, IBM has introduced Virtual Editions for its XG45 and XI52 versions that provide a virtualized option for deployment. The virtualized image includes the specialized DataPower operating system as well as all the functionality offered by the hardware appliance other than specific hardware-based features like the cryptographic optimization functionality. The aim is to ensure that development and testing with the virtualized image will deliver projects that can then be seamlessly migrated to the hardware appliance. In circumstances where a hardware appliance is not a practical option, the Virtual Editions also offer an alternative production deployment option.

Skills availability and knowledge transfer is a strong point for IBM. It has extensive experience from its long-standing involvement with SOA and appliances, which can be a great help when advising users on how to get the most out of SOA appliances, and there is a broad ecosystem of DataPower business partners worldwide. On the appliances side, through its DataPower acquisition and subsequent market success, IBM has developed a solid business approach to the appliance marketplace coupled with a good understanding of how to get the most out of appliances. All of this helps to improve time to value, but IBM has also built a number of industry packs that can help further by supplying some prebuilt configuration and integration components. Supported industry packs cover industries like Retail, Healthcare and Supply Chain.

Layer 7 SecureSpan SOA Appliances

Background

Layer 7 Technologies was founded in 2003 to deliver a range of XML security gateways. The first delivery was an XML firewall, followed by a whole range of security and governance related gateways. Right from the start, the Layer 7 strategy has been to build appliances by developing on general purpose platforms and then producing a hardened version of the stack. This approach has enabled Layer 7 to deliver its offerings in appliance, virtual and software form factors depending on user needs. It has evolved its original focus on XML security to cover SOA, mobile and cloud computing needs, and is now placing its major focus around API Management.

What is in the Layer 7 appliance portfolio?

The main Layer 7 range is its SecureSpan gateways, although for branding purposes it offers its Cloud Gateway under the CloudSpan brand. Initially, although Layer 7 started using SOA in its product branding, its products were fundamentally all about XML security. However, it has recently upgraded its SOA Gateway functionality and now offers a more convincing range of SOA appliance features such as limited ESB capabilities and web services management. The Layer 7 hardened appliances make some efforts to leverage the hardware platform with some specialized XML-handling chipsets and cryptographic support, but the design point is still based around general purpose UNIX platforms. The portfolio of offerings is depicted in the table below.

Layer 7 Appliances	Description
SecureSpan XML Firewall	Security, identity management and threat protection for XML messages Content-based routing Front-end traffic throttling Includes API Proxy
SecureSpan API Proxy	Virtual or Cloud-hosted appliance offering API security and metering Includes support for REST, JSON and OAuth
SecureSpan SOA Gateway	XML Firewall + Policy management and enforcement Services security and management Lightweight ESB capabilities
CloudSpan CloudConnect Gateway	SOA Gateway + Single sign-on and identity management SaaS usage measurement and reporting
SecureSpan Mobile Access Gateway	JSON/REST/XML/SOAP protocol and format bridging Single sign-on integrated with OAuth and other mobile schemes Device, user and application-based access
API Portal	Tool for developer on-boarding API key assignment API discovery and documentation

Figure 5: The Layer 7 SOA appliances portfolio

Most of the SecureSpan gateway offerings are the same appliance package, with functionality controlled by the acquisition of different levels of software keys. So for example, if a customer wants to move to an SOA Gateway from an XML Firewall, purchasing the new key enables this move to be achieved without any further changes. Also it is worth noting that the API Proxy is only available standalone in software or virtualized forms – if an appliance is required then both XML Firewall and SOA Gateway include the API Proxy capabilities.

Basic SOA appliance functionality

Looking at the security side first, the XML Firewall is specifically designed to provide security, identity management and threat protection for XML traffic, and this functionality is extended with the SOA Gateway to cover policy management and enforcement. Most common message formats and protocols are covered, including XML, SOAP, REST and JSON. Policies can be set up to remove, block or transform inappropriate or illegal content and to handle data validation and privacy. In addition, threat protection includes in-line anti-virus screening of payloads, using third-party AV products, and protection from attacks such as SQL and command injection, Denial of Service and malware.

SecureSpan appliances offer the expected range of identity management, authentication, authorization, privacy and integrity services. Identity management is designed to operate in a federated environment and to integrate with third party identity management products from companies like CA, Microsoft, IBM, Oracle and Novell. Credential sharing provides federated identity capabilities, while there is support for SAML, OAuth, keys and certificates. Key storage, encryption and signing operations can be handled through Federal Information Processing Standards (FIPS) 140-2 certified hardware in the appliance, or through an external module. A wide range of WS and WS-I security standards is also supported. Layer 7's highest levels of security and robustness are delivered in its hardened appliance form factor, which provides a more tamper-proof environment than delivered in the software or virtualized form factors. The hardened SecureSpan appliances include mirrored disks and redundant hardware features such as power supplies, and there is also some limited disaster recovery assistance with the ability to store individual appliance configuration details centrally so they can be rapidly accessed and re-used if required.

Policy-based control based around security, compliance, SLAs and quality of service is provided by the SecureSpan SOA Gateway. Policies are created with SecureSpan Manager, a graphical policy editor based on the WS-Policy standard, and can be updated live across single appliances or clusters. These policies can include a level of orchestration, for example enforcing different policies based on message content. Layer 7 SecureSpan appliances can be federated and then administered from a single point of control. The key tool is the Enterprise Service Manager which provides administration of the entire Layer 7 installation, providing consolidated monitoring and reporting.

Layer 7 offers a number of price/performance measures across its range of appliances. In terms of XML processing, the hardware form factor has a number of ASIC-based hardware accelerators for complex XML operations as well as an optimized XML parser design to make general XML processing more efficient. Qualities of service are controlled through the policy specifications, with traffic being blocked or throttled at the front end. In addition, processor offload scenarios are enabled through support for a number of third party ESBs such as IBM WebSphereMQ, TIBCO EMS, Oracle Service Bus and other JMS-compliant offerings.

The Layer 7 Enterprise Service Manager (ESM) is a centralized tool that manages all Layer 7 appliances and clusters, and provides a range of reports and dashboards reflecting both current operations and historical performance data. It can monitor entire installations or individual services, reporting on such elements as service performance, policy violations and SLA conformance. It is also the central point for policy management, providing policy organization and views together with the ability to roll out policies across any or all appliances. In terms of standards, Layer 7 pays considerable attention to the major standards around security and identity management, offering FIPS 140-2 compliance and support for related WS-* standards such as WS-Security and WS-Trust.

Value-add areas

In order to respond to SOA needs, Layer 7 has added some integration and mediation capabilities to its SOA Gateway. XSLT transformation is offered to meet the needs of switching between different formats, and content-based routing is supported. Transport and protocol mediation is also offered to switch between different environments. However, apart from a fairly basic range of adapters for third party messaging products, there are no additional adapters. For B2B needs, Layer 7 provides an XML VPN Client for use with XML Firewall, which applies security policies at the client side.

The mobile and cloud use cases have driven some specific responses from Layer 7. The main contribution of the CloudSpan CloudConnect Gateway is to offer single sign-on support combined with token mapping to bridge between different identity tokens from different environments. Apart from that, although there is some specific measurement and monitoring technology for tracking activity with different Software-as-a-Service (SaaS) suppliers, the CloudConnect gateway really just offers the same sort of security and connectivity capabilities as the XML Firewall, for example supporting REST applications.

The Mobile Access Gateway offers a number of areas of support for the mobile-based application environment, and relates closely to Layer 7's API Management facilities. In identity terms, the Mobile Access Gateway provides mappings between single sign-on and SAML tokens and mobile environments like OAuth, OpenIDConnect and JSON Web tokens. Access control is provided at the user, application and device levels, and can also be governed by geolocation and message content. Threat protection is extended to the mobile protocols and formats, and there are additional caching features for frequently called back-end data to assist performance. Protocol and format bridging is carried out between XML, REST, JSON and SOAP models, and traffic compression is available to optimize bandwidth usage.

Closely related to the Mobile Access Gateway is Layer 7's API Management portfolio. This consists of API Proxy, available either as a software / virtualized stack or as part of a SecureSpan Gateway, API Portal and an OAuth toolkit. API Portal is a tool designed to address the needs of on-boarding new developers, assigning API keys and providing API discovery, documentation and publishing services for developers. The API Proxy performs the run-time functionality required for API Management support, handling security and metering needs at the API level. The OAuth toolkit simplifies the task of implementing the OAuth standard.

Layer 7 has a close partnership with Oracle, and as a result has a number of examples of Oracle-specific support. It includes adapters for Oracle Internet Director and Oracle Access Manager for authentication in an Oracle environment, and can integrate with Oracle Service Bus, the Oracle ESB. It can also interoperate with Oracle Web Services Manager and pick up service interface definitions from the Oracle Registry.

Throughout its range of appliance offerings, Layer 7 supports a range of deployment options; a hardened appliance, a software stack for use with Linux or Solaris and virtualized images for use with VMWare or in the Amazon EC2 Cloud. These can provide a cost-effective approach to testing, but come with the drawbacks of a software stack versus a hardware appliance as discussed earlier in this paper. On the skills and support front, Layer 7 has a lot of experience in the areas of XML and security but much less in the SOA arena. However, it is starting to build up a reasonable level of experience in the area of API Management, and has already achieved some successful deployments.

Vordel API Server

Background

Vordel started business in Ireland in the early 2000s as a provider of XML security technology. It originally offered an XML Firewall providing threat protection and identity management. This evolved into an SOA Gateway, an Application gateway (with the addition of cloud service broker functionality) and most recently its API Server. Today, Vordel is headquartered in the US but still has much of its organization in Ireland.

What is Vordel API Server?

The Vordel API Server is a combination of Vordel's previous XML Firewall and SOA Gateway technologies together with specific functionality to support API management. The API Server product is available as a software stack, in virtualized form or as a hardware appliance.

Vordel SOA appliances	Description
Vordel API Server	Connectivity and access control Threat protection Identity management Authorization, authentication and privacy management Policy-based security management and traffic control API management and lifecycle support
Vordel VS4000 Appliance	Hardware appliance version of the Vordel API Server Includes hardware-assisted cryptography technology Supports a secure key storage component

Figure 6: The Vordel SOA appliances portfolio

Basic SOA Appliance functionality

As might be expected from a company that started out providing XML security, the security features of the Vordel API Server are reasonably comprehensive. API Server scans all messages, headers and attachments to protect from traffic-borne viruses and threats such as denial of service attacks, malware and command injection. Vordel uses an in-line virus protection facility, but also supports calls out to third party virus-checkers such as McAfee, Sophos and CLAM AV. API Server also protects from 'user error' threats; for example, clients that are continually sending messages that are rejected can be either blocked or throttled, and schema validation can protect from programming errors. Beyond threat protection, the Vordel API Server offers the full range of security and identity management facilities including authentication, authorization, audit, trust relationship management, identity federation, encryption and digital signature support. For companies wanting to use a corporate identity management solution, API Server also comes with pre-built integrations to most of the leading identity and access management solutions in the industry from companies like IBM, Oracle and CA.

While Vordel API Server is designed to run on general operating systems such as Linux, the VS4000 hardware appliance 'hardens' the operating system by disabling unwanted options that are not required in a dedicated security gateway. It also offers high availability features such as dual power supplies and RAID disk access.

Vordel's Policy Studio provides an Eclipse-based drag-and-drop tool to develop and control policies. These policies cover areas like security rules, compliance rules, data privacy and SLA management. Policies can dictate different qualities of service for different consumers, and can all be managed from a single point of control. Vordel API Server provides policy lifecycle management, from creation to deployment and production usage. In addition, the product ships with a set of out-of-the-box policies for some common usage scenarios.

While the hardware variant of the API Server, the VS4000 appliance, includes specific hardware-assisted performance acceleration for cryptographic needs, other XML/SOA performance measures are available in all form factors. The cornerstone of the XML optimization offered by Vordel is its patented VXA (Vordel XML

Accelerator) technology. The key to VXA's automation is the way it splits trust issues apart from any other XML tasks such as XML validation and message/payload examination. VXA processes each of these aspects of the XML message in parallel threads, and as soon as one thread makes a decision to reject the message then processing is immediately terminated in all the other threads. This parallelization and critical path processing, on top of more traditional XML parsing optimization measures, speeds XML traffic handling and throughput.

API Server also provides a number of traffic throttling mechanisms to try to smooth traffic flows and protect from over-usage or flooding scenarios. The administration tool enables all sorts of limits to be set, but all the throttling is front-end; that is, the mechanism is that if the limits are exceeded the client request is blocked. In terms of standards, Vordel API Server offers support for a range of connectivity and security standards covering styles and formats like JSON, REST, SOAP and XML and including many WS-* web services standards.

The administration tool, Vordel Manager, offers a range of real-time monitoring and analysis functions, while Vordel Analytics offers offline analytics and reporting services. Monitoring and management can be done from a single point of control for all federated instances of the API Server, with usage being tracked at user, data and transaction levels. In addition, integrations are provided for a wide range of third parties so that alerts can be shared with management tools such as HP OpenView, Oracle Enterprise Manager and CA Unicenter.

Value-add areas

While Vordel API Server is not an ESB in the fullest sense, it does offer some integration and mediation functions for the SOA environment. For example, there are a number of routing options supported, either based on policies or XPath-based content routing. XSLT transformations are supported and data can be enriched in transit, with SQL calls for instance. It does offer a number of linkages and adapters for other environments however, in particular to a range of ESBs from suppliers like IBM, TIBCO, Oracle, Progress Software and Fiorano. For B2B usage, Vordel provides support for a range of industry message formats and protocols including HL7, ebXML, ACORS, FIXML and AS2/3/4.

As part of its journey from an XML Firewall to the current API Server offering, Vordel has added support for the mobile and cloud usage patterns. REST and JSON are fully supported, with protocol bridging and format mapping available between them and the SOA SOAP / XML world. Because mobiles operate with lightweight operating systems and will almost certainly be communicating through untrusted domains, additional security measures have been added to Vordel API Manager such as device authentication, contextual authorization and remote wiping, together with support for the OAuth standard. Cloud support measures include single sign-on and centralized storage of API keys.

Unsurprisingly, API Management is a major focus for Vordel API Server. Vordel has implemented the full range of API lifecycle management facilities spanning API development through to secure provision and usage, activity measurement and policy enforcement. APIs are created using the Policy Studio tool, and are then managed by Vordel Manager. The drag and drop interface allows APIs to be mashed up to generate APIs that themselves drive a number of different lower level APIs from different suppliers. API Server also offers a single repository for all the API information. Where APIs are being supplied by third parties, API Server offers API brokering functionality, performing mediation tasks to bridge between the different API formats and characteristics. For example, if different third parties have used different identity and authentication schemes, API Server will map between them, and if APIs need to be mapped it supports Javascript, Groovy, Jython and Ant. All API usage is measured and reported, and service levels can be varied based on traffic volumes and the particular consumers or users.

Vordel offers specialized support for SharePoint environments and also some help for Siebel users. On the SharePoint side, Vordel integrates with the rather arcane Microsoft security and authentication systems, interoperating with Windows Desktop Signon and supporting standards required by Microsoft such as Kerberos. It also supports use of SharePoint from mobile applications and provides a caching facility to speed up SharePoint interactions. The Siebel support is basically auditing support that understands the various Siebel session aspects such as client, user, transaction, data and view.

SOA appliances – Competitive assessment

Having summarized the offerings from the four vendors under consideration, it is now possible to assess them against each other, in competitive terms. In order to make this assessment as relevant as possible, the basis will be the most common user-based drivers for adopting SOA appliances, namely:-

- Enhance SOA security and governance
- Reduce SOA complexity / total cost of ownership (TCO)
- Factors that increase the Value Potential of the SOA appliance (eg additional use-cases, other relevant factors)

Of course, prospective buyers of SOA appliances are often looking to enjoy a combination of these three benefits, and may have other aims too, but these are the most common. On this basis, the competitive assessment is grounded around these three areas.

Enhance SOA security and governance

Setting the scene

Most SOA infrastructures have reasonably strong support for security, and many also offer governance options for controlling the creation, deployment and operations of SOA services. However, the perceived exposure is not so much the internal SOA network but rather the touch points between the network and other domains, such as other departments, partners or the internet. As SOA becomes more and more important, and connectivity becomes increasingly ubiquitous, organizations start to worry a lot more about exposure to hackers or other external sources of threats, and whether everyone is following the agreed corporate policies as traffic flies around the SOA network. In particular, organizations often worry about putting software out in the DMZ – the view is that if you have to put a security gateway out there, it should be tamper-proof. Problems can arise from non-malicious SOA services too. Popular services that are accessed by many systems may negatively impact end-to-end SOA performance. A means to detect excessive usage and to then govern access to such services is needed to ensure performance is maintained and SLAs are met. Some of the more recent SOA use-cases to have emerged increase the security and governance challenges by an order of magnitude; Cloud access introduces issues over data security and federated identity management, and providing mobile application access dramatically increases the potential touch-points with devices that may be only lightly protected themselves.

Competitive assessment

XML Gateways have been around for more than ten years, and SOA gateways for only a few years less, so it is not surprising that vendor maturity has grown over that time to a point where most vendors provide reasonably closely matched functionality at the basic level of SOA security and governance, at least in the traditional corporate SOA use-case. The addition of new considerations like bringing in traffic from cloud-based and mobile applications or through exposure of corporate APIs has placed new requirements on security and governance, of course, but even here there are limited areas of differentiation between vendors. So for example, all the vendors considered in this assessment provide FIPS-140 compliance. They all provide threat protection, federated identity management, token bridging, encryption, digital signatures and key management, and support for third party identity management systems. They all also offer policy management and traffic control, enabling policies to be set up to govern different security requirements for different services and applications. However, at the lower level there are still some differences.

While all the appliances support antivirus checking of traffic, some prefer to use third-party AV services while others provide their own AV functionality. Vordel provides its own technology, while Forum embeds SourceFire's ClamAV checker, but all vendors also provide ICAP protocol access to compliant third party antivirus checking services. On the standards front in general, all vendors provide support for the WS-* web services standards.

Perhaps the major area of difference in terms of security and governance is that of the initial appliance design point. As discussed earlier, the vendor's design point will have implications on the final appliance functionality; a design point of using general purpose system software (operating system, database system, communications system) and hardening it will generate different operational characteristics from a design point of developing a purpose-built appliance of hardware and firmware for the specific task of SOA security and governance. Forum Sentry and IBM DataPower were developed as purpose-built appliances, while Vordel API Server and the Layer 7 SecureSpan range were built as hardened versions of general software stacks. While all four vendors have implemented various hardware assists for the hardware appliance form factor, the implication is that for the absolute highest levels of security and tamper-proof robustness the IBM and Forum appliances have the edge.

Moving to consider some of the security and governance issues presented by the most recent use-cases, once again all four vendors have adapted to provide protocol mapping support between the cloud/mobile world of REST/ JSON and the XML/SOAP environment, as well as supporting the OAuth open authentication protocol and handling identity token bridging. Single sign-on is also supported by each appliance.

B2B introduces its own security and governance issues, and here there are wider differences between the four vendors. Some of the challenges presented by B2B usage are the different standards-based formats used in EDI transactions and the governance of trading partner relationships where trading partners may span many different locations and users. Layer 7 and Forum Systems have only basic support for the B2B use-case; both support the FTP protocol and the transfer of large payloads, but beyond that they offer little. Vordel provides stronger support, with support for a number of B2B standards and message formats including HL7, ebXML, AS2/3/4, ACORD and FIXML. However the strongest B2B support is found in the IBM B2B Gateway appliance, with its comprehensive support for B2B trading partner profiles, formats and protocols and the B2B-specific management and governance tools.

API Management provides a very specific governance headache. APIs that are being exposed externally need to be carefully controlled to avoid unregulated chaos. Forum Sentry does not really play in this use-case at all, but the other three vendor offerings do. In this use case, the IBM DataPower appliance works in conjunction with the Cast Iron Live Web API Services offering; for Layer 7 the relevant offerings are the SecureSpan API Proxy and the SecureSpan SOA Gateway; for Vordel it is its API Server. Each of these solutions offers tools to govern allocation of API keys and metering of API usage from different users and applications, with the ability to block or throttle requests according to the specified policies.

XML handling also differs between vendors. Forum Sentry offers basic XML parsing optimization but not much more. Vordel splits XML trust actions from other XML activities so that it can stop processing immediately if one of the trust tests fails, and also provides some hardware assistance in its appliance form. Layer 7 offers a combination of hardware ASICs and optimized parsing, while IBM delivers hardware acceleration as well as parsing, processing and compression optimizations.

Reduce SOA complexity / total cost of ownership (TCO)

Setting the scene

A major issue for many organizations is that as SOA becomes more heavily embedded in their operations, the SOA network and supporting infrastructure can expand rapidly, across many different domains and nodes. In simple terms, the SOA infrastructure becomes a collection of many moving parts – ESB nodes, XML servers, security components in servers in every domain, and so on. The SOA appliance idea produces a way of reducing the number of moving parts, enabling sets of them to be consolidated into single appliances. These appliances all look the same, have the same interfaces, and implement the same standards, and as such they make the infrastructure more uniform. The result is that as the number of entities and the extent of variations to be supported decreases, the people costs to support them falls. Putting a new appliance in place becomes a repeatable process, particularly since appliances tend to come more or less preloaded with only minor configuration required. Supporting functionality in one place makes maintenance cheaper and more reliable, and being able to look in one place to get a picture of system activity and performance also reduces time and effort. Another side effect of appliance adoption is that the greater efficiency reduces the number of servers that require cooling, space and power.

A critical factor in this reduction of TCO, though, is the form factor and design point of the appliance. One of the reasons that appliances can often be between five and ten times cheaper to support than server stacks is that, as mentioned above, they reduce the number of moving parts. This means fewer places where maintenance may need to be applied / tracked / managed. Some SOA appliances support software or virtualized form factors where they are deployed as a software stack. Immediately this is done, the TCO savings are heavily impacted, because now each of these software stacks requires maintaining. Even with appliances based on a hardened form factor of general purpose software, the TCO savings will be reduced because important updates to the general purpose system software layer will either have to be applied to the appliances too or will introduce the risk of the hardened software level on the appliance getting of step with current levels of systems software maintenance. It is only in the purpose-built SOA appliances that the TCO savings will be maximized.

This whole area of simplification with the corresponding reduction in TCO is perhaps the most powerful of all the factors driving SOA appliance purchases. But another area that is an important contributor is that of price/performance. The extent to which an appliance can offload processing from critical, general purpose business systems improves TCO, and the efficiency with which it can execute the processing will also enable increased simplicity through server node concentration.

Competitive assessment

The first observation to be made is that, as in the case of SOA Security and Governance, growing vendor maturity in the SOA appliances space has resulted in a greater degree of commonality in functionality to reduce complexity and TCO. One obvious example is managing federated deployments of appliances; all four vendors offer monitoring and management tools that enable single point of control and management of multiple appliances, all working from a single, central repository of definitions. All four vendors also offer XML and SOA policy management to control security and governance measures for specific users / applications / systems, and provide support for interoperating with third party management frameworks.

However, digging deeper does show up some differences. For instance, IBM offers the WebSphere Appliance Management Center to reduce the time and effort required to manage firmware deployment across the DataPower appliances. This provides a significant benefit because this is the type of maintenance challenge that can consume a lot of time and energy if it has to be done manually. Vordel and Layer 7 both offer a selection of out-of-the-box policies for common scenarios, and Layer 7 provides the ability to back up the configuration information and policies so they can be restored remotely in a disaster recovery scenario.

In the area of reducing TCO through improved price/performance, there are much wider differences between the four vendors. Each vendor claims to provide optimized XML handling and hardware assisted cryptographic functionality, but when looking more broadly at offloading processing onto the appliances it is a different story. As well as optimizing XML parsing/processing and cryptography, SOA appliances need to look to provide connectivity to as many application types as possible and to support more mediation / brokering / integration activities. This increases both the number of applications that can offload activities and the number of activities that can be offloaded, increasing price/performance efficiency and thereby reducing TCO.

As a result, all vendors have now delivered lightweight ESB-type functionality; basic XSLT data transformation, XPath routing, some data enrichment capabilities and adapters to common ESBs such as IBM WebSphere MQ, TIBCO EMS and Oracle Service Bus. But IBM is the only vendor to extend this to full integration support with its DataPower XI52 Integration Appliance, including a comprehensive array of adapters to many different environments. In particular, for SOAs that include IBM mainframe systems the XI52 offers major differentiation for offloading processing from the mainframe. The critical component is optimized transformation support for non-XML data formats; the other appliance vendors are all locked into an XML view of the world, but much of the data on mainframes is not in an XML format. This allows the IBM appliance to offload a lot more SOA integration work from the mainframe. The IBM appliance also has connectivity to the main IBM legacy systems such as CICS, IMS and DB2, and it has two alternative form factors that can be used; as a component of the IBM mainframe zBX rack for added integration, or as a blade in an IBM Bladecenter.

Looking more widely to some of the other SOA appliance use-cases, more differences between the suppliers are evident. Both B2B and API Management are appliance use-cases that can benefit significantly in terms of simplification and TCO reduction. In the case of business-to-business scenarios, it is important to be able to manage the range of trading partners effectively in order to maintain service quality and increase trading partner satisfaction. This can be quite a time-consuming task, with partners that may span different locations, different subsidiaries and different application needs. While Vordel and Forum Systems do not do much to help, Layer 7 offers its VPN Client which can make it easier for companies to control the security expectations of different trading partners. However it is IBM that does the most for B2B; it provides trading partner profile support and specific tools to monitor trading partner activities in a consolidated fashion, reducing a lot of the manual workload required to support these valuable channels.

API Management also introduces TCO and support issues because there may be many different external development organizations or individual developers who want to have access to the corporate APIs, and these all have to be authorized, tracked, managed and monitored. Once again, Forum Systems does not provide much support in this area, but the other three vendors all offer tools to make administering, managing and supporting API exposure easier and less labour-intensive.

As mentioned earlier, form factor flexibility can be a two-edged sword in terms of simplicity and TCO, but can be particularly interesting for development/test environments that may be remote from the eventual deployment locations. Layer 7, Vordel and Forum Systems all offer software stacks and virtualized images of the appliance functionality. The IBM DataPower range of hardware appliances also offers virtualized images; these images include the specialized DataPower operating system to ensure they maintain the closest possible compatibility with the hardware appliance range. One other TCO reduction measure that deserves mention here is the Layer 7 software key approach to appliance functionality. When customers purchase a Layer 7 appliance, the functionality it delivers is governed by use of a software key. The actual hardware is common across most of its SecureSpan appliance range, but functionality is controlled by the key. This means that if a customer wants to upgrade to a higher level of functionality, for example from an XML Firewall to an SOA Gateway, the only change required is to purchase a new key – the appliance does not have to be replaced.

The other component of reducing support costs and increasing processor offload effectiveness is ensuring that traffic and workloads flow optimally through the entire infrastructure. Traffic flow problems will impact performance for everyone and will therefore reduce the usage and effectiveness of the appliance as an offload device, while increasing the load on helpdesks and support organizations. While all four vendors offer traffic management functionality, most of this support is front-end based enforcement of traffic policies. In other words, excessive requests or requests that exceed the specified limits will be blocked. Layer 7 SecureSpan appliances also provide a primitive load-balancing algorithm for routing work to available back-ends. But the stand-out in terms of traffic and workload management is IBM DataPower, with its Application Optimization feature providing intelligent load-balancing across both front and back ends. Not only can front end traffic be throttled to avoid the system becoming flooded, but also the feature includes the ability to dynamically discover target systems, monitor real-time performance feedback and balance work to back-end systems accordingly. This ensures the greatest degree of processing efficiency in heavily loaded environments, increasing offload potential and reducing support calls due to poor response.

Value Potential

Setting the scene

There are basically two areas of factors that increase the value potential of different SOA appliances; broadening the possible use-cases where the appliance could be deployed, and building out the product into a more complete solution. The first has already been discussed earlier, but to recap, beyond the 'standard' usage of an SOA appliance as a security gateway / processor offload / integration engine option within a corporate SOA, there are a number of additional use-cases that have become popular:

- B2B Gateway – linking trading partners
- Mobile/Cloud Gateway – providing the access point for mobile/cloud applications
- API Management server – providing gateway and management facilities for exposing corporate APIs

The second value-add area covers the 'whole product' view of the SOA appliance combined with any ancillary offerings such as professional services, skills, industry-specific specialization and partner availability and support.

Competitive assessment

As technology has continued to move on, SOAs are proving fertile ground for delivering corporate application functionality to wider audiences in an increasing number of ways. Companies are not only using SOA services internally, but want to expose them to trading and development partners as well as in different operational modes such as mobile and cloud computing environments. It is therefore no surprise that most SOA appliance vendors have moved to embrace some, if not all, of these new use-cases. However, a closer inspection shows some marked differences in support across the four vendors considered in this assessment.

Forum Sentry is the least advanced of the SOA appliances under consideration in supporting these newer use-cases. It does support FTP protocols and can tolerate large payloads, making file transfer a practical option in B2B scenarios, and it has also added support for common mobile needs like JSON, REST and OAuth, with mediation functionality to map these formats to the XML/SOAP world and back, but beyond this Forum Sentry has yet to show much additional support.

Vordel API Server has put considerable effort into broadening its base of supported use-cases. It has included support for a number of the most common B2B protocols and formats such as HL7, ebXML, ACORD and FIXML to satisfy some of the requirements of B2B usage, but its major focus has been to encompass the Mobile/API Management worlds. Here, it has included support for JSON, REST and OAuth, offering specific mobile-oriented features such as device authentication, contextual authentication and remote wiping. On the API Management front, it offers full API lifecycle management including centralized storage and management of API keys used to authorize API usage by particular developers. API mashups can be created by dragging and dropping APIs to orchestrate them together, with mediation provided to map between APIs from different suppliers if required. For API mapping, Vordel support such mechanisms as Javascript, Groovy, Jython and Ant. In summary, Vordel API Server offers basic support for B2B and Cloud scenarios, with stronger support for mobiles and API Management.

Layer 7 provides a number of different appliances for use in different use-case scenarios. The CloudSpan CloudConnect appliance is really just the SOA Gateway appliance with the inclusion of support for single sign-on, with token bridging to accommodate different security domain requirements, and also some specific technology to monitor usage of different SaaS applications and services. The SecureSpan Mobile Access Gateway offers the same single sign-on and OAuth support but with some specific mobile features such as device-level and geolocation-based access control and some additional caching to optimize data requests from smaller mobile devices. The SecureSpan API Proxy appliance together with the API Portal tool provides Layer 7's response to API Management needs. The API Proxy is the run-time component responsible for securing, metering and governing the use of the exposed APIs, while the API Portal provides administrative functionality, such as on-boarding developers or development organizations and allocating API keys, as well as API discovery, documentation and publishing services. In addition, Layer 7 offers an OAuth toolkit; OAuth is notoriously tricky, and so Layer 7 has produced a toolkit to make the task of providing OAuth definitions and specifications with the Layer 7 appliances as easy as possible. The Layer 7 API Management support is comprehensive, but it does little for the B2B use-case and support for mobile and cloud scenarios is limited.

IBM provides different appliances for different scenarios as does Layer 7, and also leverages the IBM Cast Iron Live offering for API Management needs. As already discussed, IBM's B2B support is strong, with support for a range of standards and EDI formats coupled with a set of tools to make B2B management as smooth and simple as possible. Beyond support for single sign-on, REST and JSON formats and the OAuth protocol, IBM does not include anything specifically for Cloud or mobile needs, other than its Secure Cloud Connector facility for providing a secure tunnel to Cloud applications. However its API Management solution including the Cast Iron Live Web API Services cloud-based service covers all the bases. The three distinct views offered by the Cast Iron Live service provide role-based access for developers, where they can self-register and hook into the social networking world, together with the devOps and Business Operations roles to deal with API assembly/ administration and API relationships / management respectively. Execution of the API calls is through the DataPower gateway appliance as in other use-cases. This leaves IBM with strong support for B2B and API Management together with more basic Mobile and Cloud support.

Beyond supporting different use-cases, this section also considers ancillary offerings, either explicit or implicit, from each vendor that increases the value of the SOA appliance solution. Forum Systems has a considerable amount of security knowledge and expertise that it can share with prospective clients, but not much more. Vordel has some specific added value offerings however, including in particular its SharePoint and Siebel gateways. The Siebel gateway essentially provides control of Siebel traffic flows together with auditing based on Siebel factors such as clients, users, transactions services and data. There is a specific Siebel adapter to make communications easier and more reliable. The Vordel support for SharePoint deployments is more extensive, including integration and support for Microsoft SharePoint environment specifics like Kerberos, Windows Desktop Signon and ADFS. Because of the complex nature of SharePoint interactions with the non-Microsoft world, Vordel also adds in mobile and remote access as well as providing cache services to enable SharePoint performance to be maintained in these scenarios.

Layer 7 has a strategic relationship with Oracle, and therefore provides specific Oracle support in some areas. At the authentication level its SecureSpan appliances can interoperate directly with Oracle Internet Directory and Oracle Access Manager, and it has an adapter for the Oracle ESB, Oracle Service Bus. It can also interoperate with Oracle Web Services Manager, and look up service information directly from the Oracle Registry.

IBM's main area of value-add lies in its in-depth understanding of the practical challenges of SOA in many different scenarios. IBM offers pre and post sales SOA skills and also provides an extensive range of professional services to help companies deploy and operate their SOAs effectively and successfully. IBM also offers some specific industry packs designed to help industry verticals in their SOA appliances deployments – at the present time, there are industry packs available for Retail, Healthcare and Supply Chain industries.

Competitive summary

The table below summarizes the four SOA appliance vendors against the three main assessment areas.

	Security and Governance	Reduction in Complexity / TCO	Value potential
Forum Systems	■■■■■■■■□□	■■■■■■■□□□	■■■■■□□□□□
IBM	■■■■■■■■■□	■■■■■■■■■□	■■■■■■■■□□
Layer 7	■■■■■■■■□□	■■■■■■■■□□	■■■■■■■■□□
Vordel	■■■■■■■■□□	■■■■■■■□□□	■■■■■■■■□□

Figure 7: SOA Appliances – Competitive Assessment Summary

Conclusion

Appliances have been serving business needs for many years, particularly as security gateways in the DMZ, and more recently in service oriented architecture (SOA) deployments. With SOA making heavy use of XML-based connectivity between different environments across the enterprise and beyond, appliances have quickly fitted in as gatekeepers to the SOA network, but have also emerged as a cost-effective and efficient means to perform the mechanical and repetitive calculations required to process XML traffic. In the former case, the hardened, tamper-proof nature of an appliance makes it an ideal security measure, while in the latter its ability to focus purely on SOA-related tasks, combined with specialized hardware acceleration, enables improved performance and throughput without consuming critical processing capacity elsewhere in the enterprise. But there is another important aspect of SOA appliance usage that is not so immediately obvious. By consolidating parts of SOA processing into pre-loaded, pre-configured, uniform devices, appliances can considerably simplify the SOA infrastructure. This simplification delivers on-going benefit, reducing the cost of owning, operating and supporting an SOA implementation.

As SOA appliance acceptance has grown, four vendors have emerged as key players in the market – Forum Systems, IBM, Layer 7 and Vordel. The purpose-built Forum Sentry appliance provides a powerful SOA Security Gateway, handling a wide range of security needs from key handling and digital signatures through encryption to federated identity management. Although it has expanded its SOA support to accommodate traffic coming from mobile and cloud environments, in essence it remains an XML/SOA security gateway. IBM, Layer 7 and Vordel have all expanded from their own comprehensive SOA security gateways to address broader SOA requirements, covering the needs of mobile, cloud and API-based access to SOA services and applications, but IBM retains its leadership position due to its comprehensive SOA coverage both as a gateway (XML and non-XML) and a key simplification / processor offload option within the SOA model, together with its level of practical SOA experience.

As SOA continues to tighten its grip on the corporate IT marketplace, new drivers such as API exposure and mobile computing needs will drive SOA access exponentially, with a corresponding increase in traffic passing between more and more locations and devices. SOA security and governance will become even more important, while the growing demands on the SOA infrastructure will place it under much strain, particularly in the areas of performance, management and governance. SOA appliances form a valuable addition to the IT armoury, providing a way to secure and simplify the corporate infrastructure while delivering wider access to corporate services with greater efficiency and performance. As a result, there can be little doubt that, although SOA appliances are relatively new, they are definitely here to stay.

About Lustratus Research

Lustratus Research Limited, founded in 2006, aims to deliver independent and unbiased analysis of global software technology trends for senior IT and business unit management, shedding light on the latest developments and best practices and interpreting them into business value and impact. Lustratus analysts include some of the top thought leaders worldwide in infrastructure software.

Lustratus offers a unique structure of materials, consisting of three categories—Insights, Reports and Research. The Insight offers concise analysis and opinion, while the Report offers more comprehensive breadth and depth. Research documents provide the results of practical investigations and experiences. Lustratus prides itself on bringing the technical and business aspects of technology and best practices together, in order to clearly address the business impacts. Each Lustratus document is graded based on its technical or business orientation, as a guide to readers.

Terms and Conditions

Customers who have purchased this report individually or as part of a general access agreement, can freely copy and print this document for their internal use. Customers can also excerpt material from this document provided that they label the document as Proprietary and Confidential and add the following notice in the document: “Copyright © Lustratus Research. Used with the permission of the copyright holder”. Additional reproduction of this publication in any form without prior written permission is forbidden. For information on reproduction rights and allowed usage, email info@lustratus.com.

While the information is based on best available resources, Lustratus Research Ltd disclaims all warranties as to the accuracy, completeness or adequacy of such information. Lustratus Research Ltd shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. Opinions reflect judgment at the time and are subject to change. All trademarks appearing in this report are trademarks of their respective owners.

Lustratus Research Limited
St. David's, 5 Elsfield Way, Oxford OX2 8EW, UK
Tel: +44 (0)1865 559040

www.lustratus.com

Ref STC/LR/19560406/V1.0