IBM WebSphere DataPower SOA Appliances
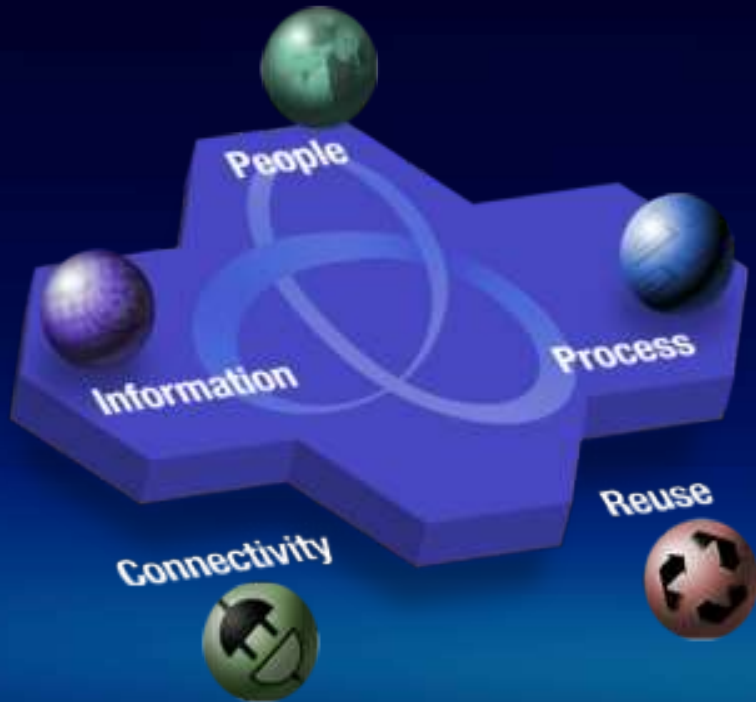*Simplify, Help Secure & Govern Your SOA*

Ad van den Boogaard
Technical Sales Specialist
advanden@au1.ibm.com

WebSphere DataPower SOA Appliances

An SOA Appliance…

Creating customer value through extreme SOA connectivity, performance and security

- **Simplifies** SOA and accelerates time to value
- **Helps secure** SOA XML implementations
- **Governs and enforces** SOA/Web services policies

WebSphere DataPower SOA Appliances redefine the boundaries of middleware extending the SOA Foundation with *specialized, consumable, dedicated SOA appliances* that combine *superior performance and hardened security* for SOA implementations.

WebSphere DataPower SOA Appliances

An SOA Appliance…

Creating customer value through extreme SOA connectivity, performance and security

- **Simplifies** SOA and accelerates time to value
- **Helps secure** SOA XML implementations
- **Governs and enforces** SOA/Web services policies

WebSphere DataPower SOA Appliances redefine the boundaries of middleware extending the SOA Foundation with *specialized, consumable, dedicated SOA appliances* that combine *superior performance and hardened security* for SOA implementations.

What are the Painpoints?

XML is the foundation of SOA, but brings new challenges:

Scalability: XML is bandwidth, CPU, and memory intensive

Performance: some XML apps literally grind to a halt

Security: connecting systems never before connected

Security: clear text over HTTP with no inherent security

Integration: connecting Web services to legacy applications

Standards: are still in flux

Governance: ability to manage your SOA

- Businesses want to deploy secure XML-based applications…but security adds further bulk to the application that slows it down.

- Businesses want to move to standards-based XML…but XML is bulky which can cause performance bottlenecks.

- Businesses want to integrate their new Web Services to each other and to existing legacy applications…but they don't want to do it point to point because that diminishes the flexibility that SOA is supposed to bring.

- Businesses want to manage and monitor their Web Services in the same way as server up/down but SOA management is more than just management from an IT perspective– achieving a level of control, policy, and governance.

DataPower SOA Appliances Are Not . . .

- Regular rack mount servers with some pre-loaded software
- Running a full standard operating system
- Traditional network packets (below layer 7)
- Java-based
- Application servers, which typically provide business logic for specific functions such as customer relationship management or sales force automation
  - XML processing is the common element found across these applications
  - DataPower appliances add headroom and scalability, allowing application servers to process business logic while leveraging a common platform for the heavy lifting that comes with XML processing and security
- Routers, load balancers or IP firewall replacements
  - DataPower augments existing network infrastructure by adding a layer of intelligent infrastructure to the enterprise network
  - Devices are IP-addressable and designed to be deployed alongside existing network infrastructure without requiring adjustments to network topology

Why an Appliance for SOA?

- **Hardened, specialized hardware for helping to integrate, secure & accelerate SOA**
- **Many functions integrated into a single device:**
  - *Impact: connectivity will require service level management, routing, policy, transformation*
- **Higher levels of security assurance certifications require hardware:**
  - *Example: government FIPS Level 3 HSM, Common Criteria*
- **Enables run-time SOA governance and policy enforcement**
  - *Impact: dynamically control service availability, security, performance, and endpoint selection*
- **Higher performance with hardware acceleration**:
  - *Impact: ability to perform more security checks without slow downs*
- **Addresses the divergent needs of different groups:**
  - *Example: enterprise architects, network operations, security operations, identity management, web services developers*
- **Simplified deployment and ongoing management:**
  - *Impact: reduces need for in-house SOA skills & accelerates time to SOA benefits*
- **Proven Green / IT Efficiency Value**
  - *Example: Appliance performs XML and Web services security processing as much as 72x faster than server-based systems*
  - *Impact: Same tasks accomplished with reduced system footprint and power consumption*

WebSphere DataPower SOA Appliances Address Critical Connectivity Issues
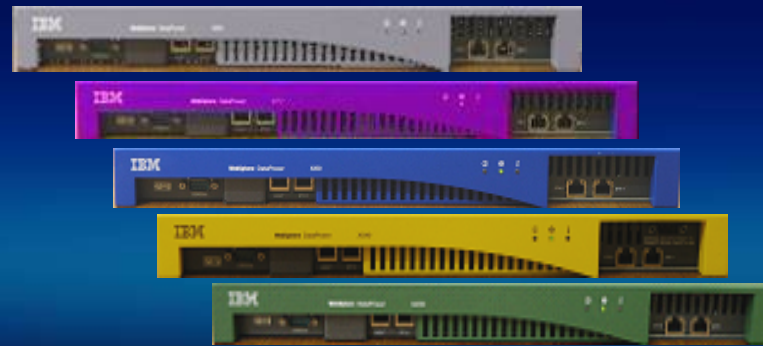
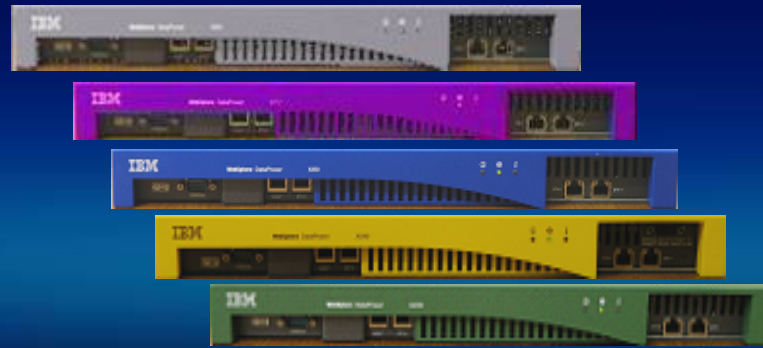## Simplicity

Robustness
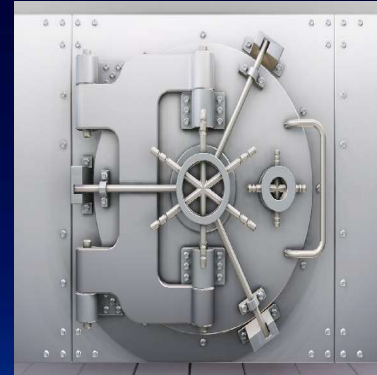
Governance

Speed

Meet the Family..

Meet the Family..

XA35

XML Accelerator XA35
Centralized XSLT Management, Offload XML Processing

- Wirespeed XML/XSLT/XPath Processing

- Schema validation, XML compression, XML caching

- SSL termination and acceleration

- Easy configuration and administration

Accelerates XML processing and SSL termination/acceleration, increasing throughput, decreasing latency, and reducing server workload.

Innovative XML pipeline processing and XML caching reduce impact of increased XML traffic, improving scalability of resource intensive applications.
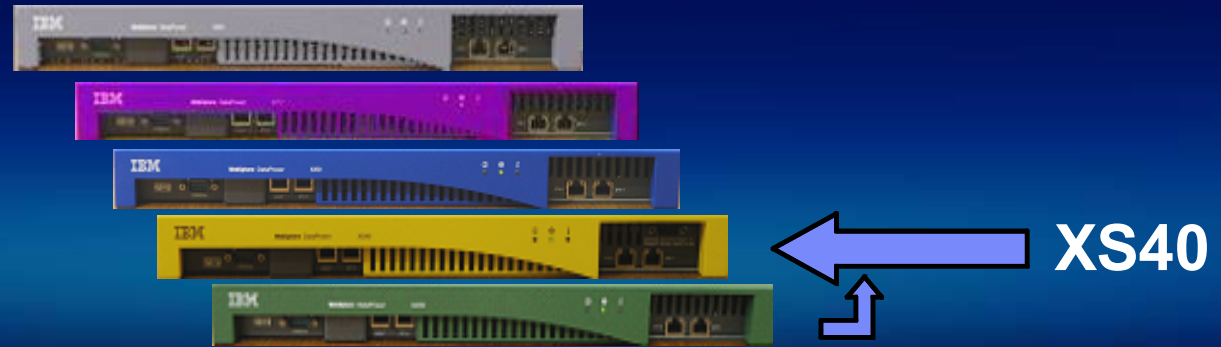
Performs XML schema validation to ensure incoming/outgoing XML documents are legitimate and properly structured.

Fully integrated with industry standard IDEs such as Altova XML Spy and Eclipse allows developers to design, debug and deploy against a single XML and XSLT processor, saving valuable cycles from pilot to production.

Meet the Family..

XS40

XML Security Gateway XS40
Web service threat protection and message security

- Centralizes XML security and policy enforcement

- Hardened security appliance for DMZ deployments

- Configuration-driven interface reduces need for specialized SOA skill sets

- Heterogeneous interoperability enables secure integrations with partners, customers, and/or vendors

 Secures next-generation applications with an XML and SOAP firewall that filters any content, metadata, or network variables at wirespeed.

 Validates XML schemas and messages, protecting against XML attacks, buffer overflows, or vulnerabilities in malformed XML documents.
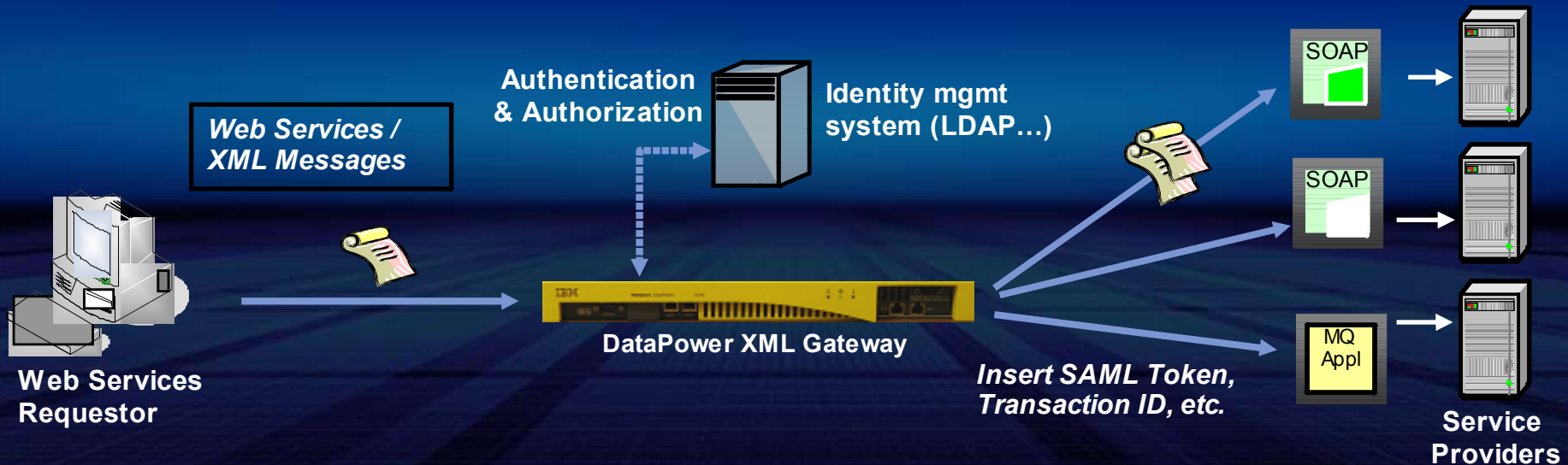
 Provides field-level XML security through encryption/decryption and signing/ verification of entire messages or individual XML fields.
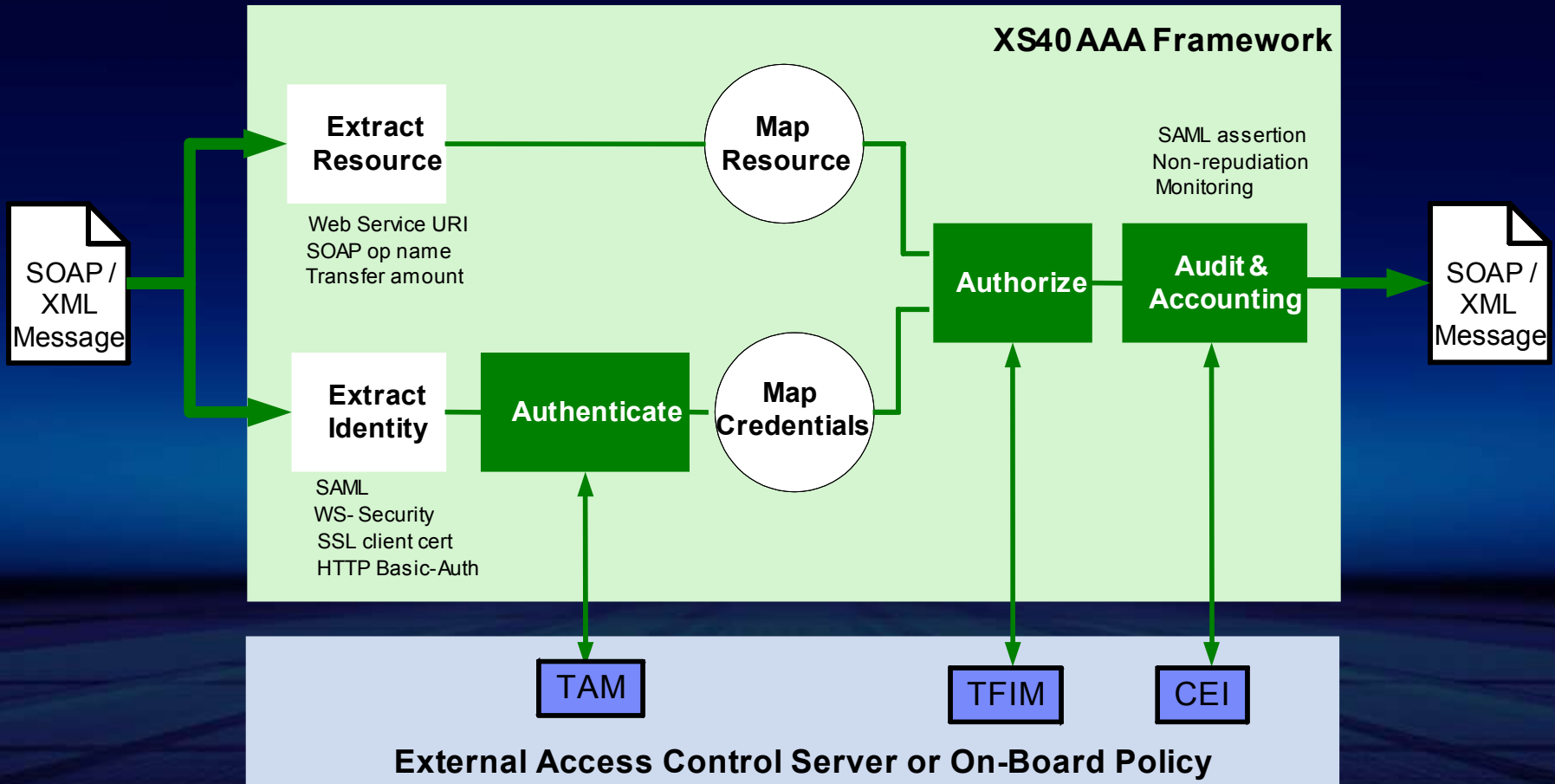
 Supports a variety of access control mechanisms, and can control access by rejecting unsigned messages and verifying signatures within SAML assertions.

Comprehensive Web Services & XML Security

- <u>Encryption of transport layer</u> - HTTP, HTTPS, SSL
- <u>XML/SOAP Firewall</u> - Filter on any content, metadata or network variables
- <u>Data Validation</u> - Approve incoming/outgoing XML
- <u>Field Level Security</u> - WS-Security, encrypt & sign individual fields, non-repudiation
- <u>Access Control</u> (AAA) - enforces access policy stored in an Identity Management Solution
- <u>Message Enrichment</u> – Insert header info, SAML token, Kerberos token, transaction ID…
- <u>Anti Virus Protection</u> - integrates with corporate virus checking through ICAP protocol
- <u>Security standards</u> - WS-Security, WS-Policy, SAML, XACML, WS-Trust, WS-Addressing…

Web Services / XML Messages

Authentication & Authorization

Identity mgmt system (LDAP…)

DataPower XML Gateway

Web Services Requestor

Insert SAML Token, Transaction ID, etc.

SOAP

SOAP

MQ Appl

Service Providers

DataPower AAA Framework Diagram

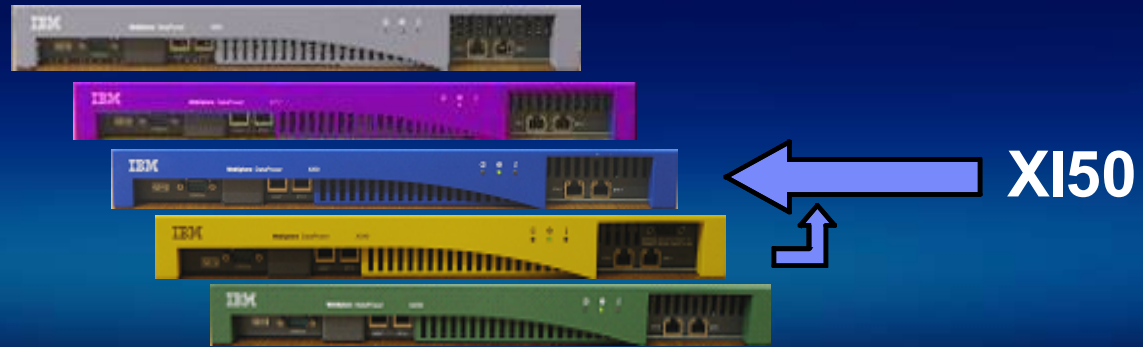# XML Threats - *Security Risks Growing*

- XML Entity Expansion and Recursion Attacks
- XML Document Size Attacks
- XML Document Width Attacks
- XML Document Depth Attacks
- XML Wellformedness-based Parser Attacks
- Jumbo Payloads
- Recursive Elements
- MegaTags – aka Jumbo Tag Names
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- Message Tampering

- Data Tampering
- Message Snooping
- XPath Injection
- SQL injection
- WSDL Enumeration
- Routing Detour
- Schema Poisoning
- Malicious Morphing
- Malicious Include – also called XML External Entity (XXE) Attack
- Memory Space Breach
- XML Encapsulation
- XML Virus
- Falsified Message
- Replay Attack
- …others

SQL injection…

See: http://www.areino.com/hackeando/

Meet the Family..

XI50

Integration Appliance XI50
Purpose-built hardware ESB for simplified deployment and hardened security
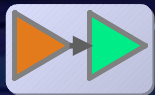

- Redefines the boundaries of middleware with specialized hardware

- Many functions integrated into a single device

- Simplified deployment and ongoing management

- Routes messages based on content and policy

Secures services on the network with sophisticated web services access control, policy enforcement, message filtering, and field-level encryption

Optimized to bridge between leading standard protocols at wirespeed, including web services, messaging, files, and database access

Enables transformation between a wide range of data formats, including XML, legacy, and industry standards, and custom formats

Captures and emits events to facilitate web services management and enable business visibility in Business Activity Monitoring solutions

Integration Appliance XI50

Purpose-built hardware ESB for simplified deployment and hardened security
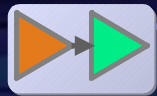
- Redefines the boundaries of middleware with specialized hardware

- Many functions integrated into a single device

- Simplified deployment and ongoing management

- Routes messages based on content and policy

Secures services on the network with sophisticated web services access control, policy enforcement, message filtering, and field-level encryption

Optimized to bridge between leading standard protocols at wirespeed, including web services, messaging, files, and database access

Enables transformation between a wide range of data formats, including XML, legacy, and industry standards, and custom formats

Captures and emits events to facilitate web services management and enable business visibility in Business Activity Monitoring solutions

Provide Service Enrichment
The ESB

An Enterprise Service Bus (ESB) is a flexible connectivity infrastructure for integrating applications and services.
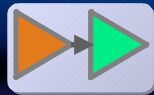
An ESB performs the following between requestor and service

MATCHES & ROUTES
communications between services

CONVERTS
between different transport protocols

TRANSFORMS
between different data formats

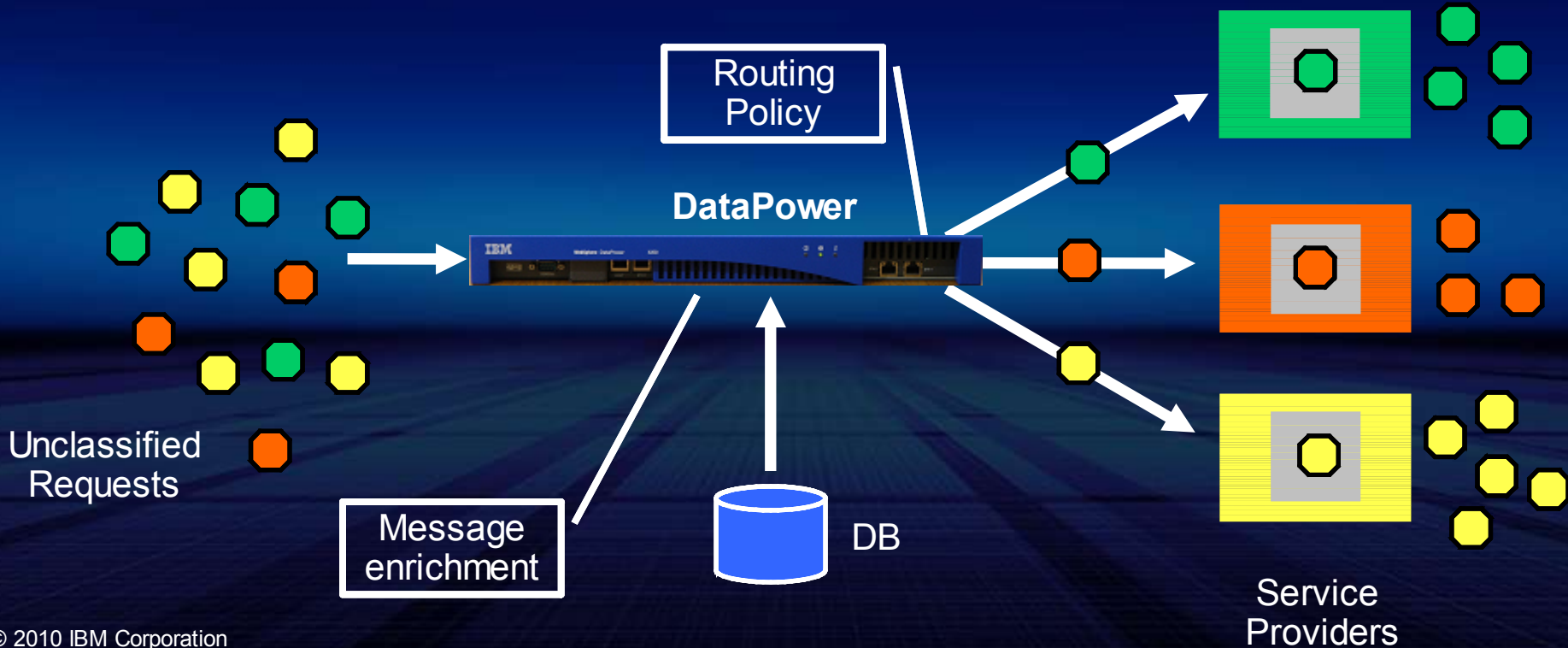**IDENTIFIES & DISTRIBUTES**
business events

ESB

Shape = Transport protocol

Color = Data format

Deep-Content Routing/Aggregation

- Route based on
  - IP information
  - SSL parameters
  - HTTP headers
  - XPath on XML/SOAP

- Load balancing
- Enrich and aggregate messages with data from
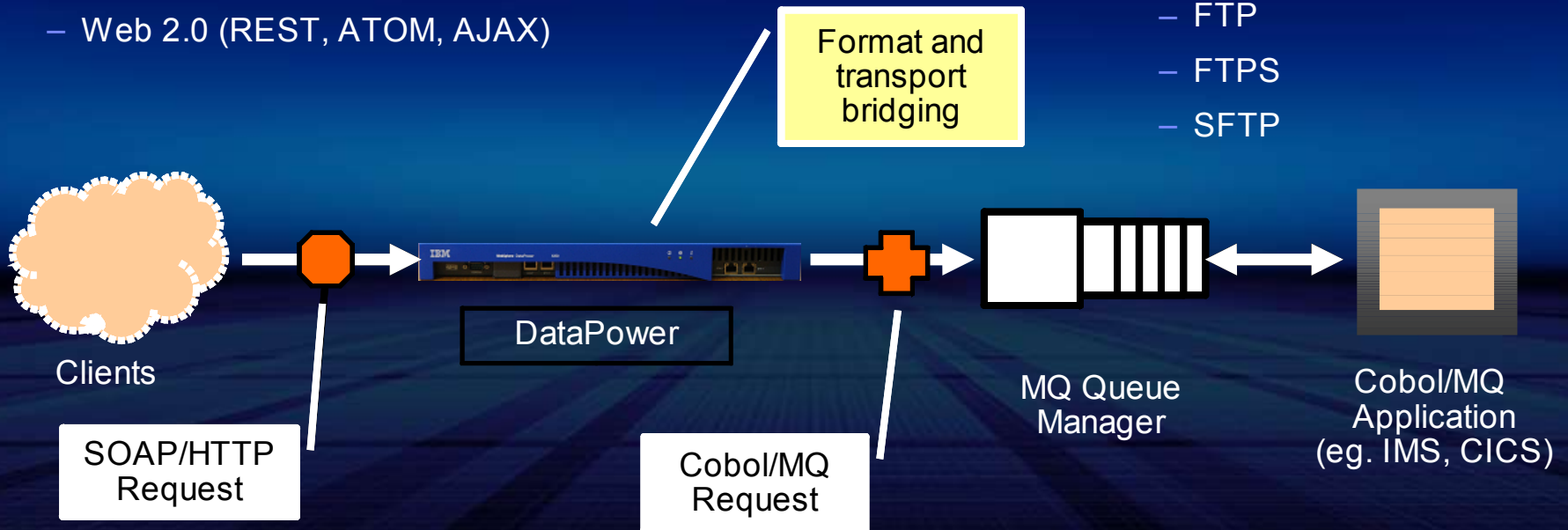 - A remote Web Service
  - A database

Routing Policy

DataPower

Message enrichment

DB

Unclassified Requests

Service Providers

Protocol Bridging & Transformation

- **Application formats**
  - EDI
  - Binary Formats
  - CORBA
  - CICS
  - ISO 8583
  - CSV
  - ASN.1
  - ebXML
  - Web 2.0 (REST, ATOM, AJAX)

- **Transport protocols**
  - HTTP
  - HTTPS
  - MQ
  - SSL
  - SOAP
 - Tibco
  - JMS
  - FTP
  - FTPS
  - SFTP

Format and transport bridging

Clients

SOAP/HTTP Request

DataPower

Cobol/MQ Request

MQ Queue Manager

Cobol/MQ Application (eg. IMS, CICS)

A choice of ESBs

IBM offers three ESBs to choose

WebSphere ESB

ESB offerings from IBM WebSphere

WebSphere Message Broker

Optimized with WebSphere Application server for an integrated SOA platform

WebSphere DataPower Integration Appliance XI50

IBM
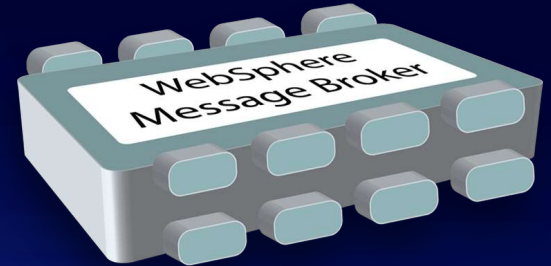
Built for universal connectivity and transformation in heterogeneous IT environments
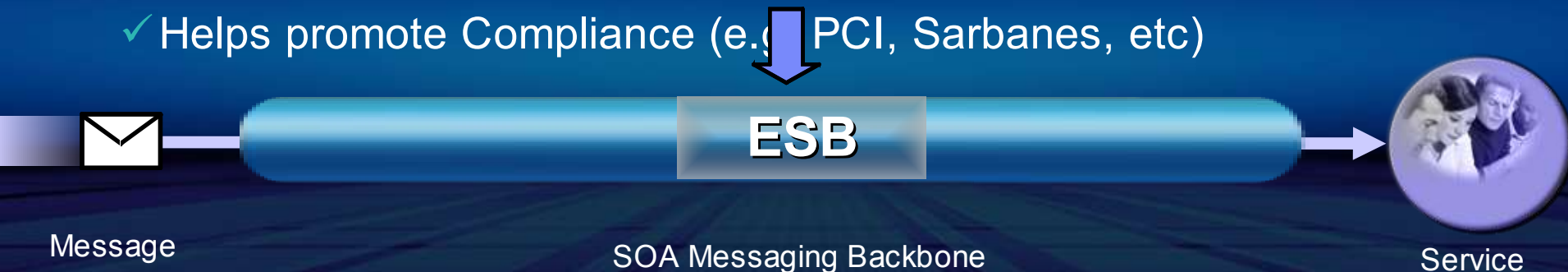
Purpose-built hardware for simplified deployment and hardened security

Departments have differing ESB requirements which are best met by different products

Smart **SOA**

Traditional ESB
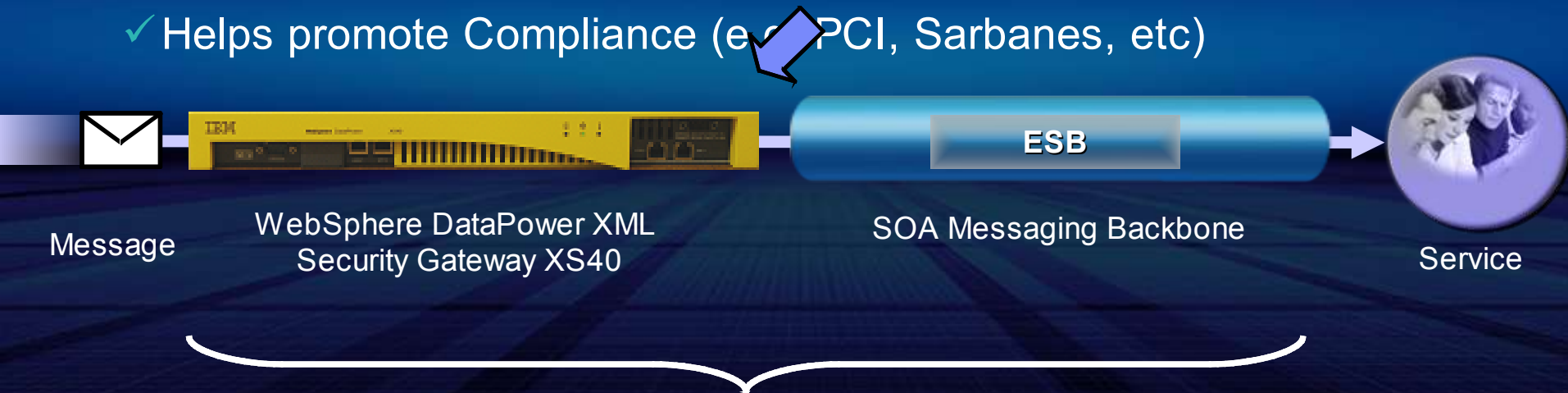
✓ XML firewall and filtering helps stop SOA threats

✓ Message-level encryption and access control enforcement

✓ Web services Authentication, Authorization & Auditing

✓ Transformation/Mapping

✓ Helps promote Compliance (e.g. PCI, Sarbanes, etc)

ESB

Message

SOA Messaging Backbone

Service

Extend your ESB to partners and customers
WebSphere DataPower XML Security Gateway XS40

✓ XML firewall and filtering helps stop SOA threats

✓ Message-level encryption and access control enforcement

✓ Web services Authentication, Authorization & Auditing

✓ Transformation/Mapping

✓ Helps promote Compliance (e.g. PCI, Sarbanes, etc)

Message

WebSphere DataPower XML
Security Gateway XS40

ESB

SOA Messaging Backbone

Service

ESB

Extend your ESB to partners and customers
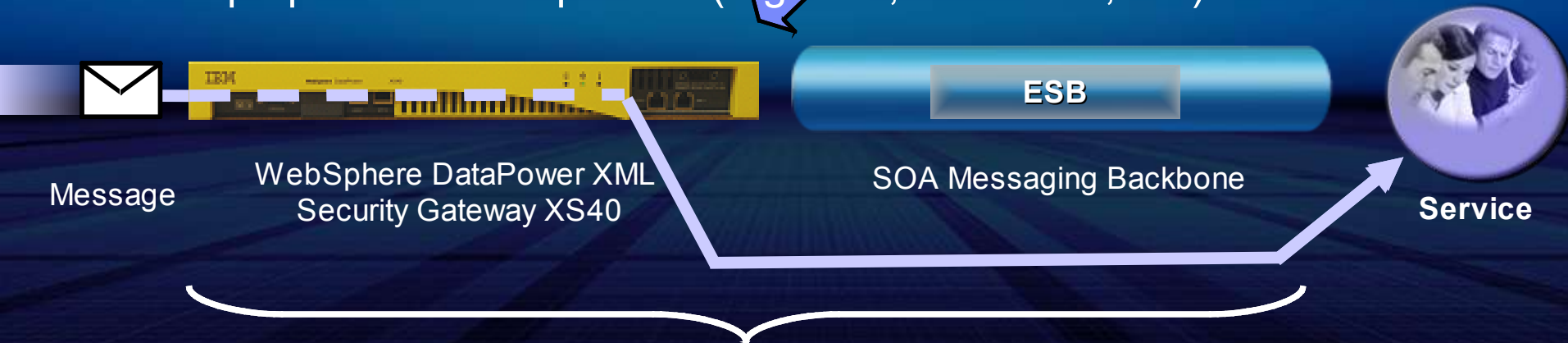## WebSphere DataPower XML Security Gateway XS40

✓ XML firewall and filtering helps stop SOA threats

✓ Message-level encryption and access control enforcement

✓ Web services Authentication, Authorization & Auditing

✓ Transformation/Mapping
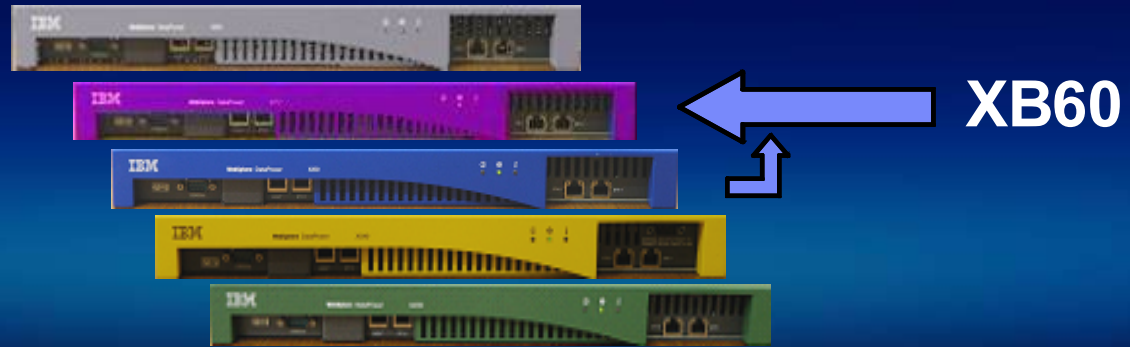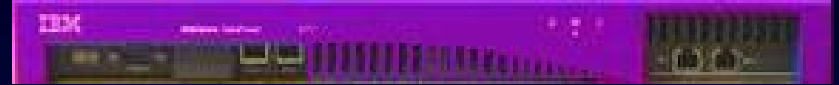
✓ Helps promote Compliance (e.g. PCI, Sarbanes, etc)

ESB

Message

WebSphere DataPower XML
Security Gateway XS40

SOA Messaging Backbone

Service

ESB

Meet the Family..

XB60

Business to Business (B2B) Appliance XB60

Purpose-built B2B hardware for simplified deployment, exceptional performance and hardened security

- Extend integration beyond the enterprise with B2B

- Hardened Security for DMZ deployments

- Easily manage and connect to trading partners using industry standards

- Simplified deployment and ongoing management

Trading Partner Management for B2B Governance; B2B protocol policy enforcement, access control, message filtering, and data security

Application Integration with standalone B2B Gateway capabilities supporting B2B patterns for AS1, AS2, AS3, ebXML, Web Services
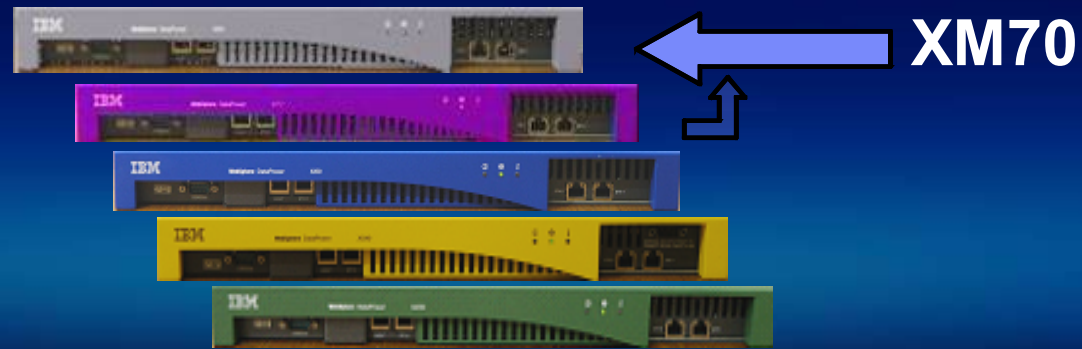
Full featured User Interface for B2B configuration and transaction viewing; correlate documents and acknowledgments displaying all associated events
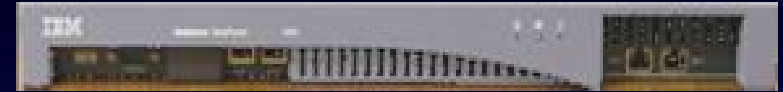
Simplified deployment, configuration and management providing a quicker time to value by establishing rapid connectivity to trading partners

Meet the Family..

XM70

Low Latency Appliance XM70

Purpose-built hardware for low-latency, network-based messaging and data feed processing

- Drop-in messaging solution which plugs into existing network infrastructure

- Enhanced QoS and performance with purpose-built hardware

- Simplified, configuration-driven approach to low-latency, publish/subscribe messaging and content-based routing

- High availability out of the box (two or more appliances)

Low-latency unicast and multicast messaging, scaling to 1M messages / sec with microsecond latency

Destination, property and content-based routing, including native XML and FIX parsers
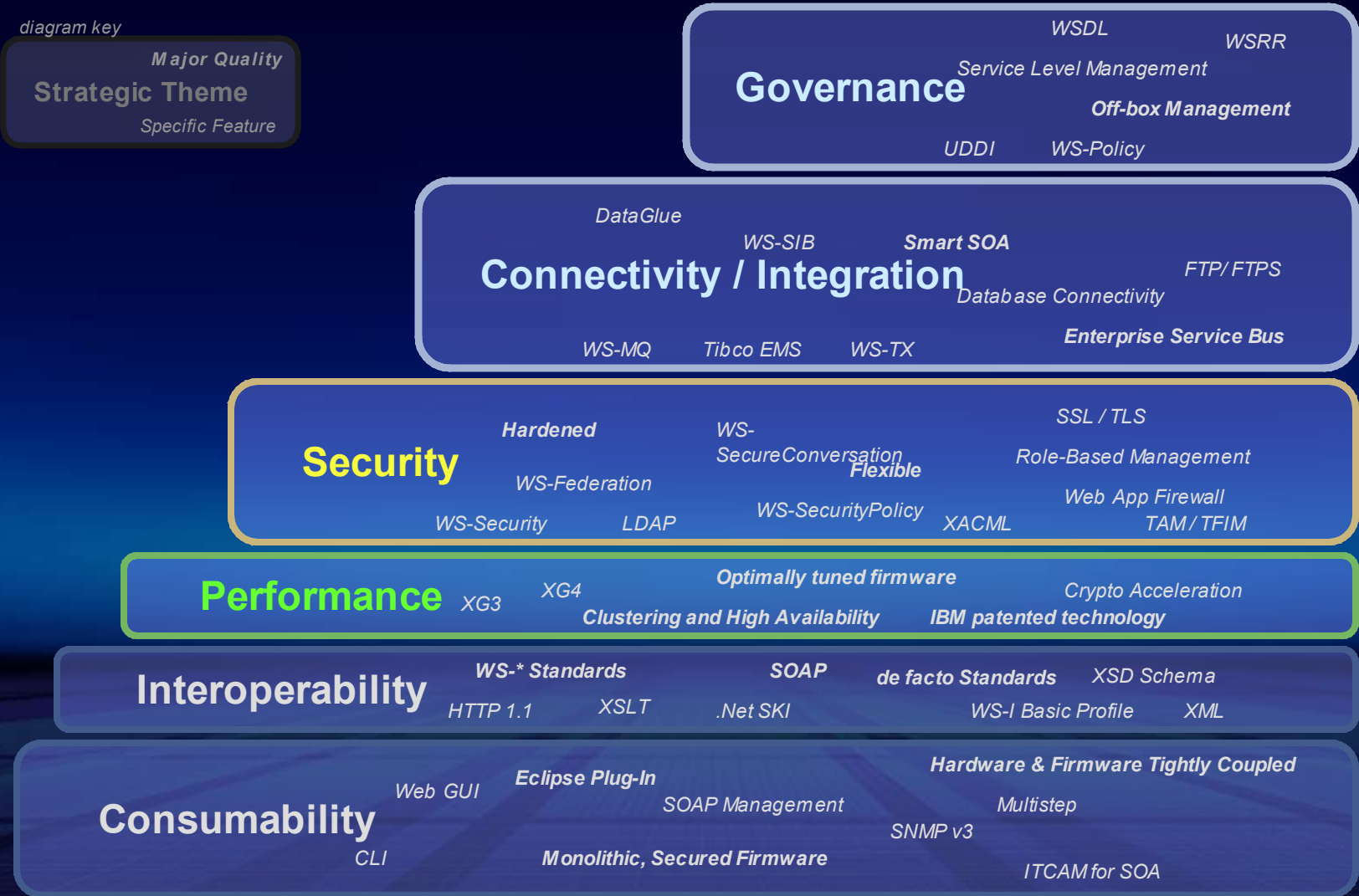
Optimized to bridge between leading standard messaging protocols such as MQ, Tibco, WebSphere JMS and HTTP(S)

Simplified deployment, configuration and management providing a quicker time to value by rapidly configuring messaging destinations, connectivity and routing
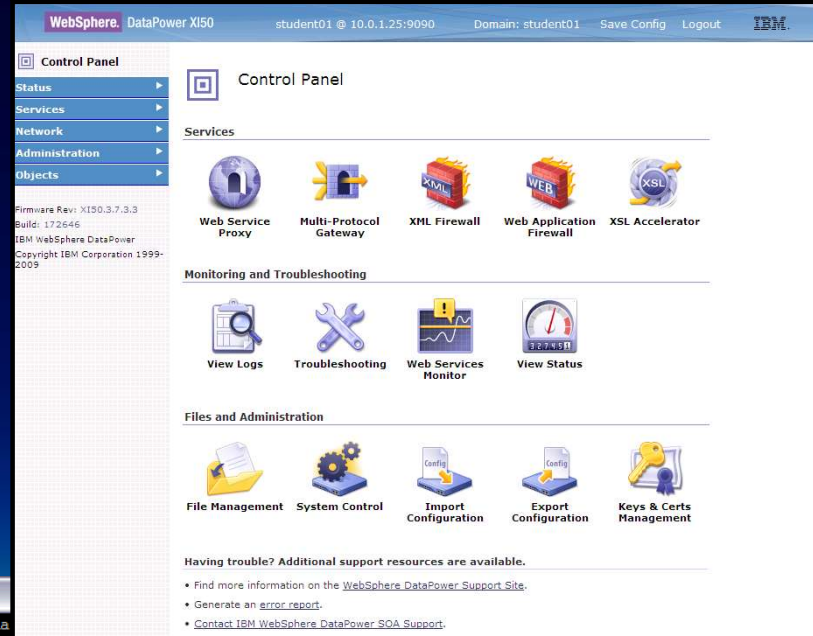
WebSphere DataPower Base Qualities & Features

Smart SOA

Maslow's Hierarchy of Enterprise Needs

diagram key

Major Quality	
Strategic Theme	
Specific Feature	

Governance

WSDL
WSRR
Service Level Management
Off-box Management
UDDI   WS-Policy

Connectivity / Integration

DataGlue
WS-SIB   **Smart SOA**
FTP/ FTPS
Database Connectivity
WS-MQ   *Tibco EMS*   *WS-TX*   **Enterprise Service Bus**

Security

Hardened   WS-SecureConversation   *SSL / TLS*
WS-Federation   **Flexible**   *Role-Based Management*
WS-Security   LDAP   WS-SecurityPolicy   XACML   *Web App Firewall*   *TAM / TFIM*

Performance

XG3   XG4   **Optimally tuned firmware**   *Crypto Acceleration*
Clustering and High Availability   **IBM patented technology**

Interoperability

WS-* Standards   **SOAP**   **de facto Standards**   XSD Schema
HTTP 1.1   XSLT   .Net SKI   WS-I Basic Profile   XML

Consumability

Hardware & Firmware Tightly Coupled
Web GUI   **Eclipse Plug-In**   SOAP Management   Multistep
SNMP v3
CLI   **Monolithic, Secured Firmware**   ITCAM for SOA

Simple Appliance Configuration for Robust Connectivity Functionality

Fits into your existing environment:

- Address broad organizational needs (Architects, Developers, Network Operations, Security)

- Complete Configuration from WebGUI, CLI interface or SOAP Managment interface

- IDE integration/Eclipse plug-in

- XPath / XML config files

Why an Appliance for SOA?
Configuration vs. Programming

-Configuration driven Web GUI

-Drag & Drop Workflow Style

-Implement Complex Policies

-No Programming, Less Errors

- All Functions Available via WebGUI, CLI & SOAP Interface
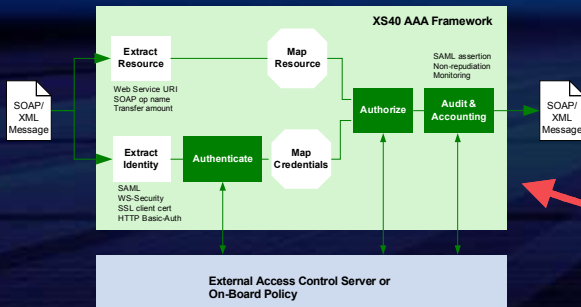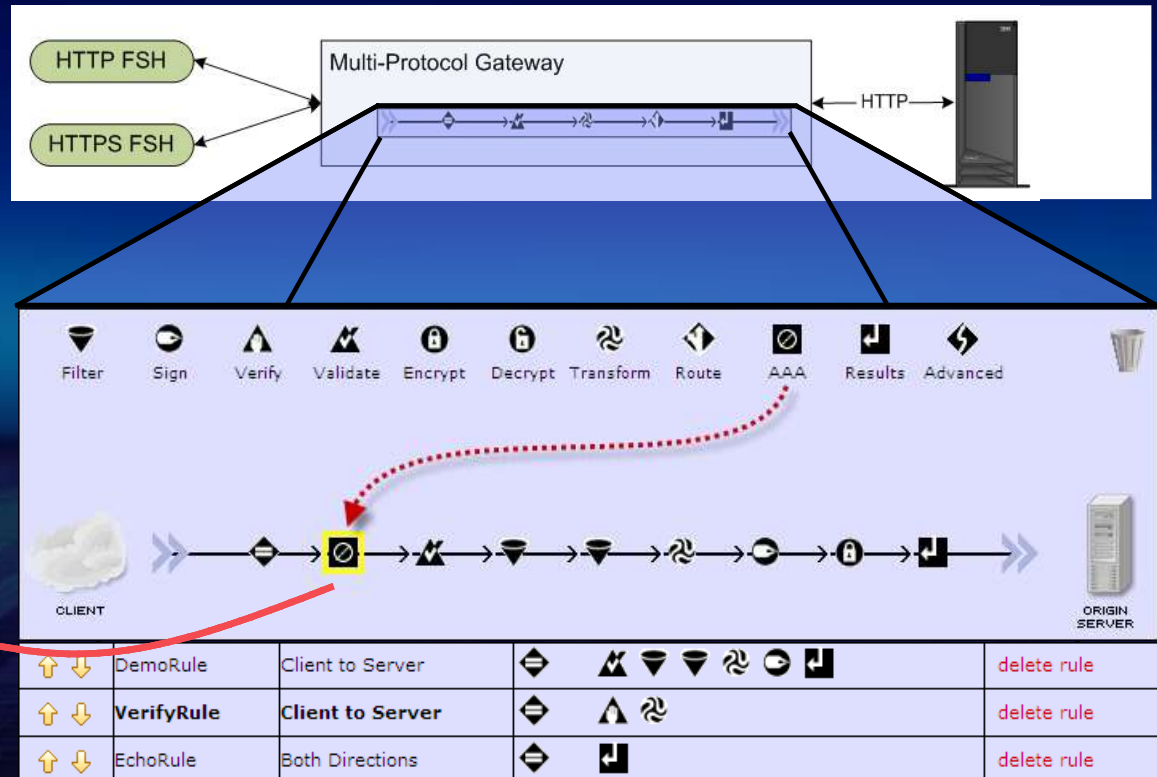
Governance and enforcement for secure connectivity

- **Natural fit for a high-speed, secure, message-aware hardware device**

- **Standards based centralized governance**
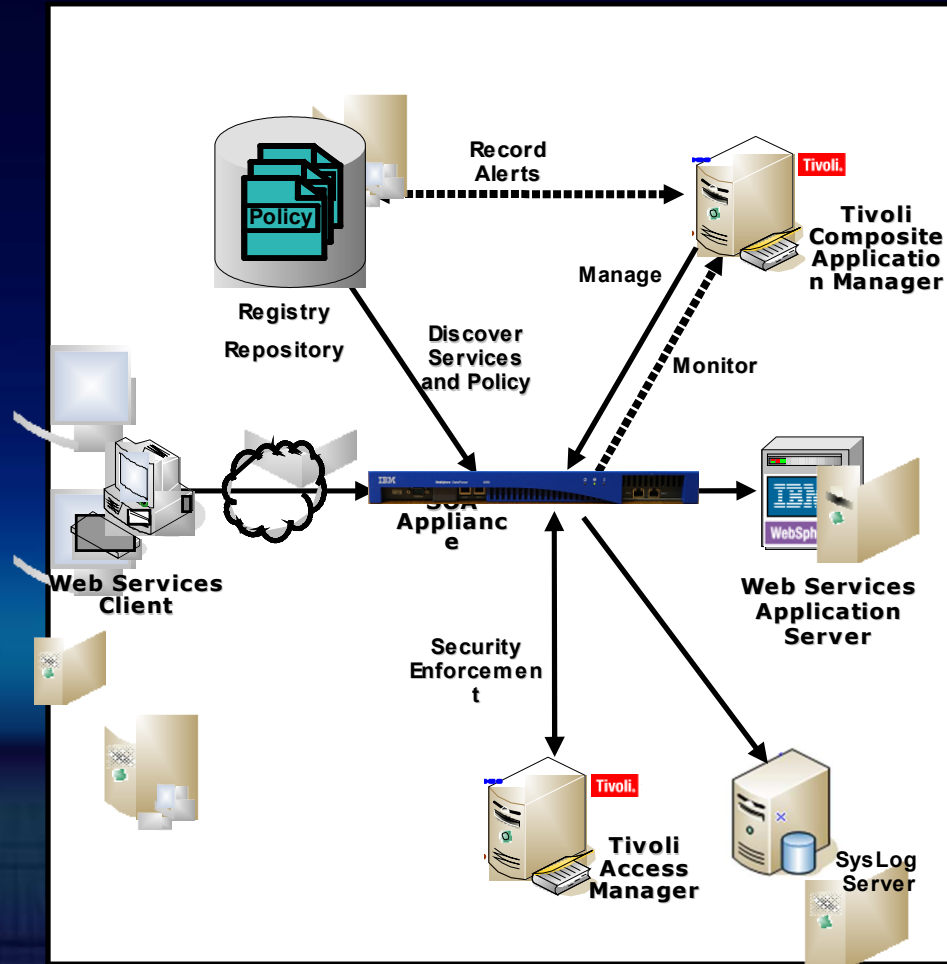 - WS-Policy and WS-SecurityPolicy
  - Integration with centralized policy stores
  - Lowers risk and management cost
  - IBM WebSphere Registry and Repository
  - UDDI v2 and v3

- **Centralized management and monitoring**
  - ITCAM SE, ITCAM for SOA, WS-Management, SOAP Management Interfaces

- **Process Integrity**
  - Service Level Monitoring
  - Authentication and Authorization
  - Extended logging option
  - Off-device logs

- **Security governance**
  - Hardware XACML enforcement
  - Existing SSO's (LDAP, 3rd party)
  - IBM TAM and TFIM

Registry Repository

Record Alerts

Tivoli Composite Application Manager

Manage

Discover Services and Policy

Monitor

Web Services Client

SOA Appliance

Web Services Application Server

Security Enforcement

Tivoli Access Manager

SysLog Server

![Smart SOA]

WebSphere DataPower Solution Categories

SOA Integration / ESB Enrichment and Messaging

– Efficiently transforming, routing, logging messages among applications and Web services using multiple protocols and data formats (XML and non-XML)

– Connecting Z or legacy applications to Web services/SOA

ESB & SOA Security

Securely enabling access to back-end systems for partners and customers

Protecting against XML-borne threats

SOA Governance & Policy Enforcement

– Manage Web services easily through service-level management, security management, enterprise management console, registry/repository integration

Business-to-Business Gateway

Extend integration beyond the enterprise with B2B

Easily manage and connect to trading partners using industry standards
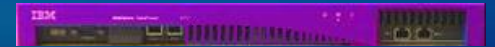
Low Latency Messaging

– Drop-in messaging solution which plugs into existing network infrastructure

– Simplified, configuration-driven approach to low-latency, publish/subscribe messaging and content-based routing

WebSphere DataPower Appliance Use Cases

Securing Web Services

Securely enabling access to back-end systems for partners and customers

Protecting against XML-borne threats

Legacy Integration

Connecting mainframe or legacy application to Web services/SOA

XML-enabling legacy systems via MQ

SOA Integration / Enterprise Service Bus (ESB)

Efficiently transforming, routing, logging messages among applications and Web services using multiple protocols and data formats (XML and non-XML)

SOA Runtime Governance

Manage Web services easily through service-level management, security management, enterprise management console, registry/repository integration

Web Application Firewall

Protect web application assets
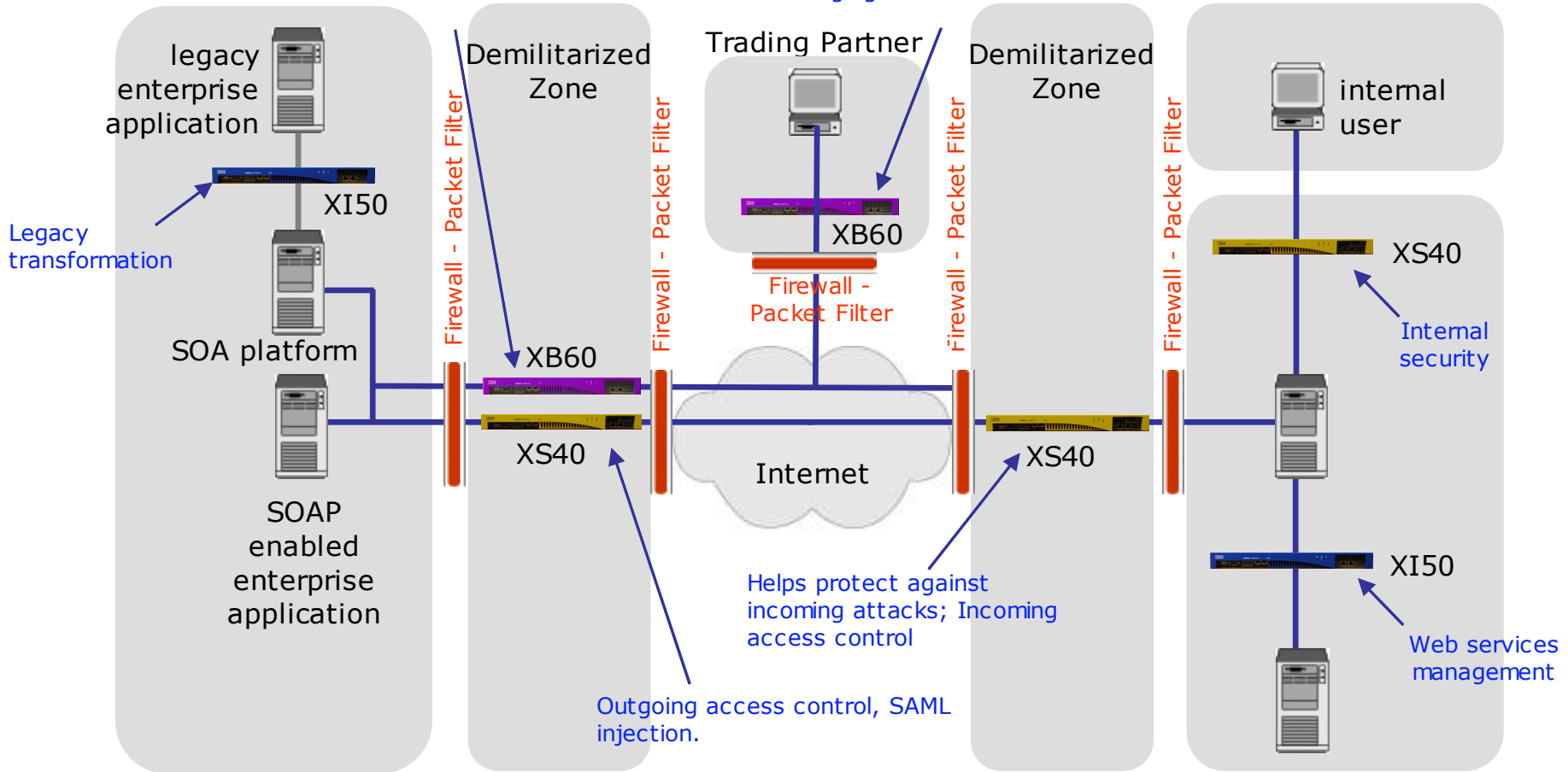
Deployment Scenarios for Advanced Connectivity

Federated Extranet

B2B Governance through adherence to the AS1, AS2, AS3 and ebXML Standards

legacy enterprise application

XI50

Legacy transformation

SOA platform

SOAP enabled enterprise application

Firewall – Packet Filter

Demilitarized Zone

XB60

XS40

Outgoing access control, SAML injection.

Internet

Outgoing B2B messages that support Trading Partner Agreements for AS1, AS2, AS3 and ebXML messaging

Trading Partner

XB60

Firewall – Packet Filter

Firewall – Packet Filter

Internet

Helps protect against incoming attacks; Incoming access control

Demilitarized Zone

XS40

Firewall – Packet Filter

Intranet

internal user

XS40

Internal security

XI50

Web services management

Firewall – Packet Filter

Integration across the IBM Software Portfolio

- **Mature integration within WebSphere software portfolio**
  - *WebSphere MQ with WebSphere DataPower: 4+ years, numerous customers*
  - *Industry-leading SOA Runtime Governance with WSRR + DataPower*
  - *Many more examples: WTX for data maps, WS-Security for WMB*
  - *Auto-configure XML firewall by importing WebSphere service descriptors*
- **Complete SOA Security and Management solution with Tivoli products**
- **Robust enterprise integration through native DB2 and IMSConnect**
  - *Deliver data as Web services into new or existing SOA solutions with DataPower/Data Studio integration*
- **IBM Autonomic Integration – CBE/CEI Certified**

Rational software

RAD, Eclipse

WebSphere software

WebSphere MQ,
HTTP,
JMS,
Web Services

WSRR,
WTX,
WS-Security
WS-Policy

IMSConnect

DB2 software

SQL, Xquery,
Data Studio

TAM, TFIM,
ITCAM4SOA,
WS-Trust,
SAML,
XACML

LDAP,
SNMP,
Syslog,
AMP,
NetView

Tivoli software

©
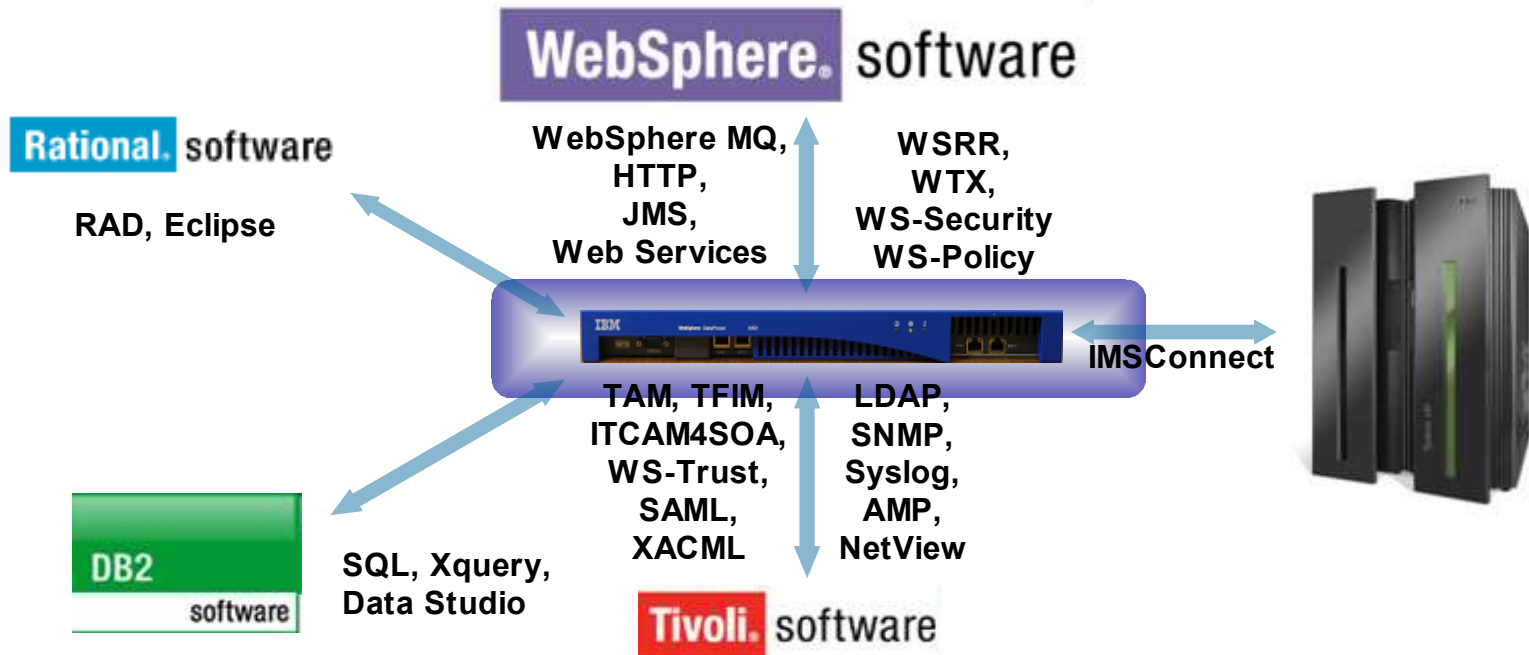
Integration with the Competition

- Standards-based integration with third party vendors
- Tighter integration with some key competitors
- No platform dependencies – hardware or software
- Exceptional interoperability through industry profiles and testing
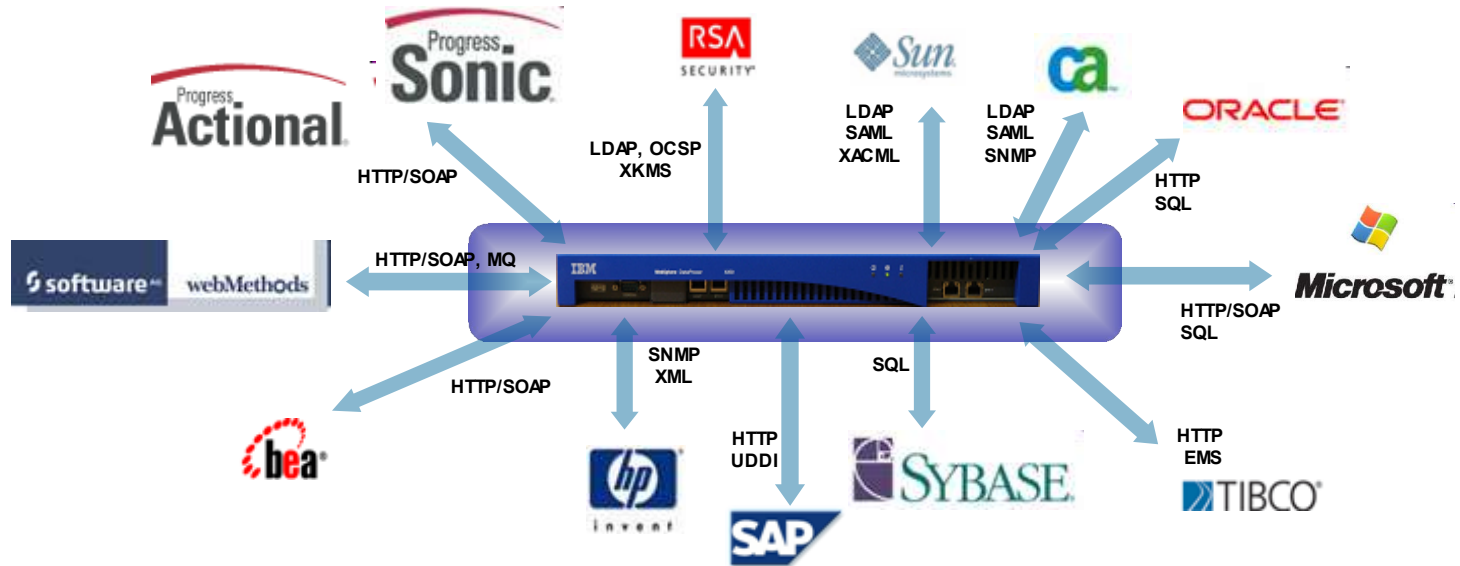
WebSphere DataPower Appliances Benefits

- **Flexible Connectivity**: an XML appliance shields the applications from security requirements, protocol changes and service versioning - no application modifications needed

- **Reduce Complexity**: Replace software servers functionality with an XML appliance, reduce infrastructure footprint, and off-load heavy processes to dedicated XML appliances

- **Lower TCO**: Dedicated XML appliances have shown to reduce operational costs by as much as 50%

- **Improved Agility by Reduced Time to Market**: dramatically decrease the testing time and amount of development required to upgrade your environment, most policies are configuration driven as opposed to development driven

- **Reduce Risk**: the XML appliance provides the connectivity layer without requiring application modification, and delivers improved security and audit support

- **Configuration Driven**: The XML appliance is configuration driven to do policy definitions, it does not involve development to support your infrastructure

DataPower 'Proof Of Technology'

You're invited!

Smart SOA

- **Discovering the Value of IBM WebSphere DataPower SOA Appliances!**

A one-day Proof of Technology (PoT) provides a hands-on experience for those needing to understand how DataPower appliances.

The objective of the session is to provide participants with a hands-on experience creating and testing configurations that demonstrate a variety of scenarios that are common in SOA implementations.

This Proof of Technology is specifically targeted for Enterprise Architects, Systems Architects, and Security Architects evaluating architectural solutions for SOA deployments.

Thank you