IBM
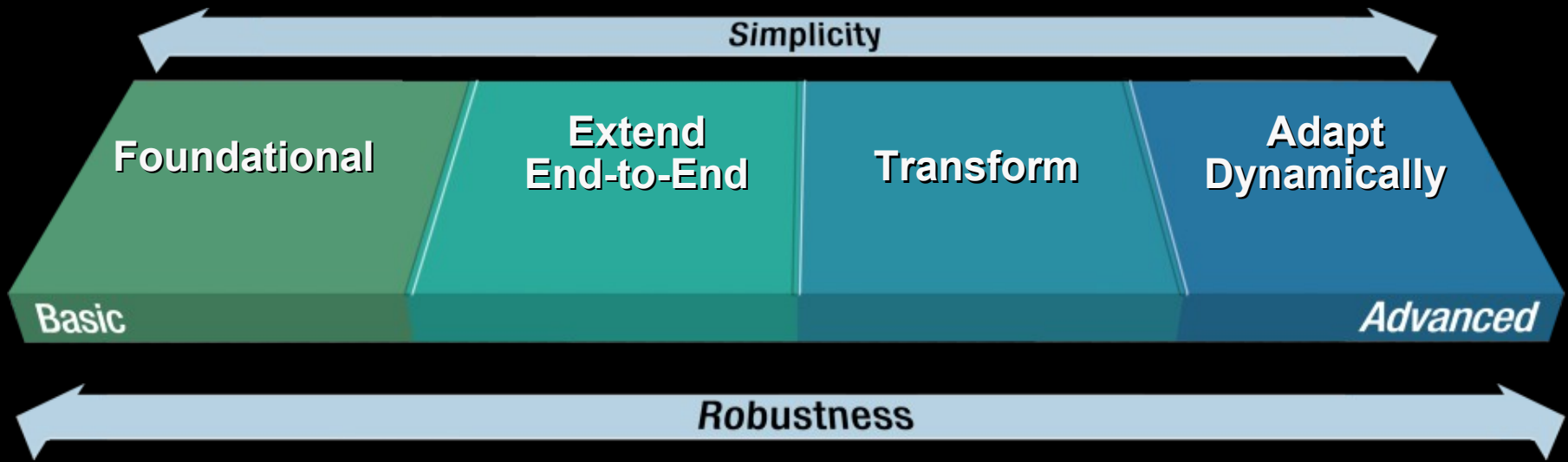
DataPower SOA Appliances
Simplify, Accelerate, Secure, Integrate & Manage SOA

Bharat Bhushan
DataPower Specialist
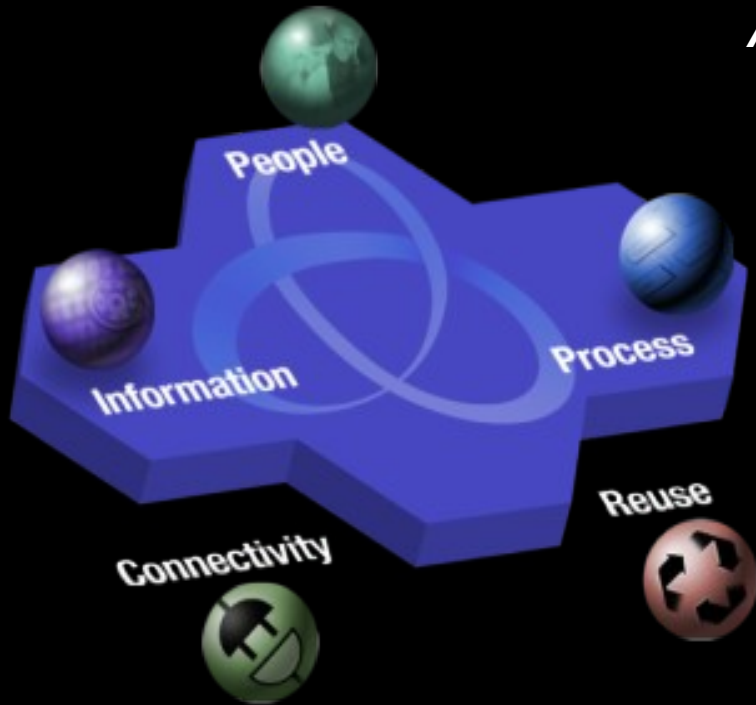Bharat.Bhushan@uk.ibm.com

IBM Delivers a Smart Approach to SOA Adoption
Aligning service-oriented approaches

A set of guiding principles to help extend the business value of deployments

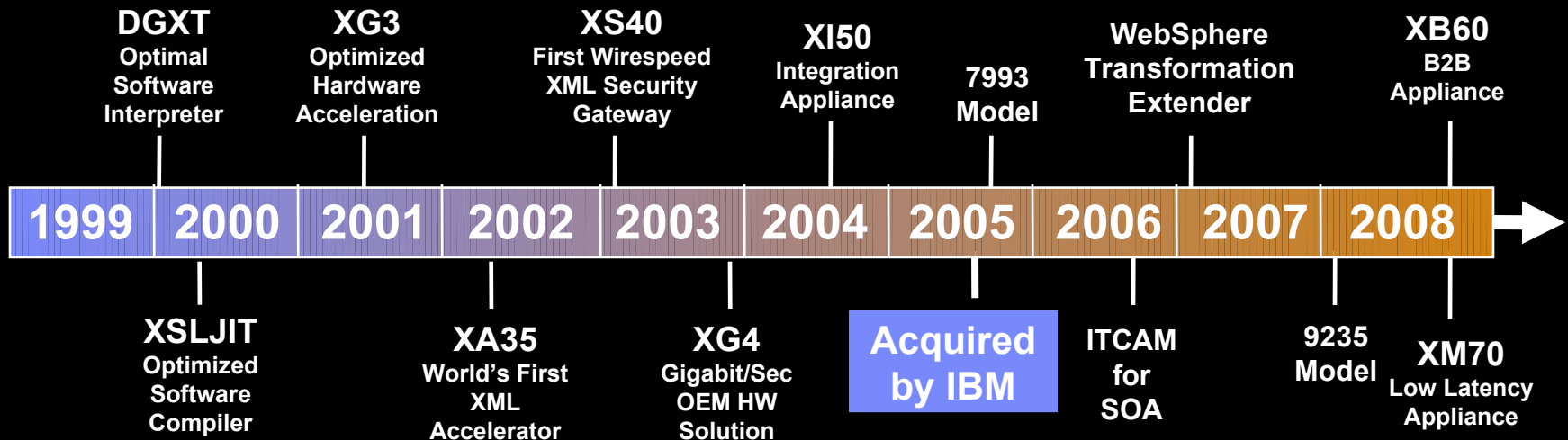# IBM's Acquisition of DataPower

An SOA Appliance…

creates customer value through extreme SOA performance, connectivity, and security.

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

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

DataPower Pre-IBM Overview

- Extensive experience in XML processing optimization

- Setting standards in XML since 1999

- Advantages: First to Market, Great Team, Deep Standards Involvement, Invented and Owns Core XML Technology, Comprehensive product portfolio

| DGXT Optimal Software Interpreter | XG3 Optimized Hardware Acceleration | XS40 First Wirespeed XML Security Gateway | XI50 Integration Appliance | 7993 Model | WebSphere Transformation Extender | XB60 B2B Appliance |

| 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 |

| XSLJIT Optimized Software Compiler | XA35 World's First XML Accelerator | XG4 Gigabit/Sec OEM HW Solution | Acquired by IBM | ITCAM for SOA | 9235 Model | XM70 Low Latency Appliance |

Post-Acquisition Innovation Continues

- 600% growth since acquisition

- Continuous hardware improvements for features and reliability

- Expanded product line – XA35, XS40, XI50, XB60, XM70

- Enhanced capabilities – WS-*, NFS, XG4, WSDL compiler, XACML, much more…

- Ongoing IBM Technology Integration – ITCAM for SOA, WebSphere JMS, DB2, WTX, etc.

Why an Appliance for SOA?

- Hardened, specialized hardware for helping to integrate, secure & accelerate SOA

- Many functions in a single device
  - Service level management, dynamic routing, policy enforcement, transformation

- Higher levels of security assurance certification
  - FIPS 140-2 Level 3, Common Criteria EAL4

- Higher performance with hardware acceleration facilitates security enforcement

- Addresses the divergent needs of different groups
  - Enterprise architects, network operations, security operations, web services developers

- Simplified deployment and ongoing management
  - Drop-in appliance, secures traffic in minutes, integrates with existing operations

WebSphere DataPower SOA Appliance Product Line

XM70

- High volume, low latency messaging
- Enhanced QoS and performance
- Simplified, configuration-driven approach to LLM
- Publish/subscribe messaging
- High Availability

XB60

- B2B Messaging (AS2/AS3)
- Trading Partner Profile Management
- B2B Transaction Viewer
- Unparalleled performance
- Simplified management and configuration

XA35

- Offload XML processing
- No more hand-optimizing XML
- Lowers development costs

XS40

- Enhanced Security Capabilities
- Centralized Policy Enforcement
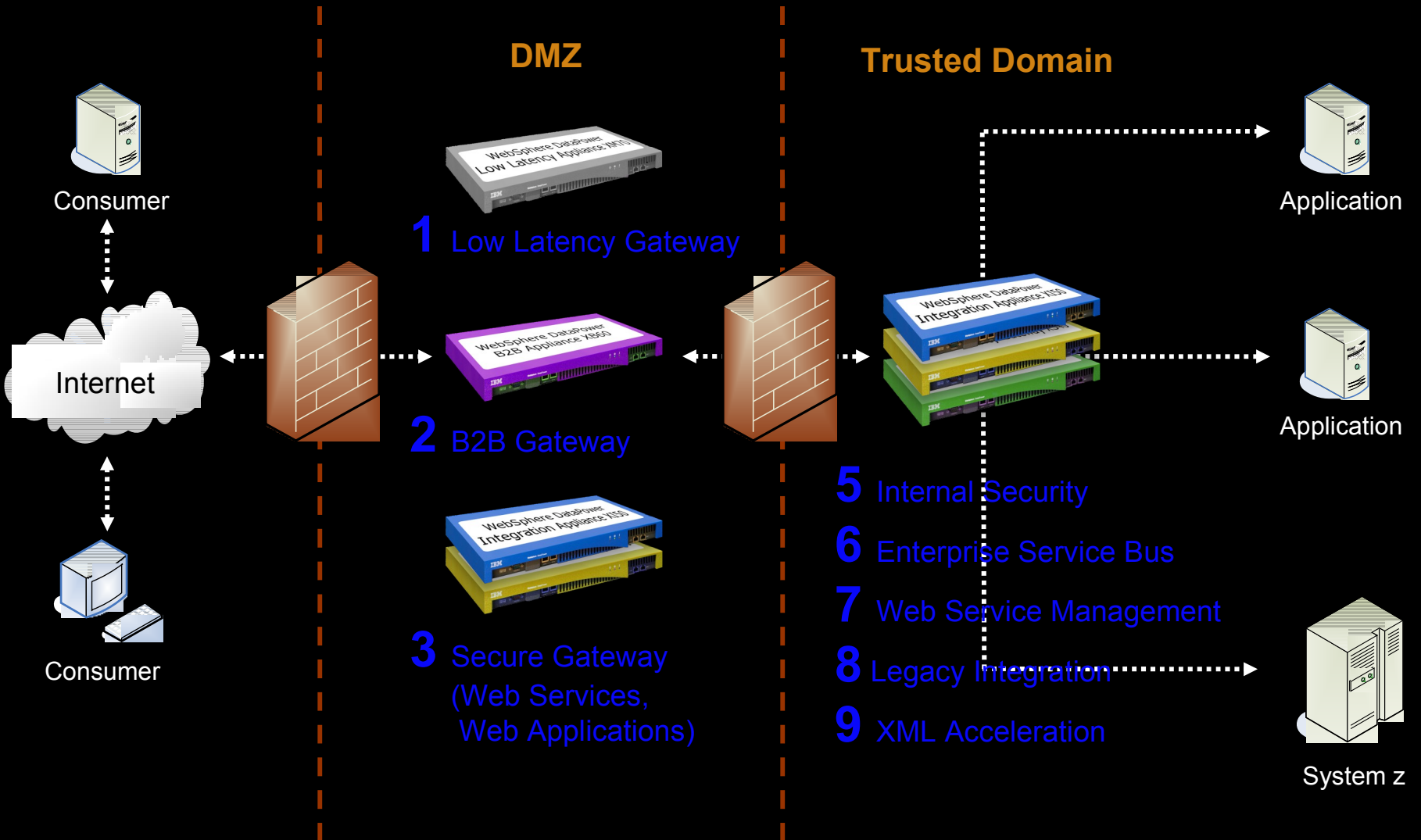- Fine-grained authorization
- Rich authentication

XI50

- Hardware ESB
- "Any-to-Any" conversion at wire-speed
- Bridges multiple protocols
- Integrated message-level security

WebSphere DataPower SOA Appliance Basic Use Cases

DMZ

Trusted Domain

Consumer

Application

Internet

1 Low Latency Gateway

2 B2B Gateway

Application

5 Internal Security

6 Enterprise Service Bus

7 Web Service Management

8 Legacy Integration

9 XML Acceleration

Consumer

3 Secure Gateway
(Web Services,
Web Applications)

System z

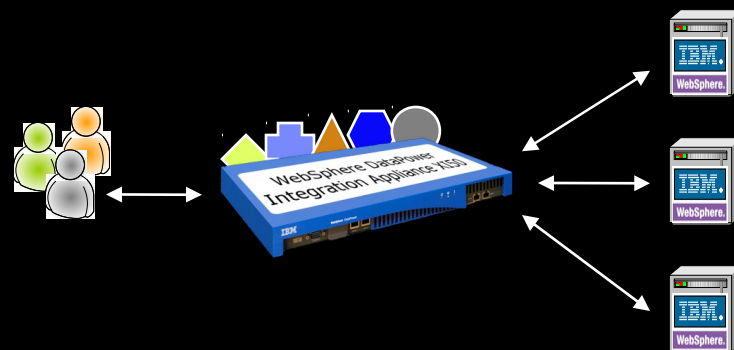# SOA Appliances Simplify and Centralize Key Functions

- Route, transform, and help secure multiple applications without code changes

- Lower cost and complexity

- Enable new business with unmatched performance

Before SOA Appliances

Authenticate

Transform

Encrypt/Decrypt

Validate
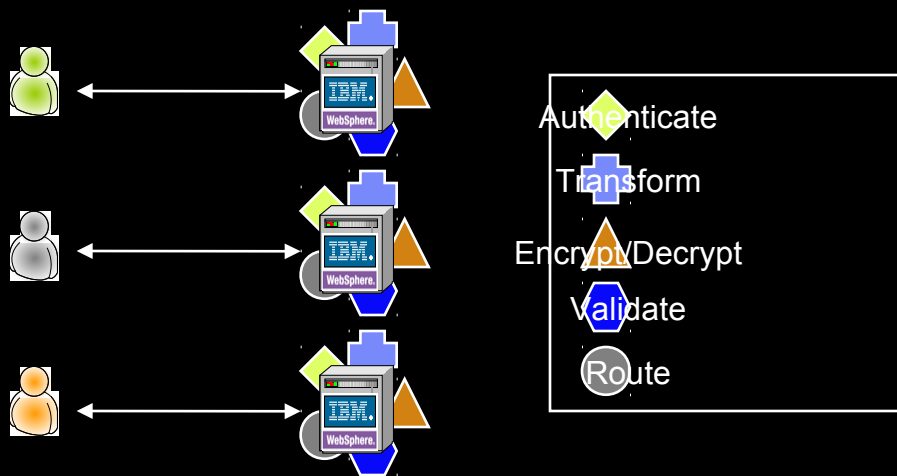
Route

Update application
servers individually

After SOA Appliances

Secure, route, transform all
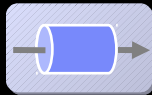applications instantly

No changes to applications

XML Accelerator XA35
Purpose-built hardware for presentation-tier transformation

- "The Original" DataPower XML Appliance

- Defines high performance architecture for all DataPower SOA Appliances

- Processes XML operations at "wire-speed"

- Ideal in an XSL-intensive HTTP presentation tier

XML Pipeline processing accelerates XML/XSLT/XPath evaluation, increasing throughput and decreasing latency by offloading XML operations to the network

Innovative drag-and-drop policy editor accelerates time to value and simplifies configuration and deployment

Logical application domains allow individual "sandboxes" and facilitate configuration management through import/export features

Multiple management interfaces serve varying needs of an organization, including browser-based WebGUI, command line CLI, and scriptable Web Services

XML Security Gateway XS40
Purpose-built hardware for assuring confidentiality, authenticity, and non-repudiation

- Native support for WS-Security policy enforcement

- Extremely secure hardware design

- Integrate with a variety of authentication and authorization systems for real-time protection

- Ideal in front-line DMZ or internal security gateway

XML/SOAP Firewall capabilities enable Layer 7 filtering on any content, metadata or network variable in a message

Web Application Firewall service offers additional security, threat mediation, and content processing for other URL encoded HTTP-based applications

Easily configurable field-level security options allow flexible enforcement of confidentiality, authenticity, and non-repudiation requirements
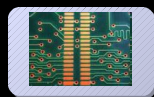
Low latency architecture leverages hardware-acceleration for cryptographic operations

Hardware Device for Improved Security

- Sealed network-resident appliance
  - Optimized hardware, firmware, embedded OS
  - Single signed/encrypted firmware upgrade only
  - No arbitrary software
  - High assurance, "default off" locked-down configuration
  - Security vulnerabilities minimized (few 3 party components)
  - Hardware storage of encryption keys, locked audit log
  - No USB ports, tamper-proof case
- Third party certification
  - FIPS 140-2 level 3 HSM (option)
  - Common Criteria EAL4

> *"The DataPower [XS40]... is the most hardened ... it looks and feels like a datacenter appliance, with no extra ports or buttons exposed… "*
> - InfoWorld

IBM

XML security threats are growing
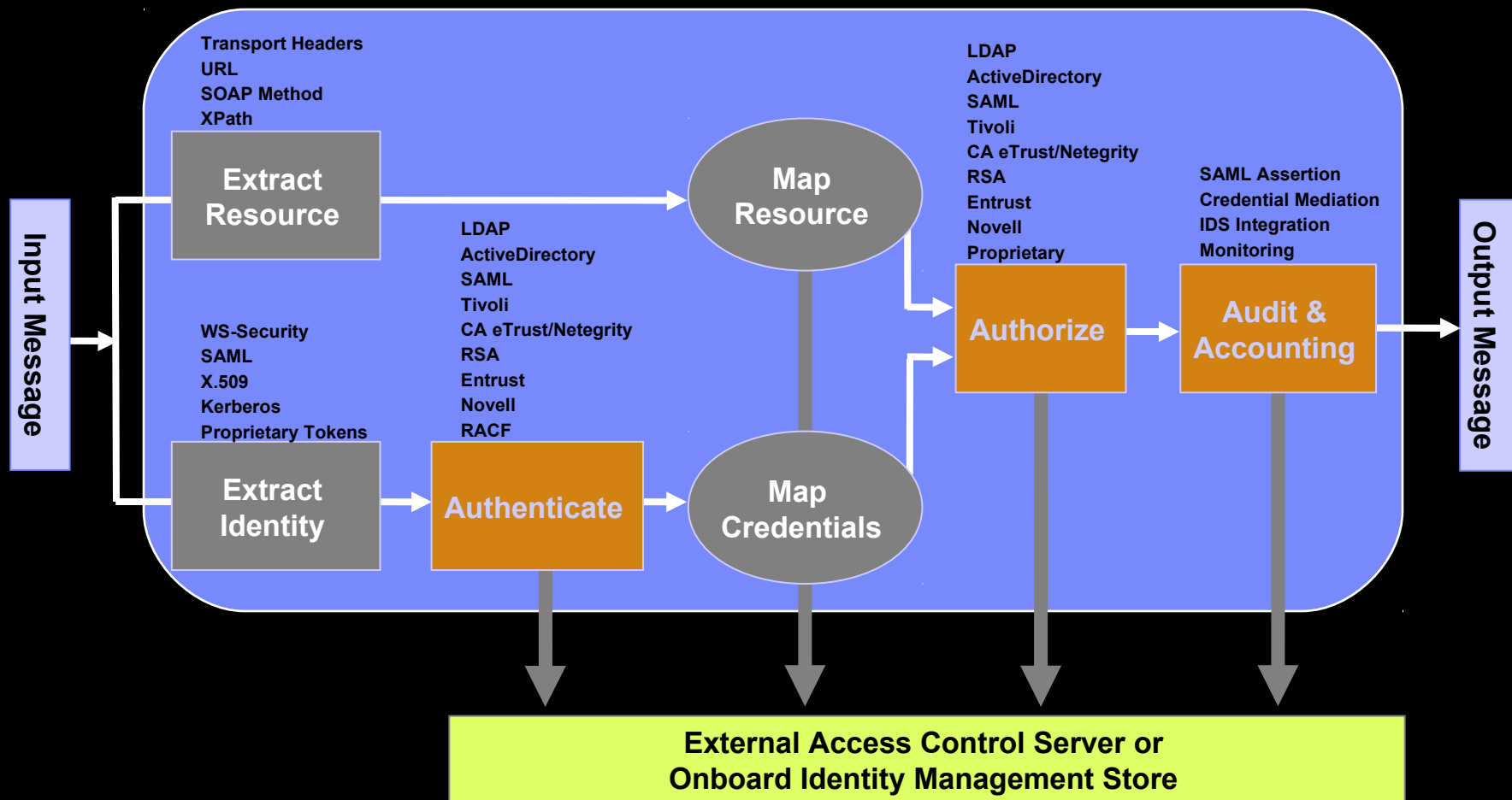*DataPower provides hardened real-time protection*

- 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

Access Control Integration Framework (AAA)
Authenticate, Authorize, Audit

WebSphere DataPower
XML Security Gateway XS40

Input Message

Transport Headers
URL
SOAP Method
XPath

Extract Resource

WS-Security
SAML
X.509
Kerberos
Proprietary Tokens

Extract Identity

LDAP
ActiveDirectory
SAML
Tivoli
CA eTrust/Netegrity
RSA
Entrust
Novell
RACF

Authenticate

Map Resource

Map Credentials

LDAP
ActiveDirectory
SAML
Tivoli
CA eTrust/Netegrity
RSA
Entrust
Novell
Proprietary

Authorize

SAML Assertion
Credential Mediation
IDS Integration
Monitoring

Audit & Accounting

Output Message

External Access Control Server or Onboard Identity Management Store

Flexible Message-level Security
Configurable cryptographic actions

- Promote PCI and other confidentiality requirements

- Easily sign, verify, decrypt and decrypt any content

- Configure XML Encryption & XML Digital Signature at:
  - Message-level
  - Part-of-message or field-level
  - Headers, as building block of other security specs

- Verify-all option (data-driven verification of all signatures)

- Secure Attachment Processing:
  - Supports the full SOAP with Attachments specification (MIME/DIME)
  - WS-Security

- Last-mile Security for SOA

Web Application Firewall

WebSphere DataPower
XML Security Gateway XS40

- URL-encoded HTTP application protection in addition to XML Web Services firewall security

- Protection for static or dynamic HTML-based applications

- Supports browser-based clients and HTTP/HTTPS backend servers

- Wizard-driven configuration

- Cross-site scripting and SQL Injection protection

- AAA framework support for web applications

- General name-value criteria boundary profiles for:

  – Query string and form parameters

  – HTTP headers

  – Cookies

- HTML Input Conversion Maps for form processing and handling

- Cookie watermarking (sign and/or encrypt)

- Rate limiting and traffic throttling/shaping

- HTTP header stripping, injection and rewriting

- HTTP protocol and method filtering

- Content-type filtering

- Dynamic routing and load balancing

- Session handling policies

- SSL Acceleration & Termination (Link)

- XML and non-XML processing policies

- Customizable error handling

Integration Appliance XI50
*Purpose-built hardware for Enterprise Service Bus functionality*

- Web Service virtualization for legacy applications

- Enforce high levels of security independent of protocol or payload format

- Integrate with enterprise monitoring systems

- Service level management options to shape traffic
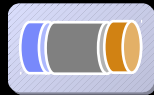
Advanced protocol-bridging seamlessly supports a wide array of transports, including HTTP, WebSphere MQ, WebSphere JMS, Tibco EMS, FTP, NFS, et al.

Any-to-any "DataGlue" engine supports XML and Non-XML (Binary) payloads, promoting asset reuse and enabling integration without coding
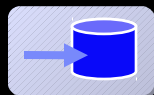
Direct database access enables message-enrichment and data-as-a-service messaging patterns (DB2, Oracle, MS-SQL, Sybase)

High performance architecture creates low-cost, easily-scalable ESB solution for Smart SOA needs

Content-based Routing
Select destination based on transaction metadata

- Dynamically determine route from transaction context and/or message content

  – Analyze originating URL, protocol headers, transaction attributes, etc.

  – Analyze legacy or XML content

- Leverage a routing table for real-time decisions

  – Quickly deploy routing changes, including protocol conversions

- Retrieve routing information from other systems

  – E.g., databases, web servers, file servers, etc.

Unclassified
Requests

Service
Providers
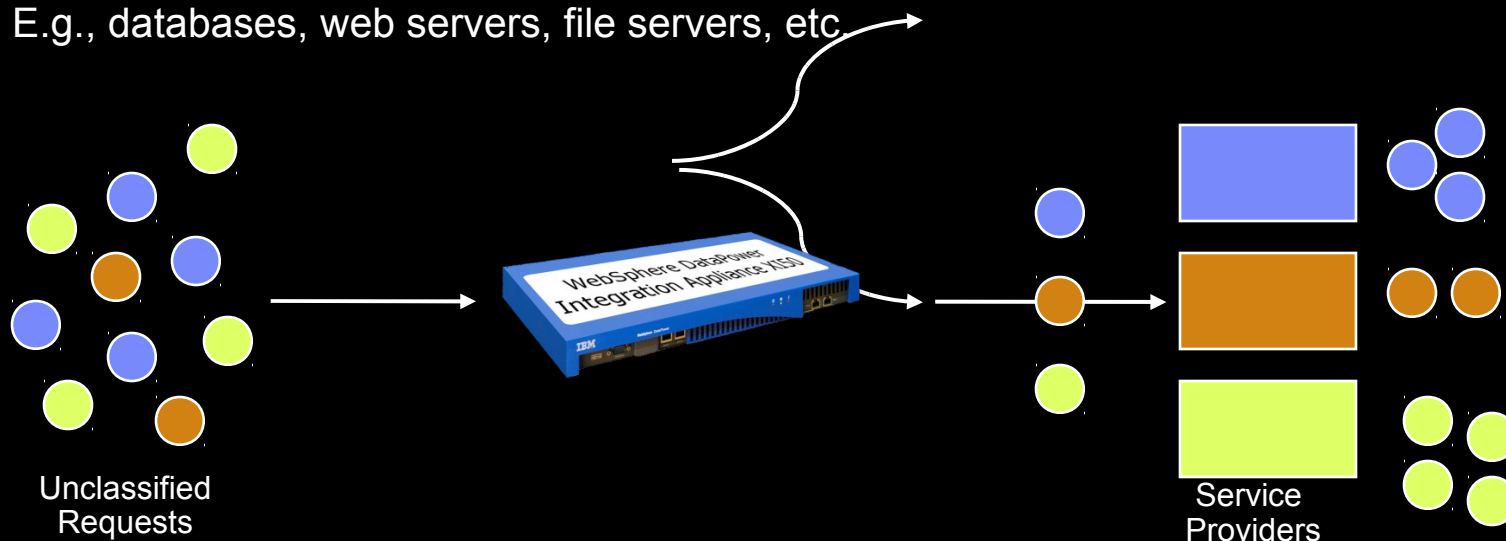
Message Transformation
"DataGlue" processes any-to-any transformations

- Transform between varying data formats (XML, Text, Binary, etc.)

- Use the same WebSphere TX mapping definitions in all IBM ESBs

- Message transformation promotes Smart SOA
  - Exposes data across previously siloed systems
  - Simplifies reuse and connectivity of existing systems
  - Promotes loose coupling

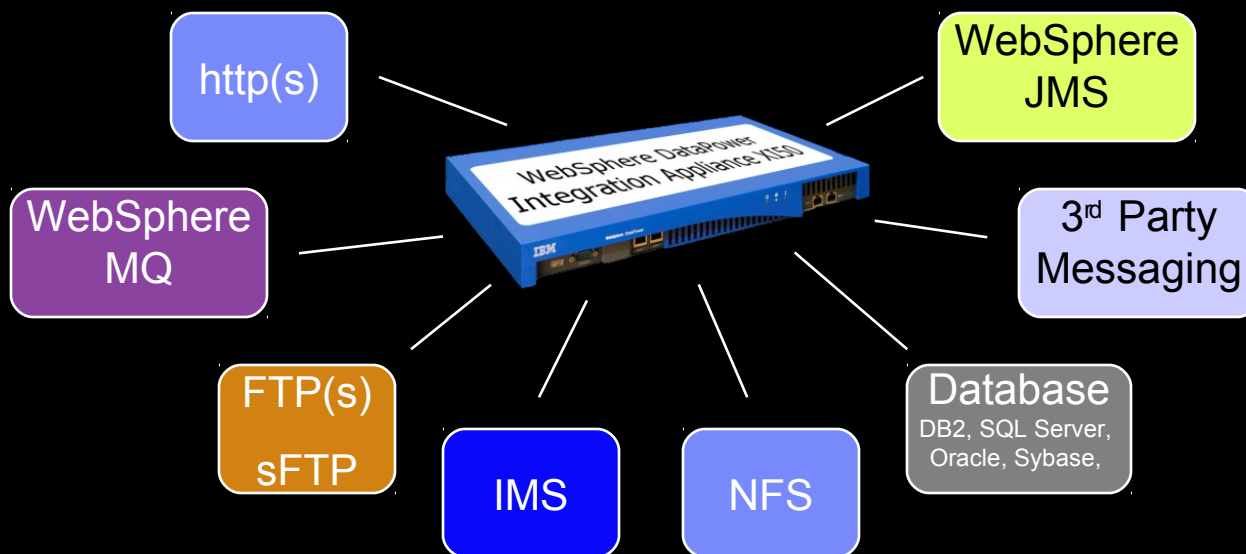- Transformation of data on the wire enables integration without coding

Input Message		Output Message
?	WebSphere DataPower Integration Appliance XI50	**?**
`<XML/>` `TEXT` *binary*		`<XML/>` `TEXT` *binary*

IBM

Protocol Mediation
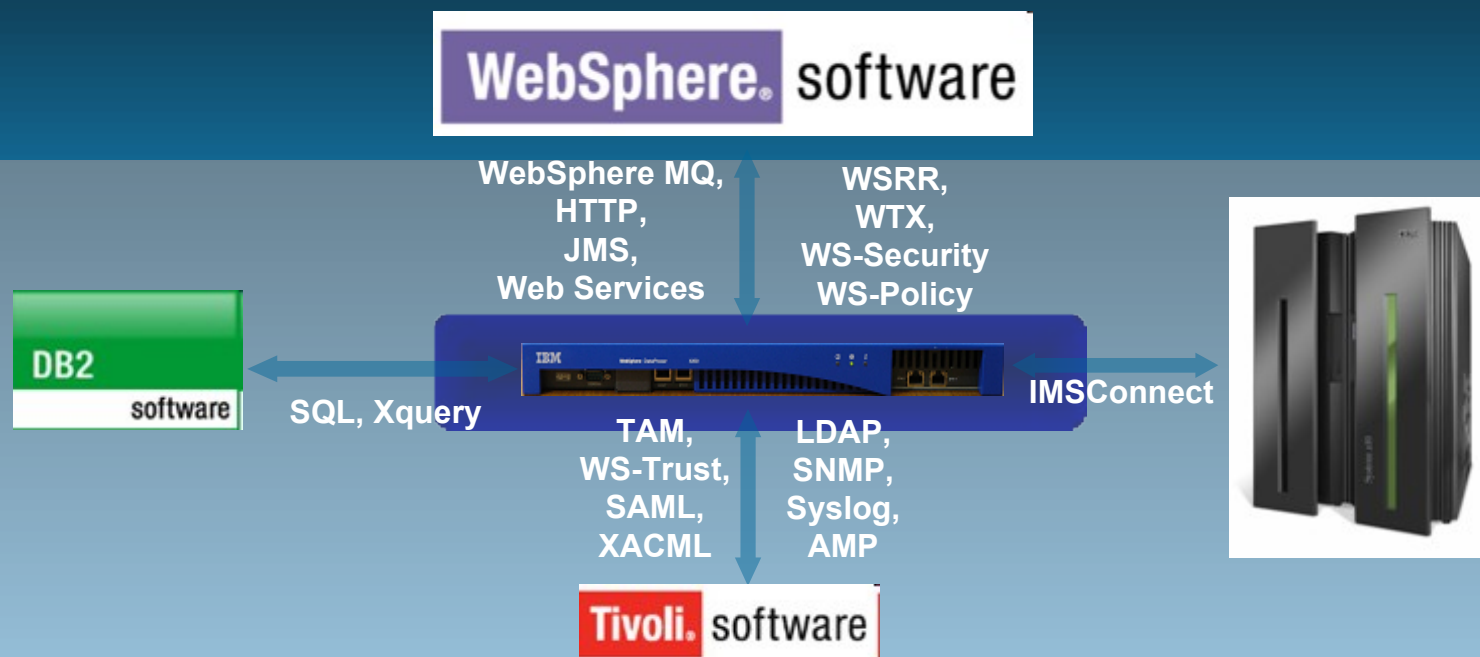## *Independently bridge inbound and outbound protocols*

- First-class support for message and transport protocol bridging

- Protocol mediation with simple configuration:
  - HTTP ←→ MQ ←→ WebSphere JMS ←→ FTP ←→ Tibco EMS

- Request-response and sync-async matching

- Configurable for fully guaranteed, once-and-only-once delivery

http(s)

WebSphere JMS

WebSphere DataPower Integration Appliance XI50

WebSphere MQ

3rd Party Messaging

FTP(s) sFTP

IMS

NFS

Database
DB2, SQL Server, Oracle, Sybase,

**DB2
Oracle
Sybase**

Integration within the IBM Software Portfolio

- **Mature integration within WebSphere software portfolio**
  - *WebSphere MQ with WebSphere DataPower: 4+ years*
  - *Industry-leading SOA Runtime Governance with WSRR + DataPower*
  - *Limitless ESB: Support for WTX for data maps, WS-Security for WMB*
- **Complete SOA Security and Management solution with Tivoli products**
- **Robust enterprise integration through native DB2 and IMSConnect**

WebSphere software

WebSphere MQ, HTTP, JMS, Web Services

WSRR, WTX, WS-Security WS-Policy

DB2 software

SQL, Xquery

IMSConnect

TAM, WS-Trust, SAML, XACML

LDAP, SNMP, Syslog, AMP

Tivoli software

Third Party Integration

- **Standards-based integration with third party vendors**
- **Tight integration with some notable vendors**
- **No platform dependencies – hardware or software**
- **Exceptional interoperability through industry profiles and testing**
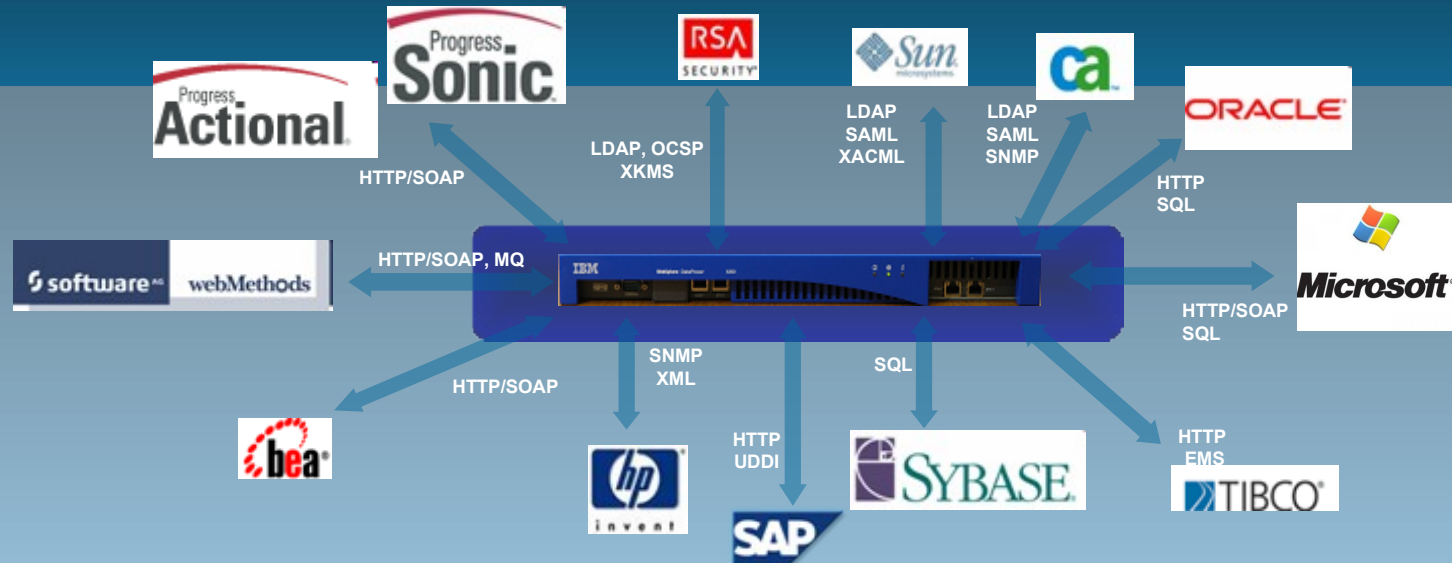
Web Services Management
Service Level Management protects application resources

- Defined as action in the policy pipeline

- Configure policies based on:
  - Any parameter: WSDL; Service Endpoint; Operation; Credential
  - Rate (TPS) or Count by Time (Outlook like Calendar)
  - Request; Response; Fault; XPath

- Enforce same thresholds across a pool of devices

- Configure service level to trigger action:
  - Notify (Alert)
  - Shape (Slow Down)
  - Throttle (Reject)

- Supports WSDM and other Web services management standards

- Allows subscription to SLM for alerts, logging, etc.

- Notify other applications such as billing, audit, etc.

Web Services Management
Service virtualization capabilities for a Smart SOA

- Creates abstraction layer between internal and external Web Services

    - Especially important for auto-generated Web Services

    - Support varying standards support between partners

    - Facilitate new versioning of services

    - Help increase Web Service scalability and availability

- Allows automatic transport-layer conversion (e.g., HTTP external to MQ internal)

- SOAP header injection / stripping / rewriting

- Eases burden of intense XML processing requirements

System z Integration
Smart SOA connectivity throughout the enterprise

- Broad integration with System z
- Connect to existing applications over WebSphere MQ
- Transform XML to/from COBOL Copybook for legacy needs
- Natively communicate with IMS Connect
- Integrate with RACF security from DataPower AAA
- Service enable CICS using WebSphere MQ
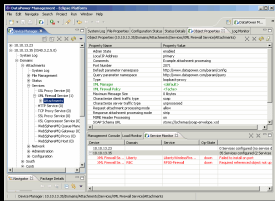- Virtualize CICS Web Services
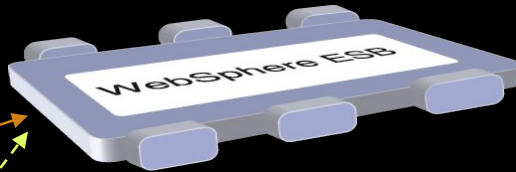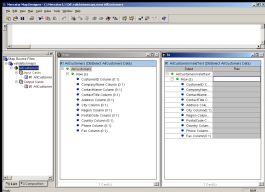
Integrated SOA Tooling Across ESB Runtimes
All 3 ESBs integrate with Eclipse, WTX, ITCAM for SOA and WSRR
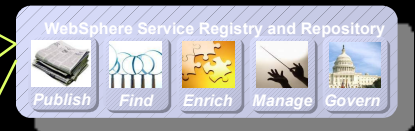
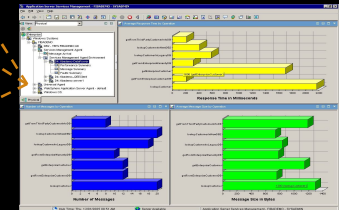

Legacy Mapping Tool:
WebSphere TX

Development Tools:
Eclipse/RAD

SOA Registry:
WSRR

SOA Management:
ITCAM for SOA

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 AS2, AS3 and Web Services
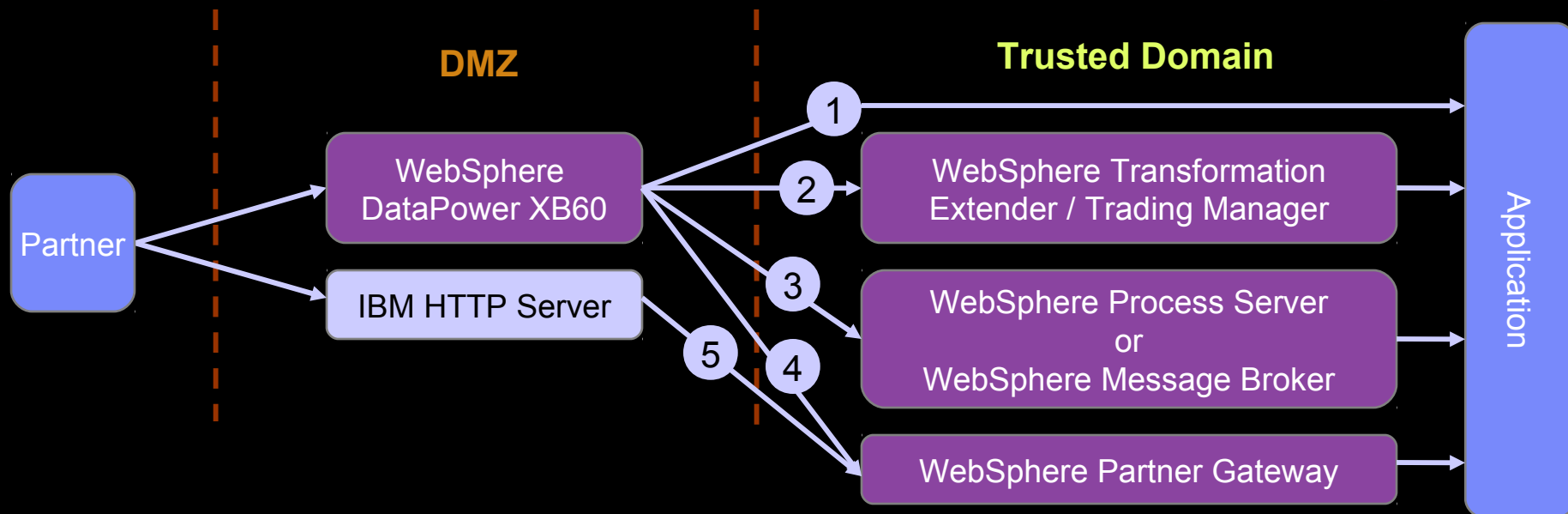
Full featured User Interface for B2B configuration and transaction viewing; correlate documents and acknowledgments displaying all associated events

Simplified deployment, configuration and management providing a quicker time to value by establishing rapid connectivity to trading partners
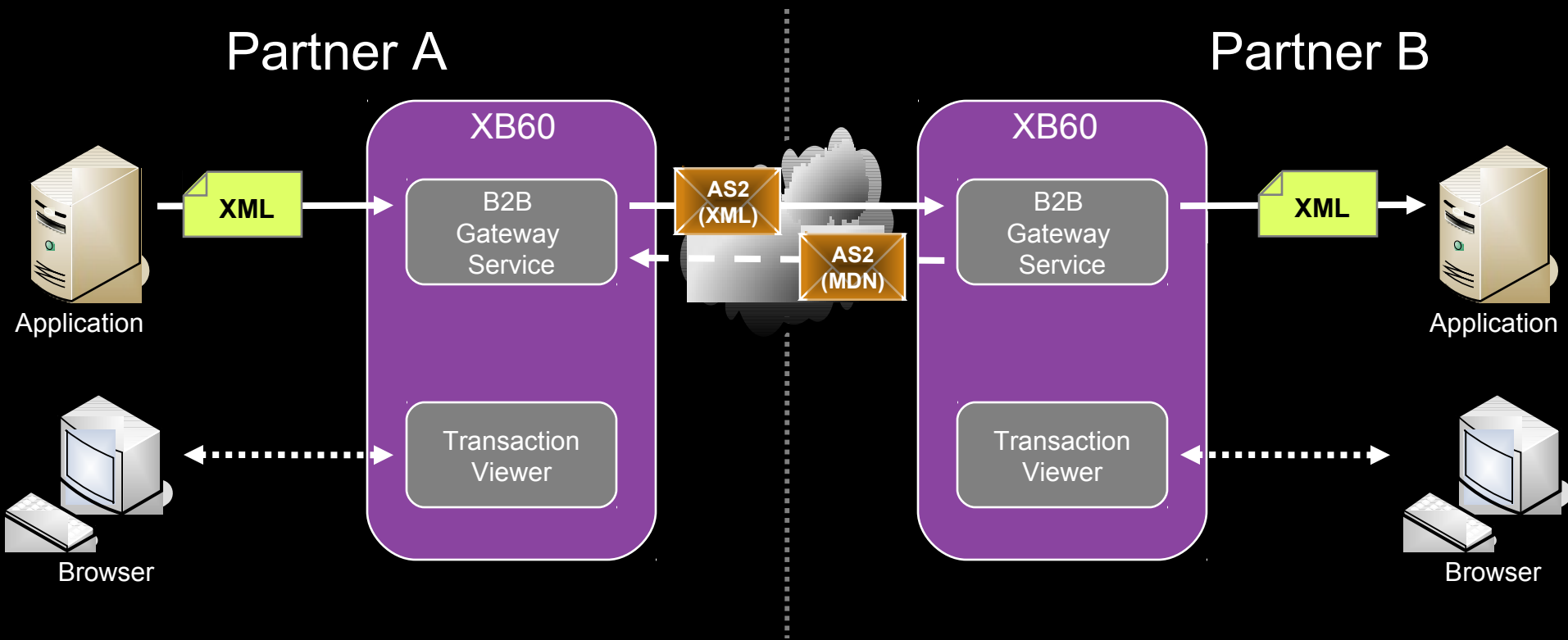
XB60 complements family of B2B solutions

1. Standalone B2B Gateway for secure AS2/AS3 Processing

2. Deploy with WTX-TM for end-to-end EDI Processing

3. Deploy as B2B entry point for BPM and ESB solutions

4. Supplement WPG by offloading security functions and advanced web services

5. WPG provides end-to-end B2B solution

Standard XML over AS2 transaction flow
Use XB60 to securely integrate over AS2 as sender or receiver

WebSphere DataPower
B2B Appliance X650

Partner A

Partner B

XB60

XB60

XML

B2B
Gateway
Service

AS2
(XML)

AS2
(MDN)

B2B
Gateway
Service

XML

Application

Application

Transaction
Viewer

Transaction
Viewer

Browser

Browser

Advanced XML over AS2 transaction flow

Transform payload format using other DataPower services

Partner A

Partner B

XB60

Application

Flat

Multi-Protocol Gateway Service

XML

B2B Gateway Service

AS2 (XML)

AS2 (MDN)

Transaction Viewer

Browser

XB60

Multi-Protocol Gateway Service

Flat

Application

XML

B2B Gateway Service

Transaction Viewer

Browser
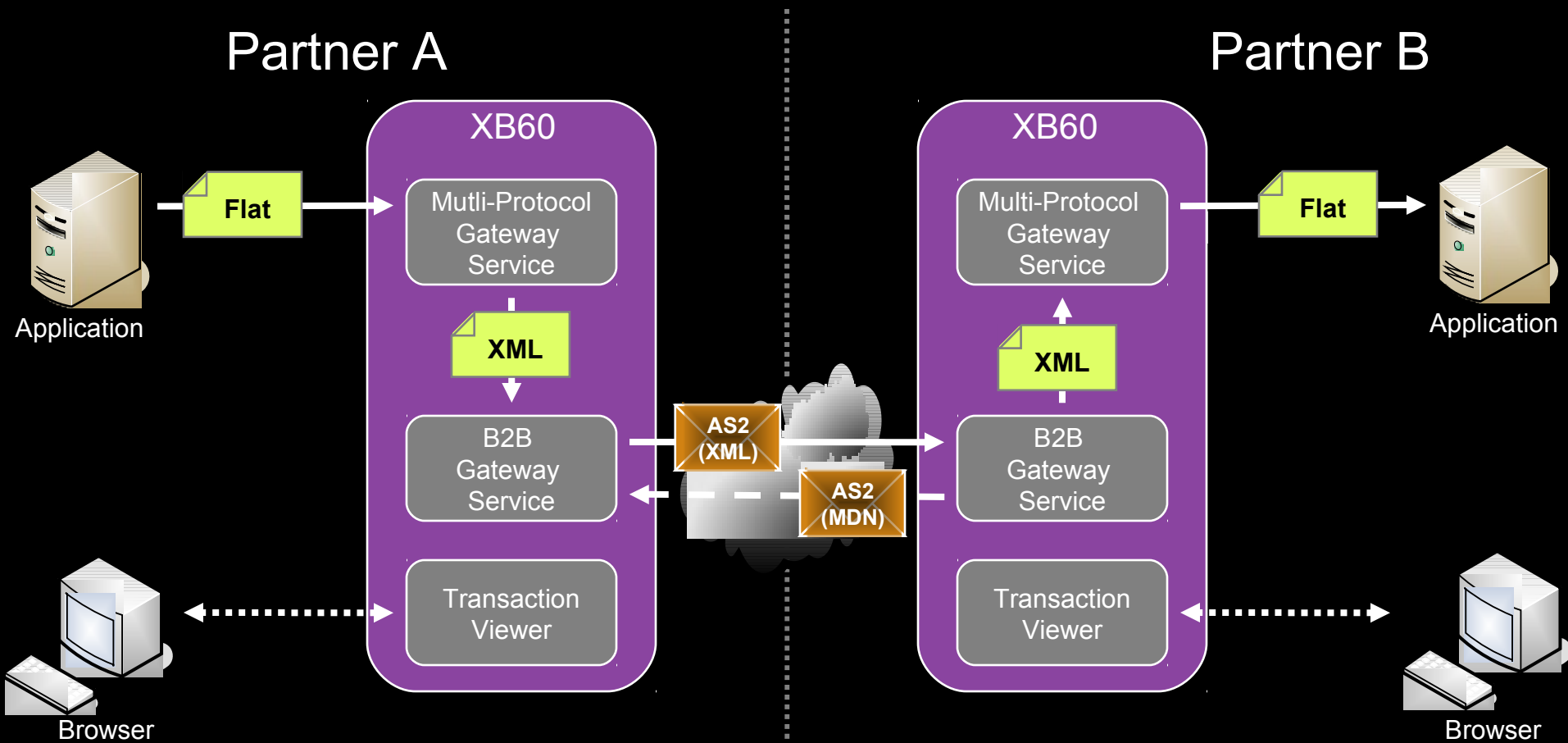
Low Latency Appliance XM70
Purpose-built hardware for low-latency, network-based messaging and data feed processing

- Drop-in messaging solution plugs into existing network infrastructure

- Enhanced QoS and performance

- Simplified, configuration-driven approach to low-latency, publish/subscribe messaging

- Native high availability with multiple 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 MQ LLM Technology

- Low Latency and High Throughput
  - Publishes up to 8 million, 12-byte messages per second on Gigabit Ethernet
  - Averages 60μs latency at typical market data rates on Gigabit Ethernet
- Support for both Multicast and Unicast modes
  - Reliable UDP Multicast (RMM)
  - Reliable UDP Unicast (Point to point RMM)
  - Reliable TCP Unicast (RUM)
- Zero or minimal messages lost due to transient network or application failure
- Automated state synchronization and stream failover for high availability
  - Simplified component replication with total order and state synchronization facilities
  - Zero messages lost during failover at high rates
- Fine-grained message filtering with message selection
  - Allows for millions of logical message flows and JMS-style message selection
- APIs to monitor statistics and performance
  - Provides visibility into the status of the network, senders and receivers
- Automatic congestion and traffic rate control
- Client software runs on a large number of platforms
  - Windows (32, 64), Linux (32, 64), Solaris (Sparc, x86, 32, 64)
  - C, Java, and .NET APIs

Multiple WebSphere MQ Low Latency APIs

- **Reliable Multicast using UDP**
 - Highly scalable, topic-oriented communication
  - Supports PGM specification.
  - NAK reliability
  - Sliding history window
  - Congestion management
- **Reliable Unicast using UDP**
  - Efficient point-to-point, topic-oriented communication.
  - Higher reliability similar to that of TCP
  - ACK reliability
  - Periodic heartbeat ensures liveness
- **Reliable Unicast Messaging**
  - High throughput, topic-oriented communication using TCP
  - Simpler than TCP streaming primitives
  - Periodic heartbeat ensures liveness
  - Can be used in WAN or through firewall
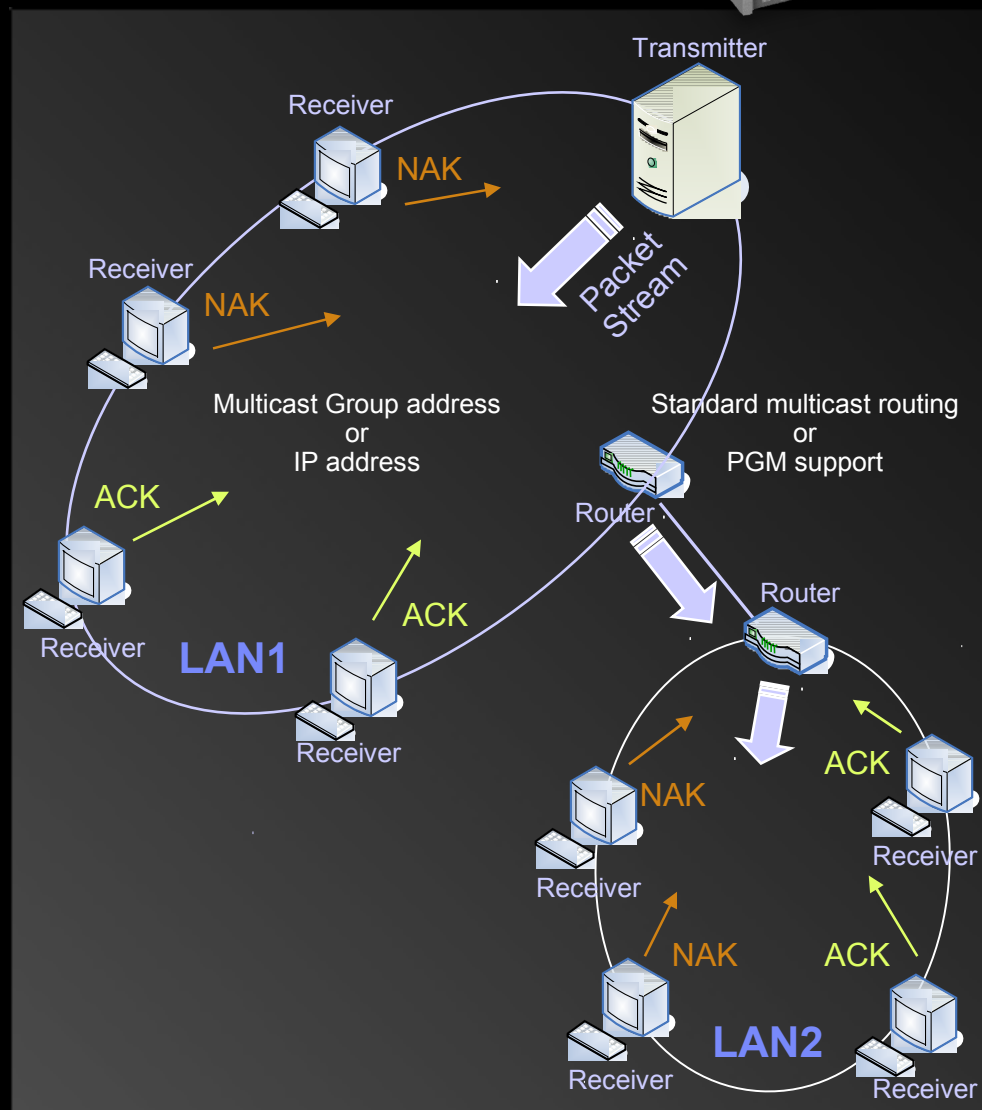
WebSphere MQ LLM in a DataPower SOA Appliance
Benefits of bridging and transformation with high availability

- High-speed content-based routing
  - FIX over MQ LLM transport
  - XML over MQ LLM transport
- Protocol bridging
  - MQ LLM, MQ,Tibco EMS, WebSphere JMS, HTTP, Tibco RV (future)
- Any-to-any data transformation
  - Uses Multi-Step pipeline for full feature processing
  - Incurs latency penalty as message travels outside "fast-path"
- Web Services Gateway functions
- Congestion management
- Total message ordering across devices
- Load distribution across devices for workload management
  - Protocol level load distribution
  - Configuration and deployment-driven best practices
- Fault tolerant stream failover configuration with multiple devices
- Message persistence for failover, replay, and late join

Configuration & Administration
Fits into existing environments

- Depth of functionality to scale to full operational complexity

- Multiple administration consoles
    - WebGUI – 100% availability of functions in all consoles
    - CLI – Familiar to network operators
    - SOAP interface – Programmatic access to all config for easy scripting

- IDE integration
    - Eclipse/Rational Application Developer
    - Altova XML Spy

- WAS 7 Admin Console for Multi-box Management

- Easy export/import for configuration promotion

- Standard operational interfaces
    - SNMP, syslog, etc.

- *Industry leading integration support across IBM and 3rd party application, security, identity management, and networking infrastructure*

Summary – IBM Specialized Hardware for Smart SOA Connectivity

- Hardened, specialized product for helping integrate, secure & accelerate SOA

- Many functions integrated into a single device

- Broad integration with both non-IBM and IBM software

- Higher levels of security assurance certifications require hardware

- Higher performance with hardware acceleration

- Simplified deployment and ongoing management

www.ibm.com/software/integration/datapower

SOA Appliances: Creating customer value through extreme SOA performance, connectivity, and security

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