IBM SECURITY TRENDS SEMINAR 2012

FORTIFY YOUR COMPANY
AGAINST INTERNAL AND EXTERNAL THREATS

Secure your SOA, B2B and Cloud Environments with WebSphere DataPower Appliances

Sid Antflick

WebSphere Sales Leader - Connectivity Appliances, IBM Australia

IBM SECURITY SOLUTIONS
RISK MITIGATION. PROTECTION. COMPLIANCE.

Agenda

What is a DataPower Appliance?

Securing Application Connection

Models and Features

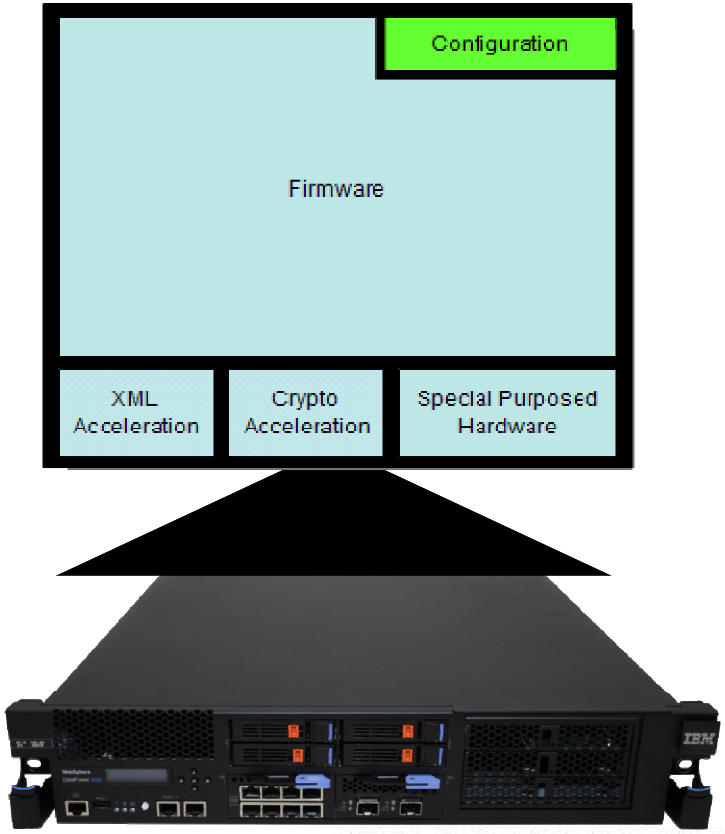
Appliance Management

Agenda

- What is a DataPower Appliance?
- Secure Application Connection
- Models and Features
- Appliance Management

The IBM WebSphere DataPower organization makes appliances

- **Simple architecture**:
  - microcode firmware + purpose-built hardware
- Delivered from the factory with everything you need to connect to the network and start working
  - No need to provision anything but the Ethernet network and CAT cables to get started
- All computationally-significant components sealed within **a tamper-proof casing**
  - Chips
  - Memory
  - Boards and cards
  - Flash-based file system (signed and encrypted)
  - Parsing and xform accelerators (patented)
  - Cryptographic accelerators (patented)



Configuration

Firmware

XML Acceleration

Crypto Acceleration

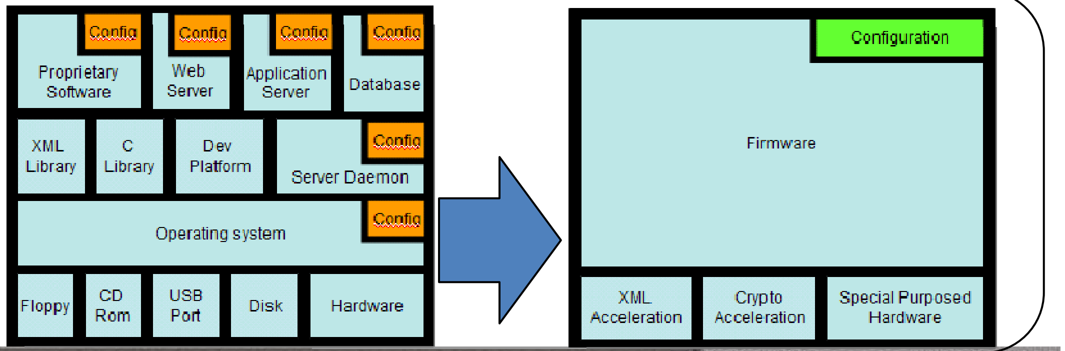
Special Purposed Hardware

But simple does NOT mean lacking in functionality

- DataPower appliances have been the best selling WebSphere product since the DataPower company acquisition in 2005
- Guiding philosophy is to take rote, **repeatable integration tasks and lock them down** in the appliance form factor, including:
  - *Services gateway functions*
  - *Service Bus (ESB) functions*
  - *B2B gateway functions*
  - *Edge optimization functions*
  - *Web application gateway functions*

Appliance "lock down" means:

- Removing need for commodity code
- Removing reliance on general purpose operating systems and run times
- Porting to purpose-built firmware
- **Simplicity = BIG TCO SAVINGS**


Config
Proprietary Software
Config
Web Server
Config
Application Server
Config
Database
XML Library
C Library
Dev Platform
Config
Server Daemon
Config
Operating system
Floppy
CD Rom
USB Port
Disk
Hardware

Configuration
Firmware
XML Acceleration
Crypto Acceleration
Special Purposed Hardware

Agenda

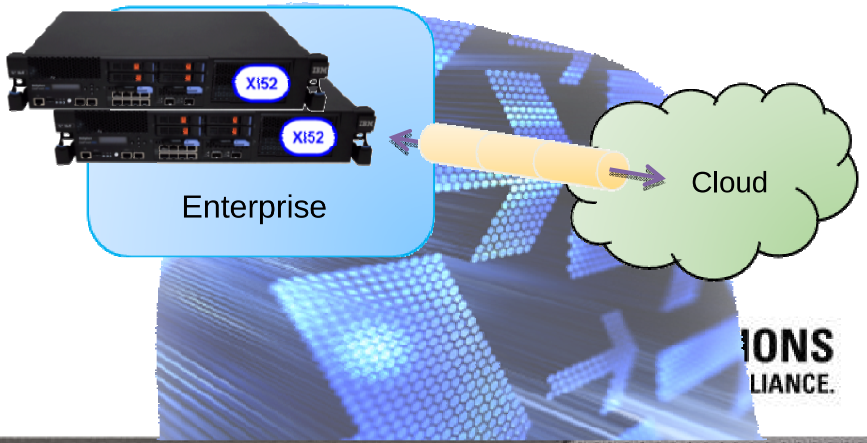
What is a DataPower Appliance?

Models and Features

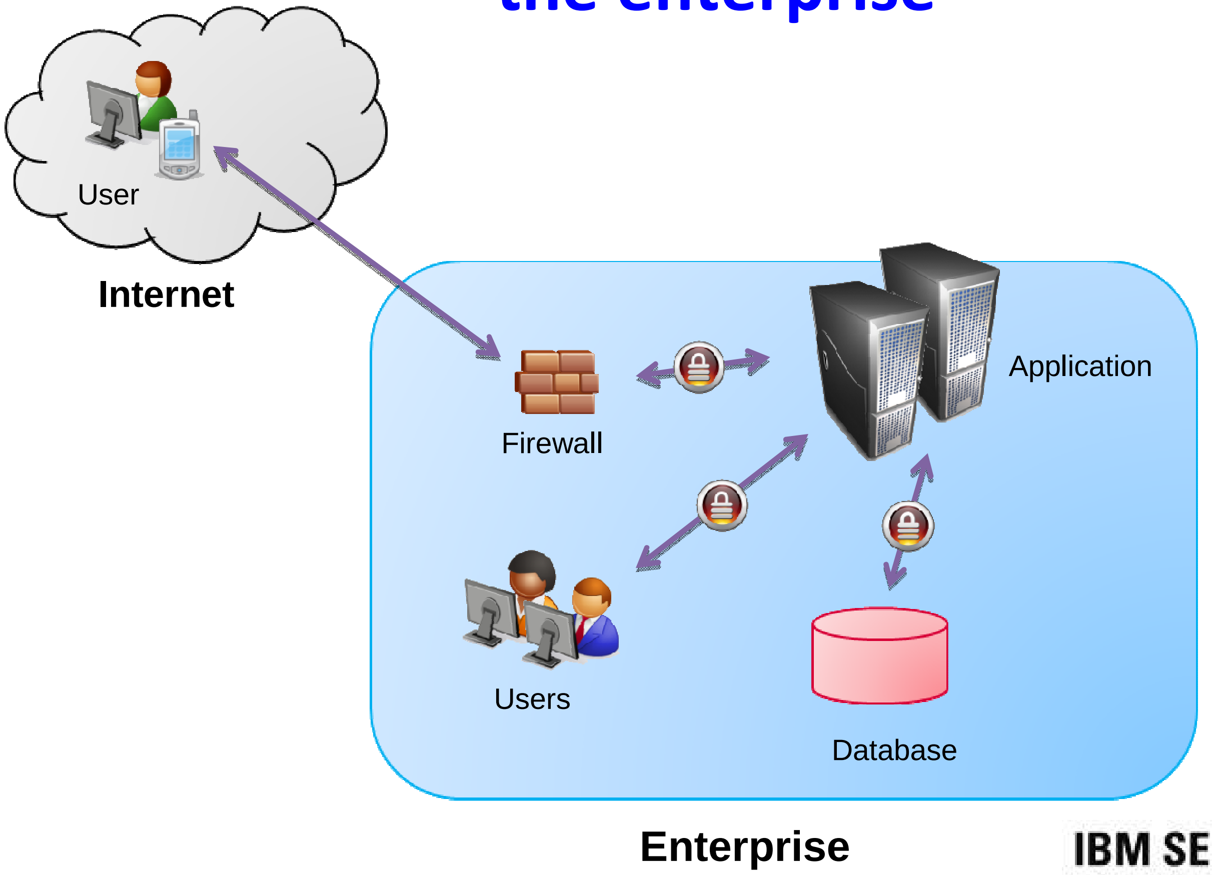
Appliance Management

Requirement - Secure the Cloud and B2B Connections

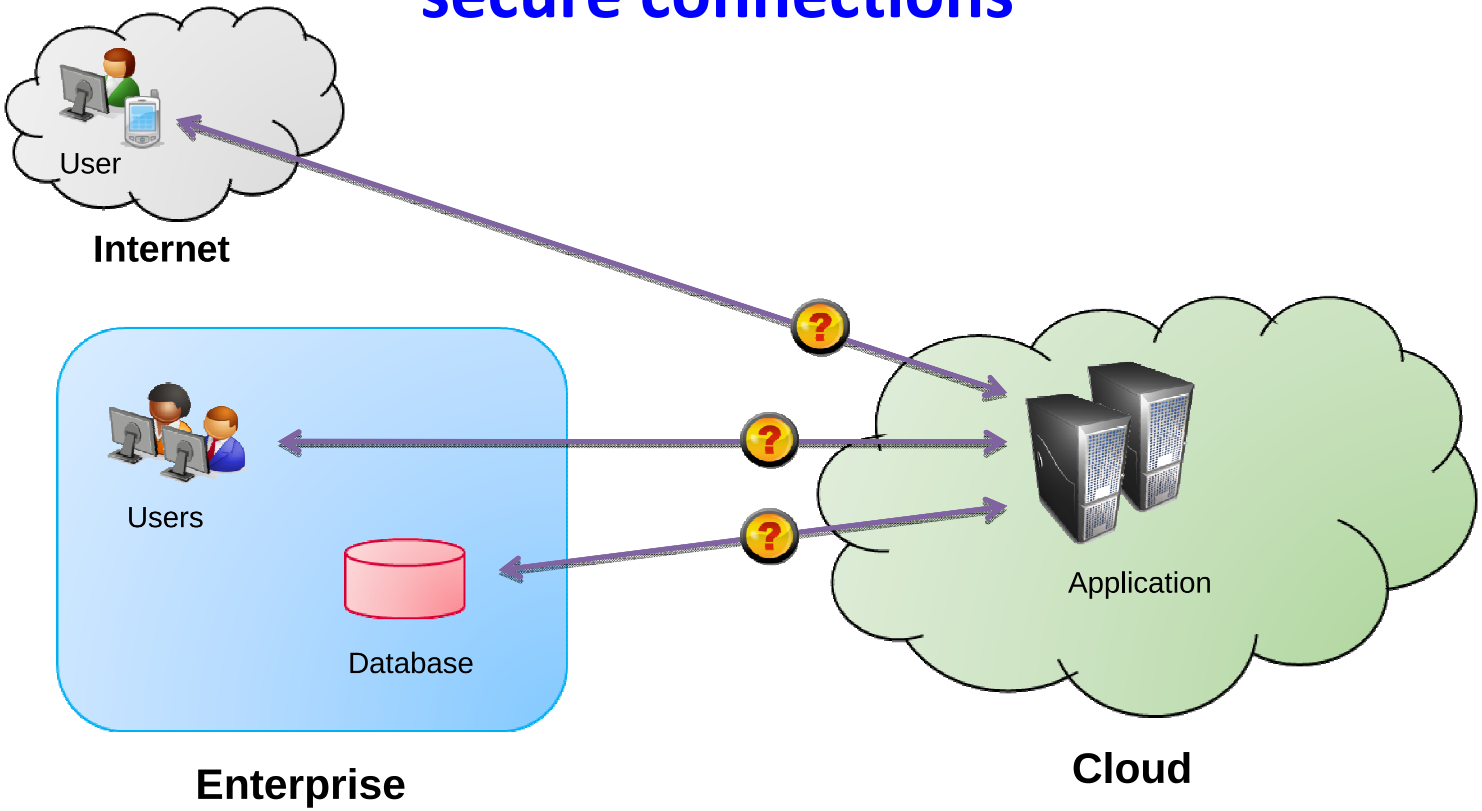
- Create a **secure channel** between the enterprise and the cloud
- Leverage **standard protocols** portable to any cloud provider
- Facilitate **self service** for establishing new connections
- Provides multiple layers of connection security:
  - Custom **authentication**
  - Resource-specific **authorization**
  - Transport-layer **encryption**
  - Connection **auditing**



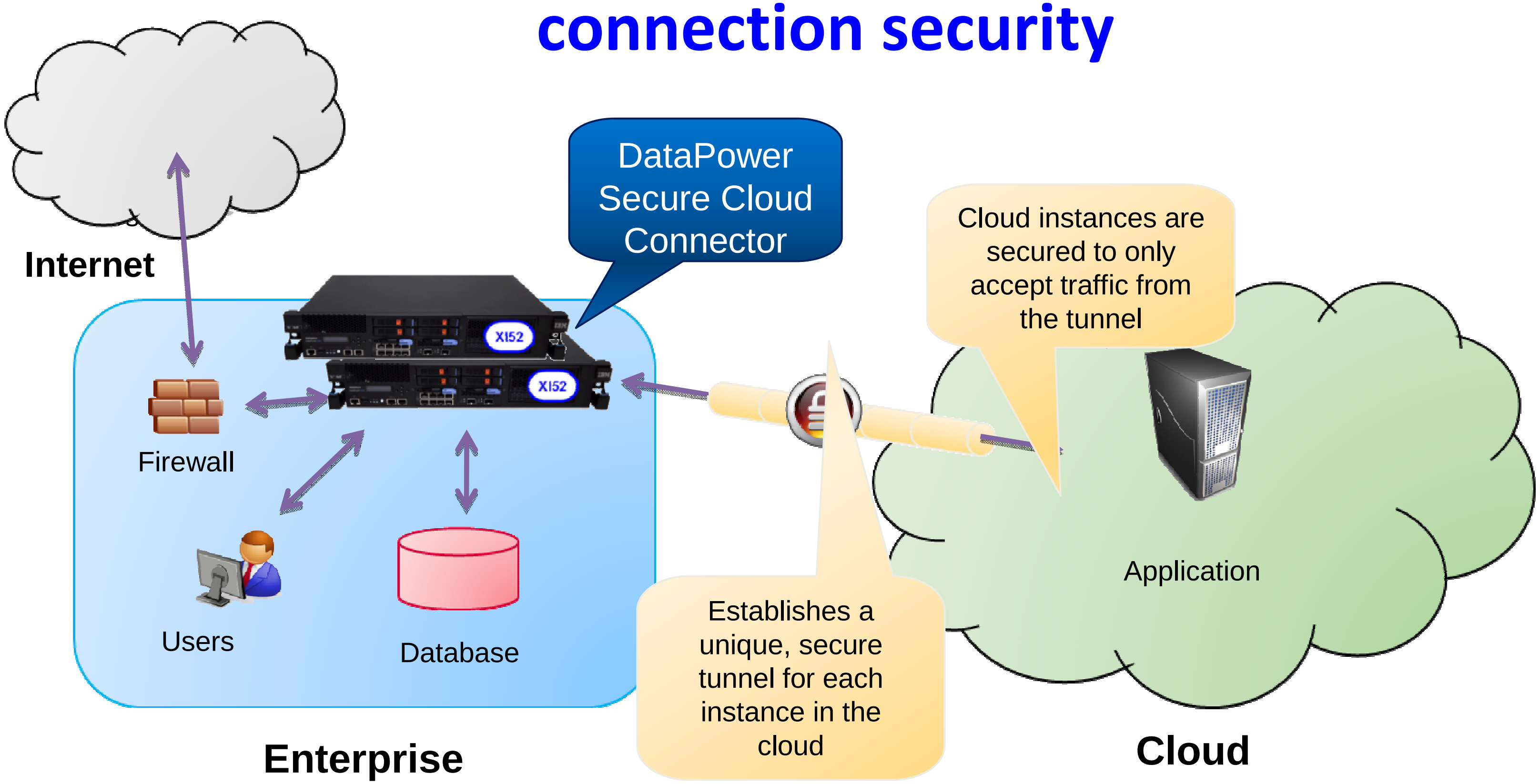
Traditional applications control connection security within the enterprise

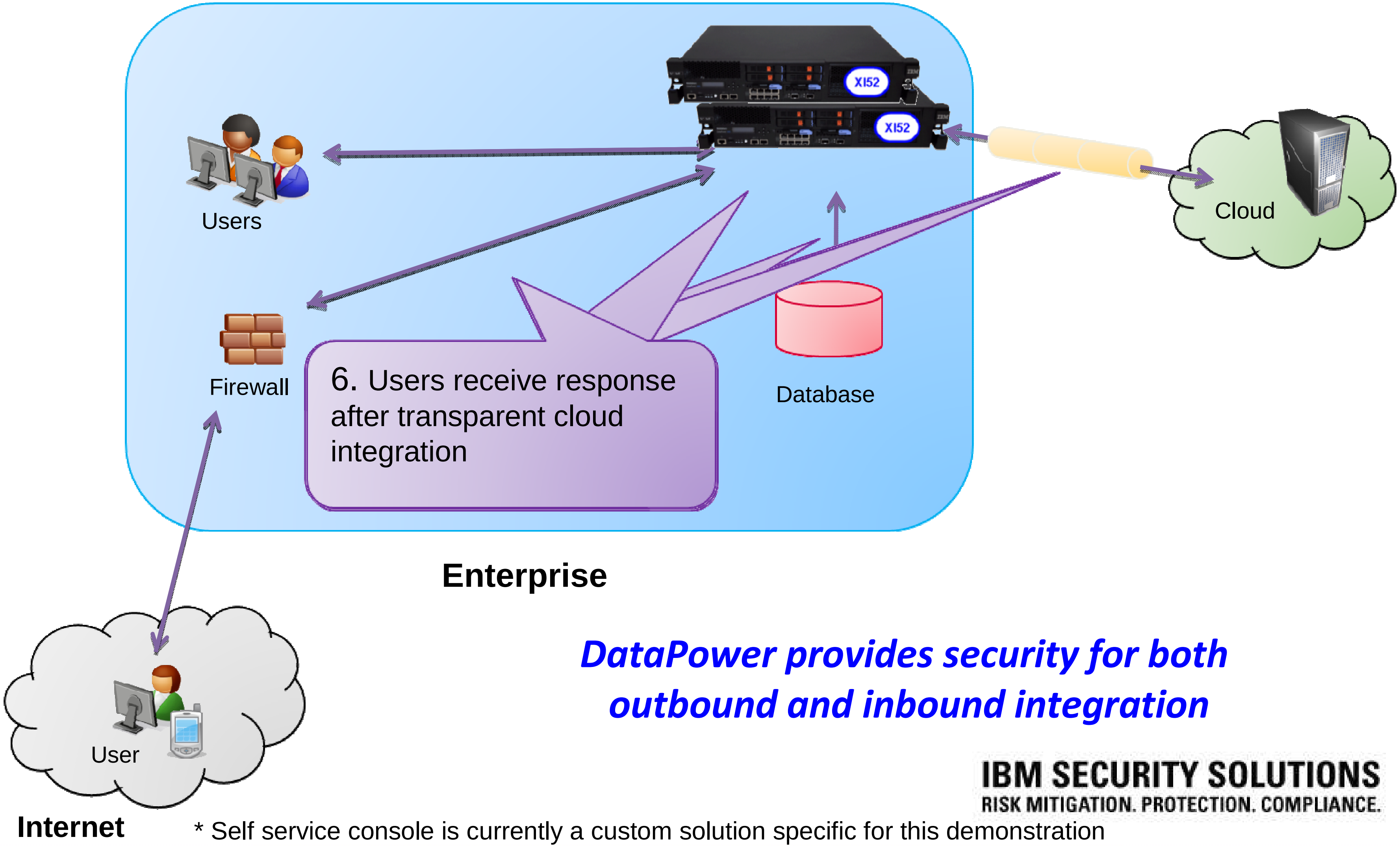


Moving applications to the cloud exposes previously secure connections



DataPower Secure Cloud Connector restores your connection security


Internet
DataPower Secure Cloud Connector
XI52
XI52
Firewall
Users
Database
Enterprise
Cloud instances are secured to only accept traffic from the tunnel
Establishes a unique, secure tunnel for each instance in the cloud
Application
Cloud



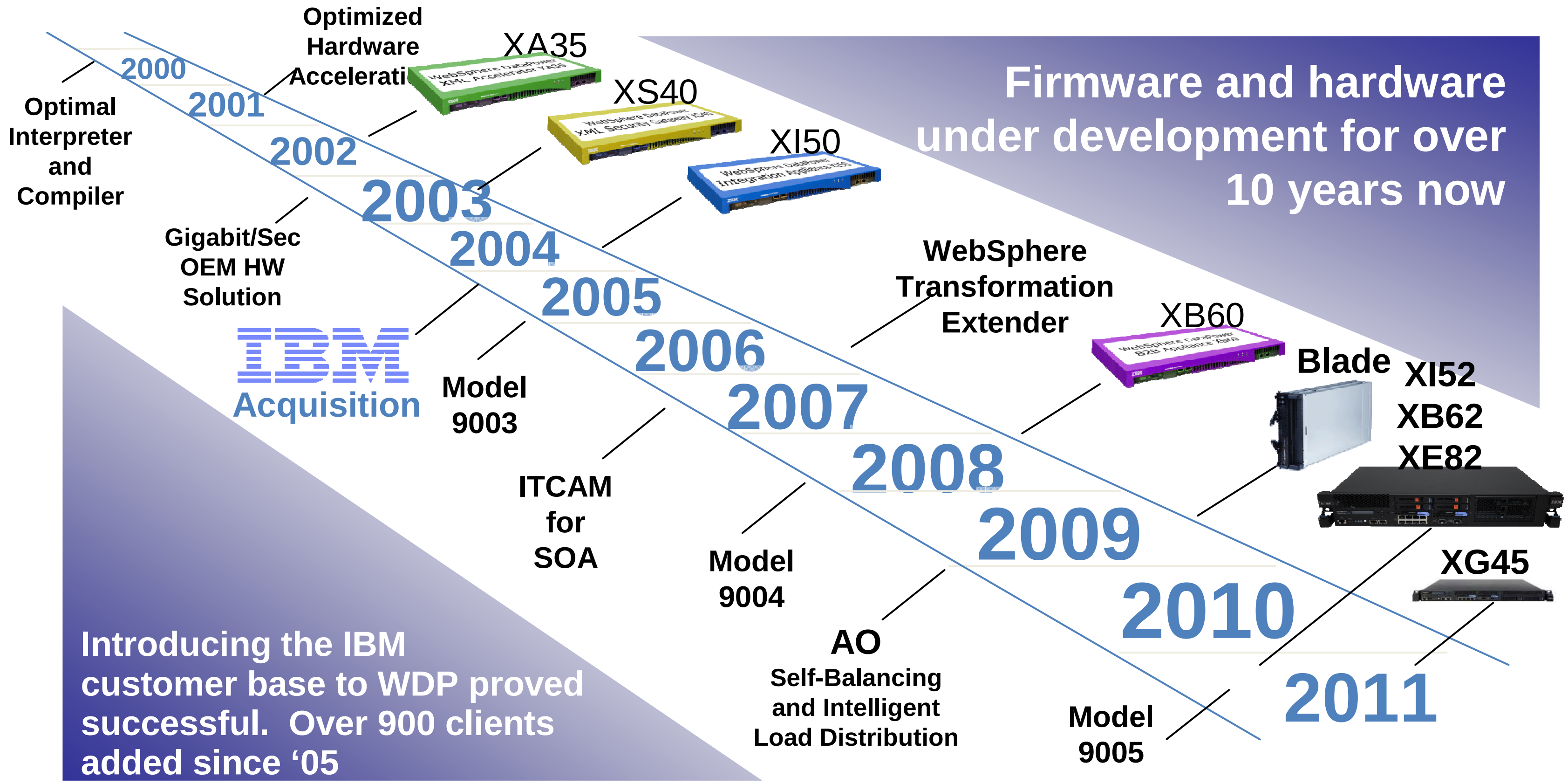
6. Users receive response after transparent cloud integration

DataPower provides security for both outbound and inbound integration

IBM SECURITY SOLUTIONS
RISK MITIGATION. PROTECTION. COMPLIANCE.

* Self service console is currently a custom solution specific for this demonstration

DataPower Boasts a Decade of Connectivity Innovation



Firmware and hardware under development for over 10 years now

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011

Optimal Interpreter and Compiler

Optimized Hardware Accelerati

XA35

XS40

XI50

Gigabit/Sec OEM HW Solution

IBM Acquisition

Model 9003

ITCAM for SOA

Model 9004

WebSphere Transformation Extender

XB60

AO Self-Balancing and Intelligent Load Distribution

Blade

XI52 XB62 XE82

XG45

Model 9005

Introducing the IBM customer base to WDP proved successful. Over 900 clients added since ‘05

Close to 1,000 worldwide installations and growing fast

Government

- Agencies and ministries
- Defense and security organizations
- Crown corporations

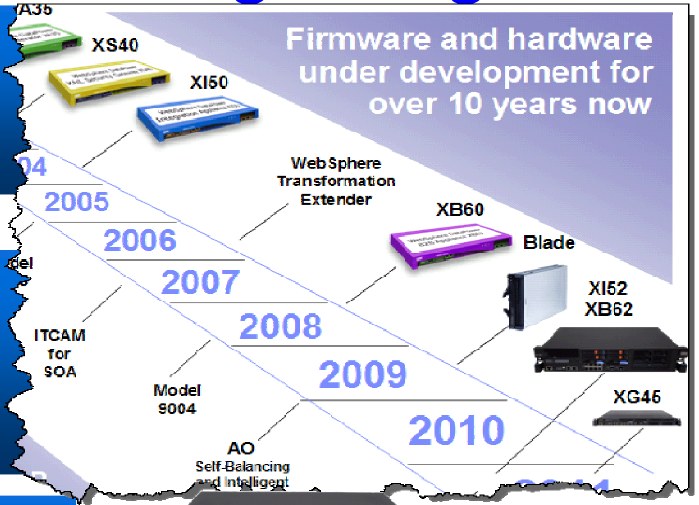
Banking

- All of the big 5 Canadian banks
- Numerous regional banks and credit unions
- SaaS providers, ASPs, regulators, etc.

Insurance

- Used by 95% of top global insurances firms
- SaaS providers, ASPs, regulators, etc.

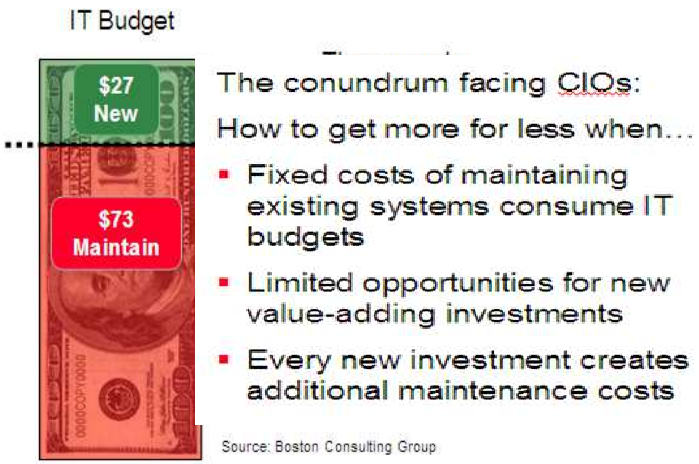
Many, many, more



Firmware and hardware under development for over 10 years now

IBM SECURITY SOLUTIONS
RISK MITIGATION. PROTECTION. COMPLIANCE.

DataPower appliances offer a classic SOA business case

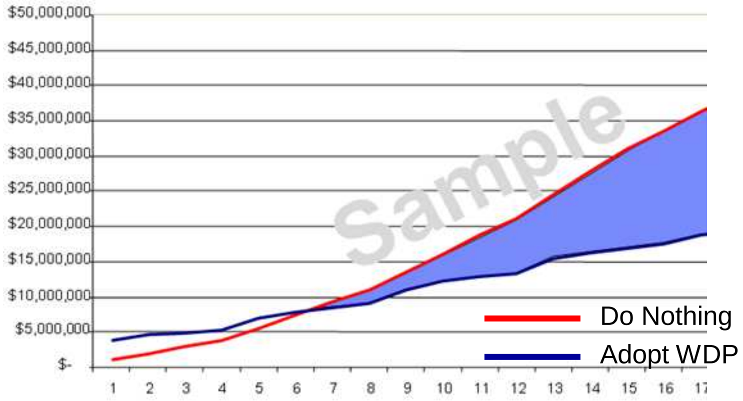


The conundrum facing CIOs:

How to get more for less when…

- Fixed costs of maintaining existing systems consume IT budgets
- Limited opportunities for new value-adding investments
- Every new investment creates additional maintenance costs

Source: Boston Consulting Group



- **Returns are typically found by:**
  - *Accelerating project timelines* (and beginning to realize new revenues earlier)
    - Drop-in deployment, even to sensitive networks
    - Configuration of tasks that would otherwise be coded
  - *Reduction of project resource requirements*
    - Configuration of tasks that would otherwise be coded
    - No tuning required for performance
  - *Reduction of existing server footprint or deferment of the need to scale up*
    - Offloading of resource-intensive functions to a platform purpose-built to do them at low resource penalties
  - *Lowering ongoing operations costs*
    - Simple architecture and low-touch maintenance model
    - Centralization of rote, repeatable integration tasks

Agenda

What is a DataPower Appliance?

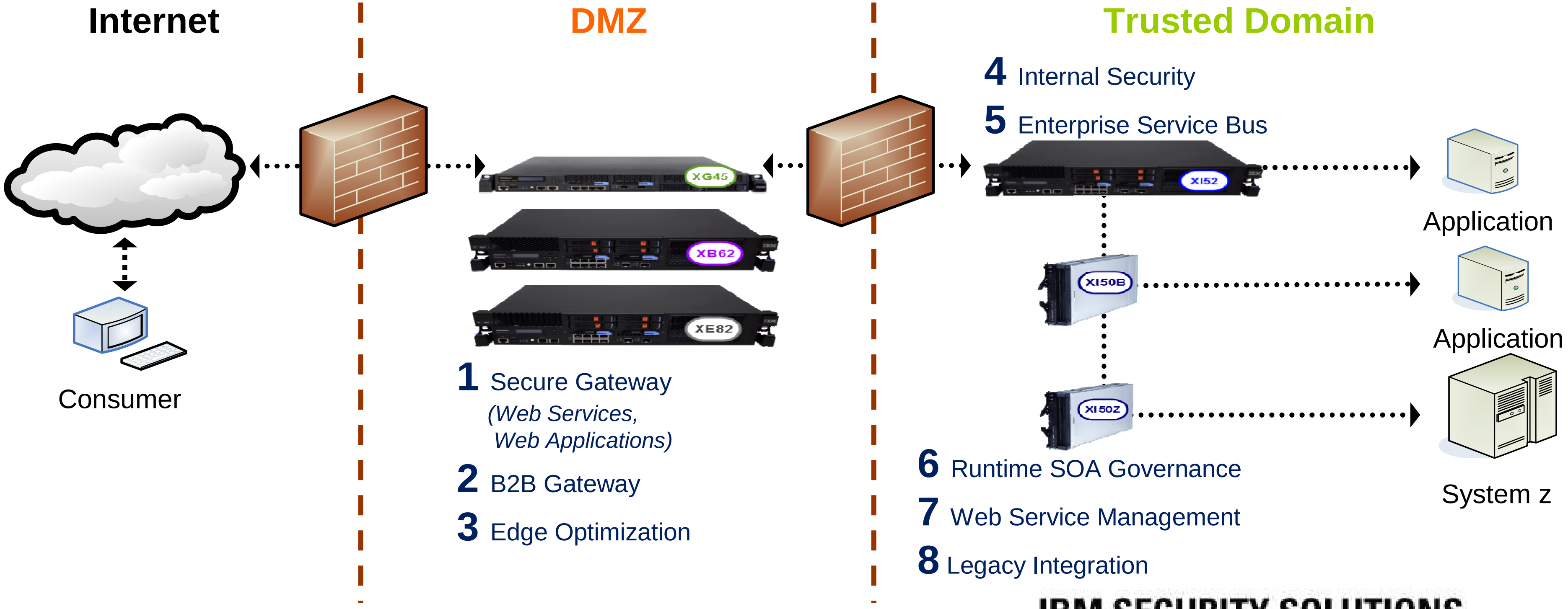
Secure Application Connection

Appliance Management

IBM SECURITY TRENDS SEMINAR 2012

FORTIFY YOUR COMPANY AGAINST INTERNAL AND EXTERNAL THREATS

Deploy WebSphere DataPower Appliances in a variety of use cases



1 Secure Gateway *(Web Services, Web Applications)*

2 B2B Gateway

3 Edge Optimization

4 Internal Security

5 Enterprise Service Bus

6 Runtime SOA Governance

7 Web Service Management

8 Legacy Integration

IBM SECURITY SOLUTIONS
RISK MITIGATION. PROTECTION. COMPLIANCE.

IBM SECURITY TRENDS SEMINAR 2012

FORTIFY YOUR COMPANY AGAINST INTERNAL AND EXTERNAL THREATS

XML Security Gateway XG45
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.

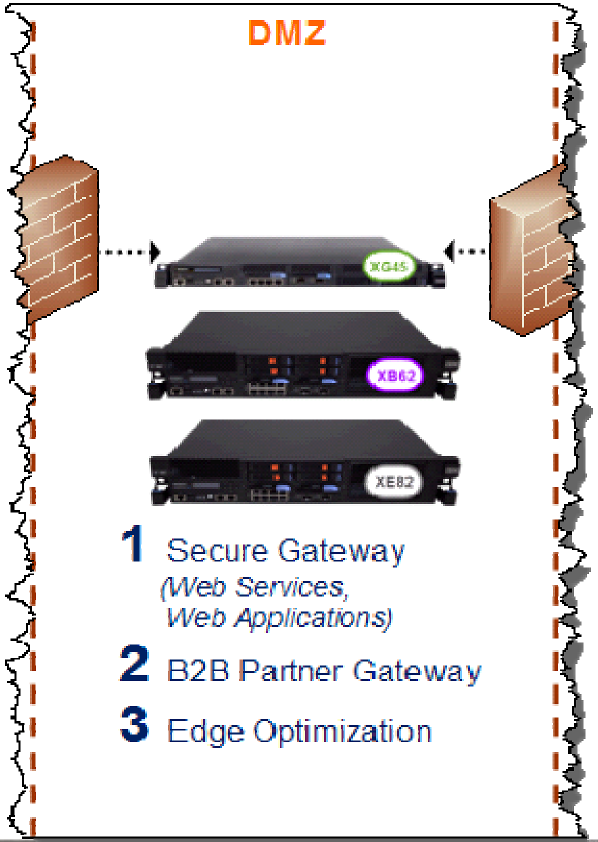
Provides field-level XML security through encryption/decryption and signing/verification of entire messages or individual XML fields.

Supports a variety of access control mechanisms, and can control access by rejecting unsigned messages and verifying signatures within SAML assertions.

IBM SECURITY SOLUTIONS
RISK MITIGATION. PROTECTION. COMPLIANCE.

The devices are ideal for deployment to less-than-fully-trusted networks

- Tamper-proof casing
- Default-off delivery from factory
- Signed and encrypted file system
- Optional Hardware Security Module (HSM)
- Certifications:
  - Common Criteria EAL 4
  - FIPS 140-2 Level 3

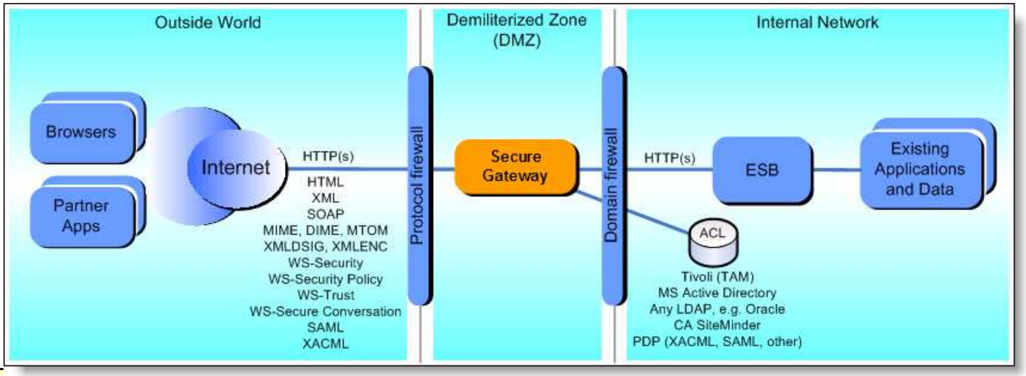


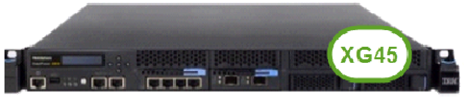
1 Secure Gateway (Web Services, Web Applications)

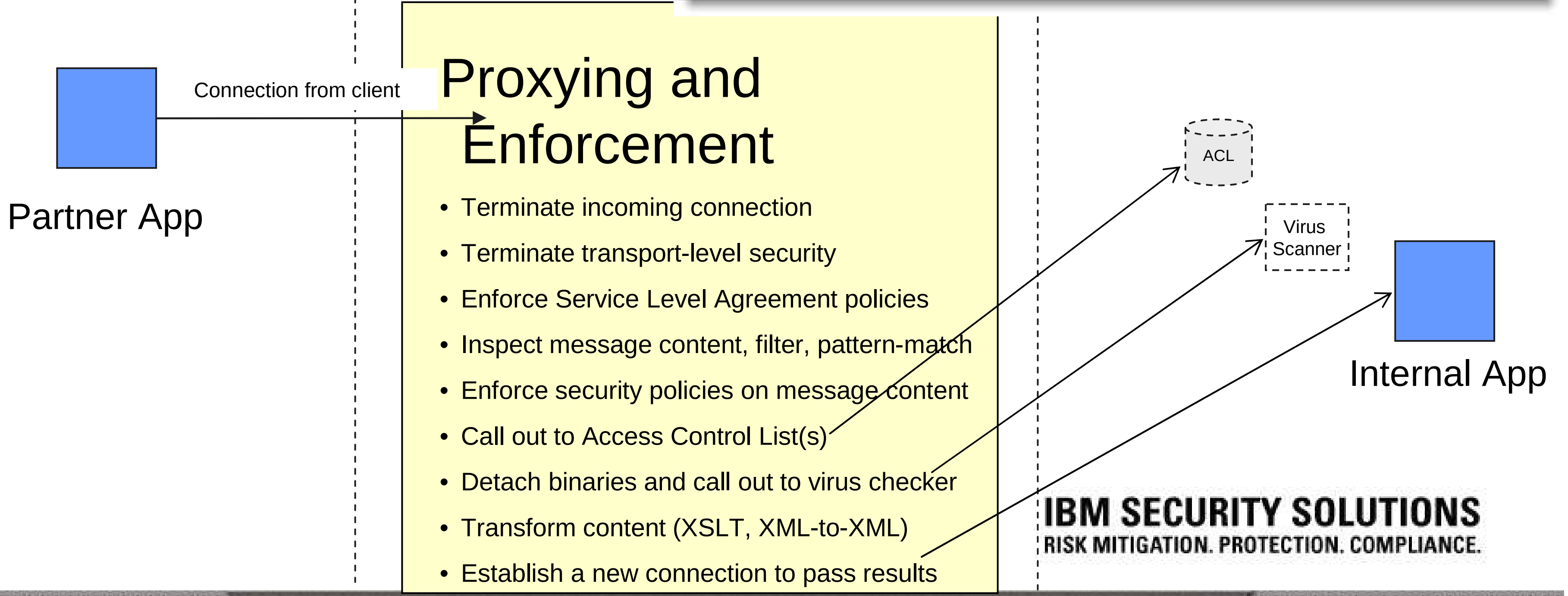
2 B2B Partner Gateway

3 Edge Optimization

Secure Gateway





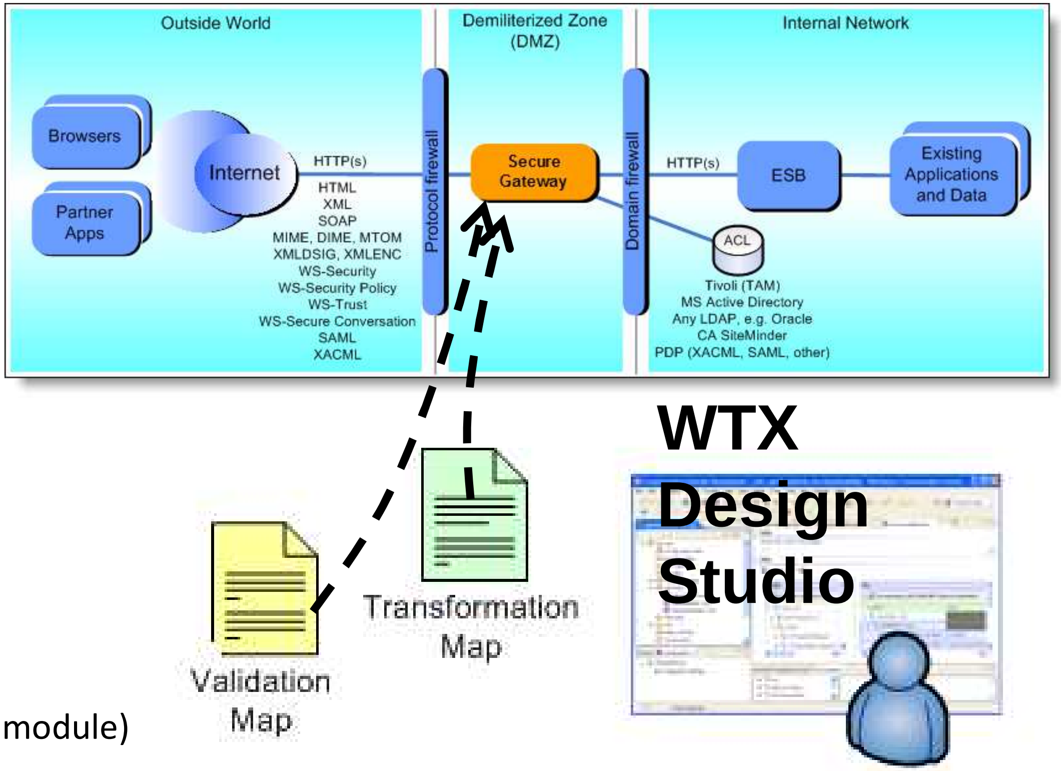


Proxying and Enforcement

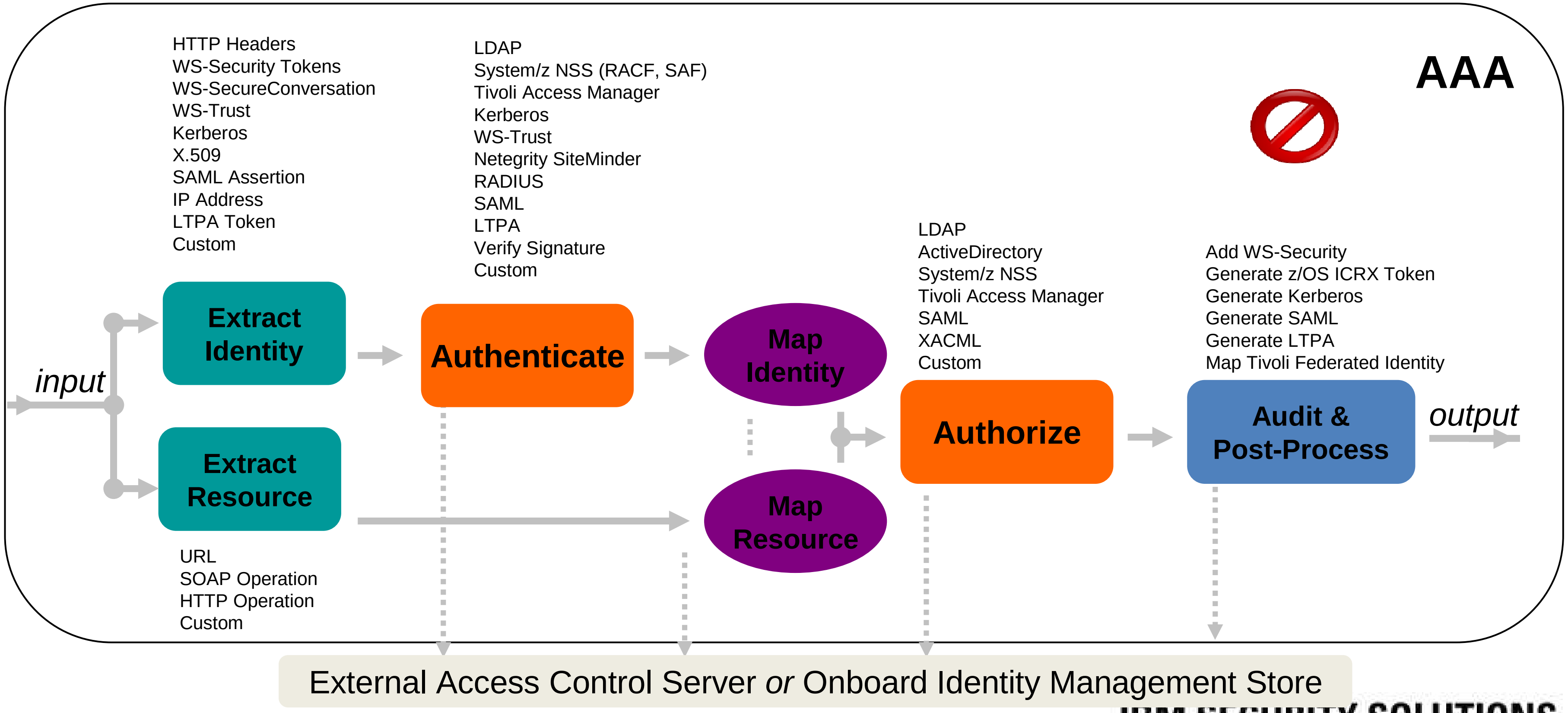
- Terminate incoming connection
- Terminate transport-level security
- Enforce Service Level Agreement policies
- Inspect message content, filter, pattern-match
- Enforce security policies on message content
- Call out to Access Control List(s)
- Detach binaries and call out to virus checker
- Transform content (XSLT, XML-to-XML)
- Establish a new connection to pass results

Secure Gateway

- Entry-level form factor
- Protocols Supported
  - HTTP(s)
  - WebSphere MQ
  - WebSphere JMS
  - FTP(s)
- Formats Supported
  - XML
  - SOAP
  - JSON
  - PKCS7 (with optional Data Integration module)
- Transformation engines supported
  - XSLT
  - DataGlue - WTX/FFD (with optional Data Integration module)

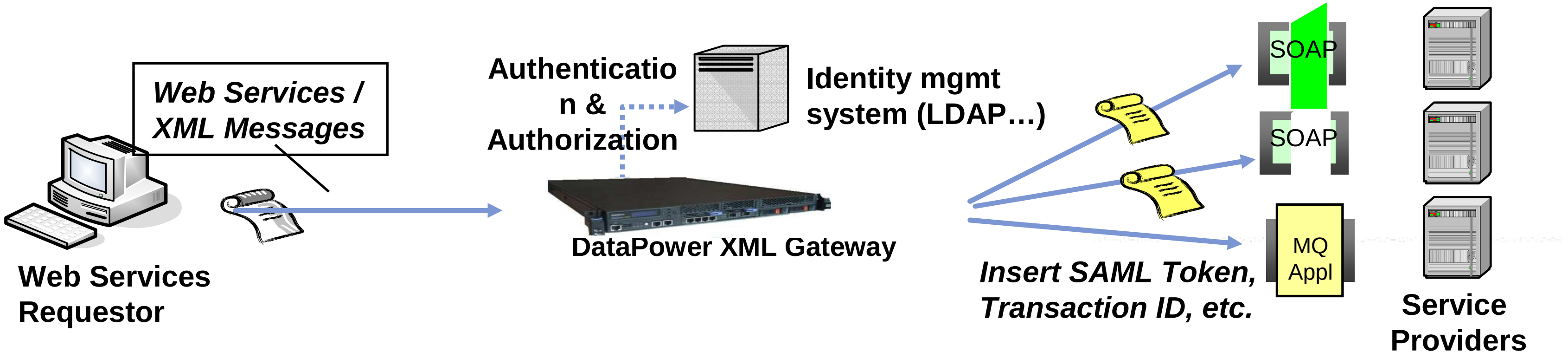


Employ flexible AAA (Authenticate, Authorize, Audit) Policies



Comprehensive Web Services & XML Security

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


Web Services / XML Messages
Web Services Requestor
Authentication & Authorization
Identity mgmt system (LDAP…)
DataPower XML Gateway
Insert SAML Token, Transaction ID, etc.
SOAP
SOAP
MQ Appl
Service Providers

IBM SECURITY TRENDS SEMINAR 2012

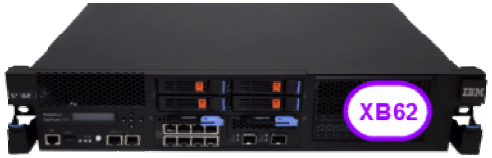
FORTIFY YOUR COMPANY AGAINST INTERNAL AND EXTERNAL THREATS

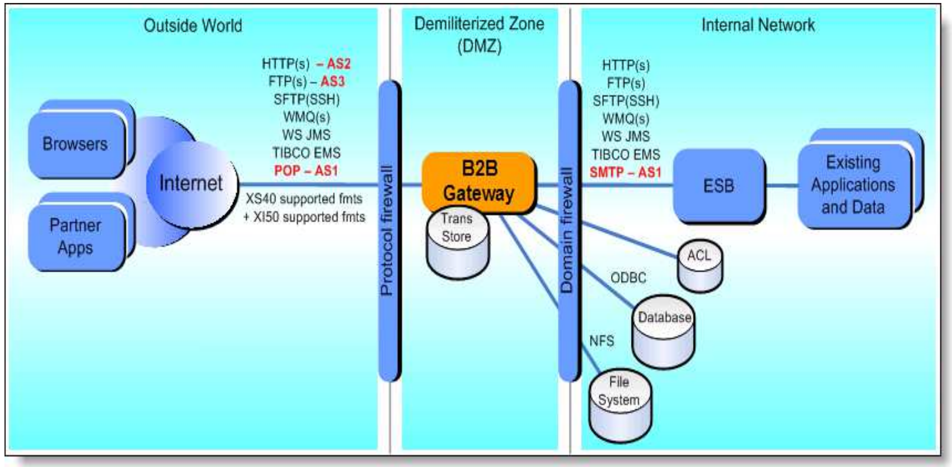
XML Threats - Security Risks Growing

- 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

IBM SECURITY TRENDS SEMINAR 2012

FORTIFY YOUR COMPANY AGAINST INTERNAL AND EXTERNAL THREATS





B2B Gateway

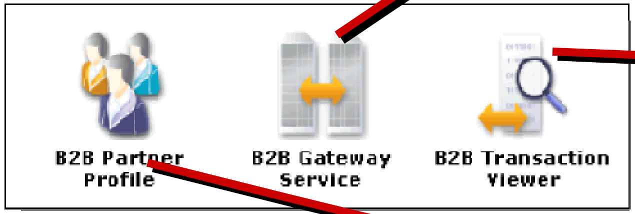
- All of the capabilities of the XG45 to proxy and enforce policies
- Partner Management functions:
  - Define partners with the web management console
  - Associate partners with network endpoints
  - Attach metadata about the partners to their definitions
- Enhanced Qualities of Service
  - Onboard persistent transaction store
  - Search messages by partner, time, etc
  - Replay messages if necessary
  - **ebXML/ebMS, AS1, AS2, and AS3 protocol bindings for greater reliability across traditionally unreliable protocols**

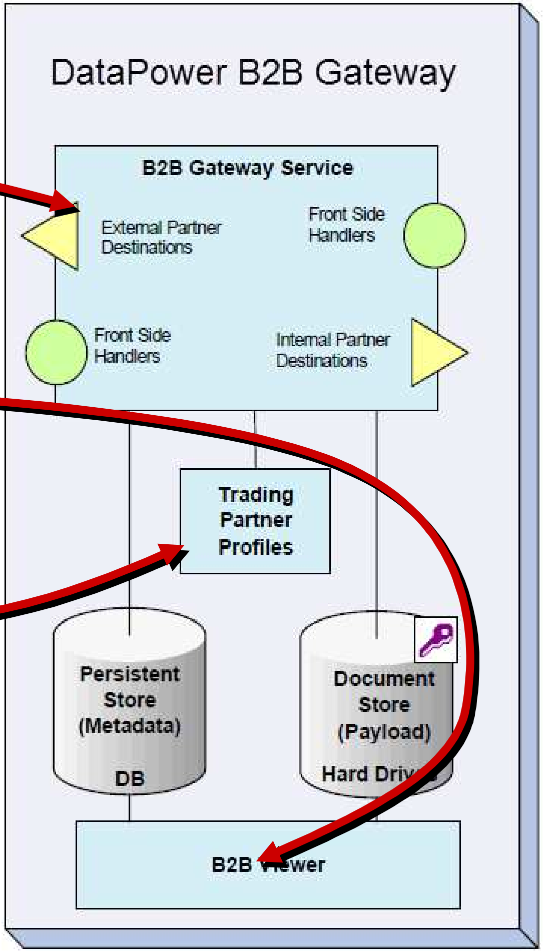
- Additional protocols supported
  - SFTP (SSH)
  - TIBCO EMS is available as an option
  - ODBC
- Additional formats supported
  - PKCS7 is included in base
- Additional transformation engines supported
  - DataGlue – WTX/FFD is included in base

IBM SECURITY SOLUTIONS

RISK MITIGATION. PROTECTION. COMPLIANCE.

B2B Gateway

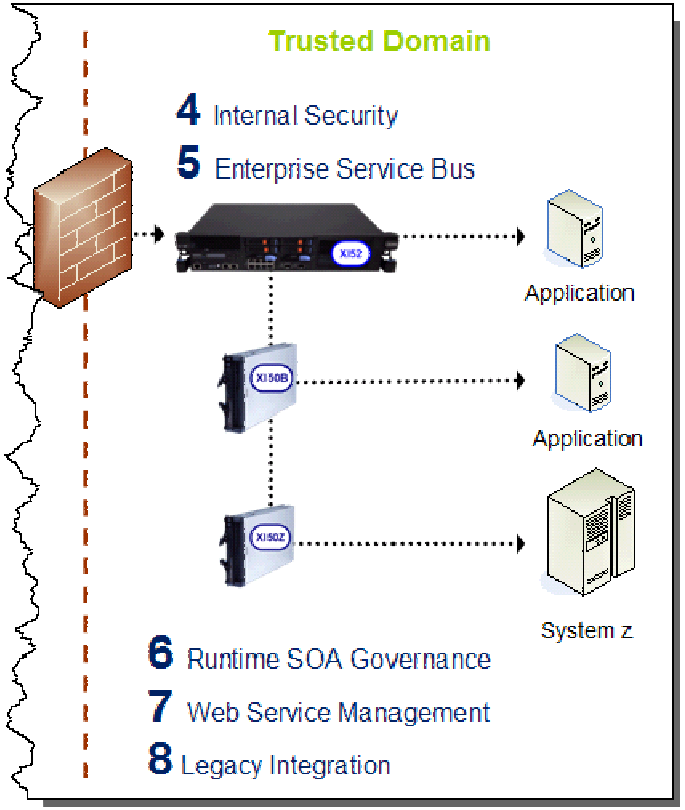




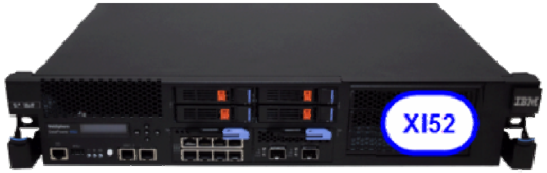
- Enhanced functionality for
  - Partner Profile configuration and management
  - Runtime B2B Gateway which can be configured to persist messages in flight
  - B2B Viewer allowing search by partner, date/time, etc. in order to quickly locate and understand the status of partner interactions

The devices are equally as popular for internal use as well

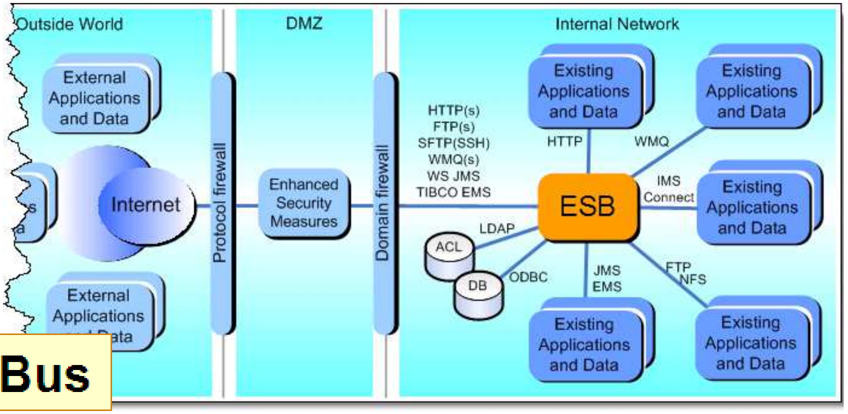
- Simplified, lower-touch maintenance
  - Average of 1-2 firmware upgrades per year
- Fast, less-expensive development
  - Configuration-only development
  - Multiple references of delivery to production in less than 1 month
- Many functions in a single box



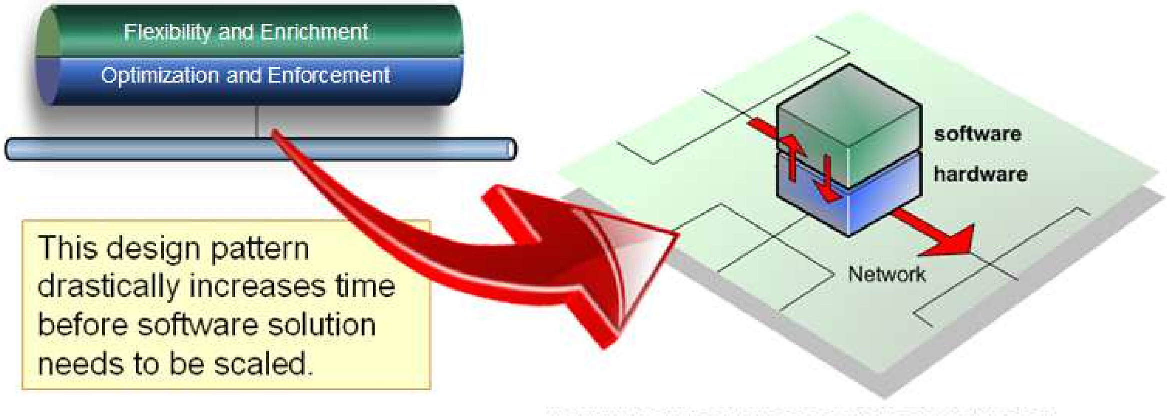
ESB and Legacy Enablement



- **IBM's "drop in" ESB**
  - Simplified deployment
  - Configure your integrations, save coding for business applications
  - Integrates smoothly into any "shop" (e.g. .Net, Java, Legacy) because a complex new application server environment does not need to be learned
- **Easily service-enable legacy apps**
  - Quickly put web service facades over existing System Z, System i, and other older applications
  - IMS Connect, MQ (to CICS etc), and file-based formats are all supported
- **Optimize existing SOA deployments by offloading the rote, repeatable, universal tasks of integration to a purpose-built platform**
  - Save idiosyncratic adapting, transaction management, and business process workflows for software


Outside World
External Applications and Data
Internet
External Applications and Data
Protocol firewall
DMZ
Enhanced Security Measures
Domain firewall
Internal Network
HTTP(s)
FTP(s)
SFTP(SSH)
WMQ(s)
WS JMS
TIBCO EMS
Existing Applications and Data
Existing Applications and Data
HTTP
WMQ
ESB
IMS Connect
Existing Applications and Data
LDAP
ACL
DB
ODBC
JMS EMS
FTP NFS
Existing Applications and Data
Existing Applications and Data

The Hybrid Bus



This design pattern drastically increases time before software solution needs to be scaled.

Agenda

What is a DataPower Appliance?

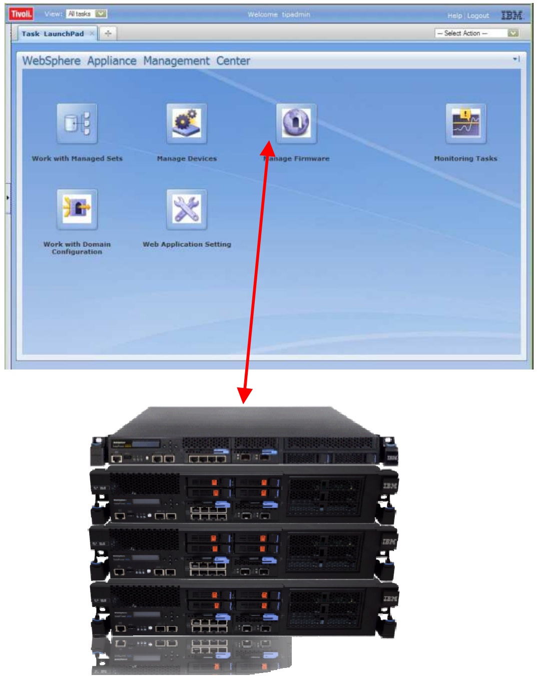
Secure Application Connection

Models and Features

Appliance Management

WebSphere Appliance Management Center (WAMC)

- **Provide multi-box DataPower appliance management**
  - Support managed sets of different appliance models & firmware
  - Exploits new support for managed domain tasks, configuration & firmware deployments
  - Manage deployment policies for DataPower appliances, individually or in managed sets
- **Simplified installation**
- **DataPower currency**
  - Support latest DP devices and agent platforms
- **Enhanced monitoring**
  - More DataPower KPIs accessible in one place than ever before
- **Ease of Use**
  - Enhanced Configuration UI
  - Navigation by user role
- **Seamless integration into Tivoli Monitoring infrastructure**
  - Plays well with enterprise-level Tivoli monitoring solutions like ITCAM



IBM SECURITY TRENDS SEMINAR 2012

FORTIFY YOUR COMPANY AGAINST INTERNAL AND EXTERNAL THREATS

THANK YOU!

Questions?

IBM SECURITY SOLUTIONS

RISK MITIGATION. PROTECTION. COMPLIANCE.