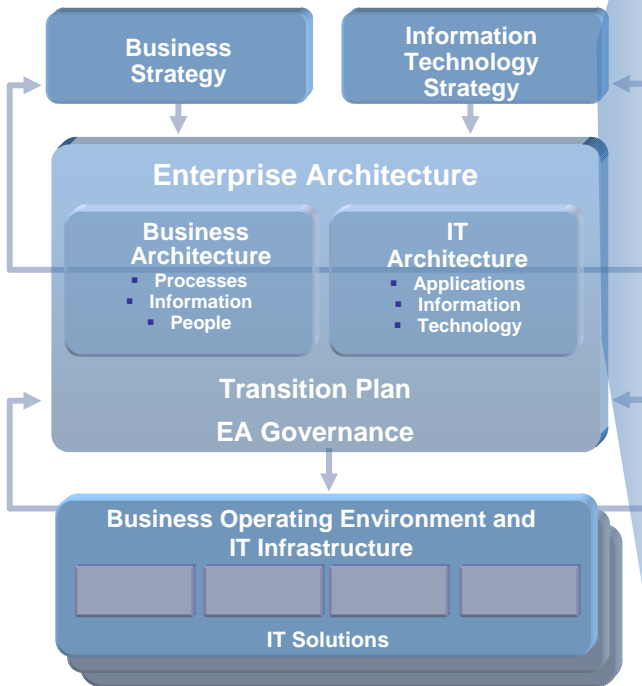# Smart Work for a Smarter Planet

Architecting the right SOA Infrastructure

Ameeta Roy
Software IT Architect Leader, IBM Software Group

What is the impact of SOA on current Enterprise Architectures?

- Alignment of Business and IT Architectures
- SOA Reference Models
- SOA Governance

Business Strategy

Information Technology Strategy

Enterprise Architecture

Business Architecture
- Processes
- Information
- People

IT Architecture
- Applications
- Information
- Technology

Transition Plan

EA Governance

Business Operating Environment and IT Infrastructure

IT Solutions

How do you develop SOA with a business focus?

- Business Components
- SOA Design
- Business Process Management

How do you reuse applications in the context of SOA?

- Asset Discovery
- Application Reuse

How do you leverage information in an SOA?

- Information as a Service
- Master Data Management

How does my infrastructure support SOA?

- Service Management / QoS
- Security

IBM

Agenda

- SOA Requires New Thinking About Infrastructure
- Infrastructure Considerations for SOA
  - Performance
  - Availability
  - Service Management
  - Security
  - Virtualization
- IBM Capabilities to Support SOA Infrastructure Architecture
- Summary

SOA Represents a Marked Change in IT Prioritization
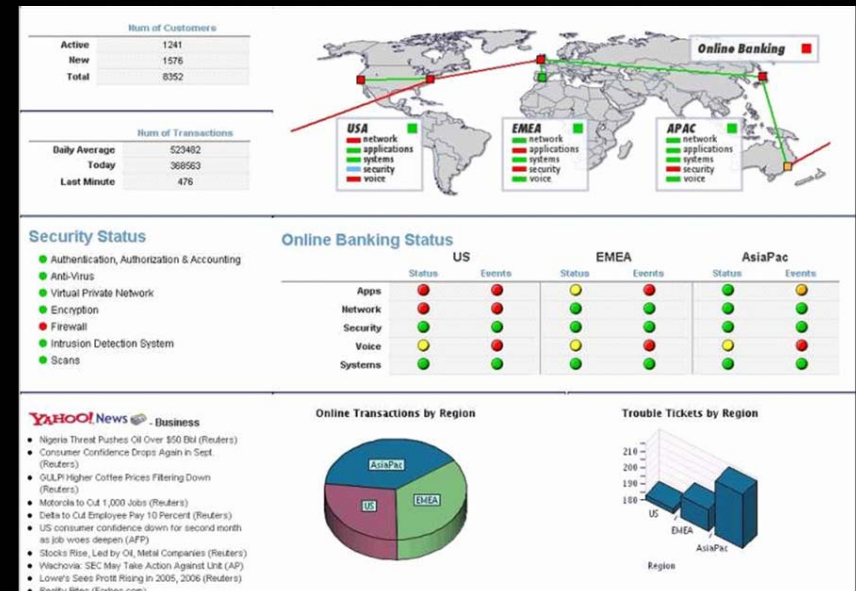## *And Requires a New Way of Thinking*

Old Thinking

IT *maintains* IT **resources** that support the business
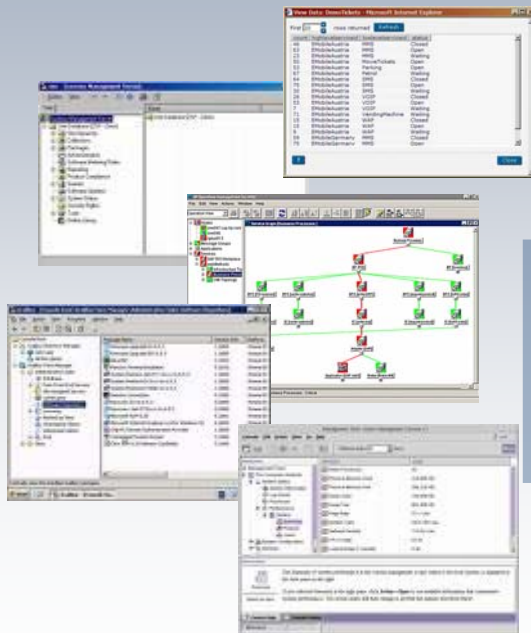
New Thinking

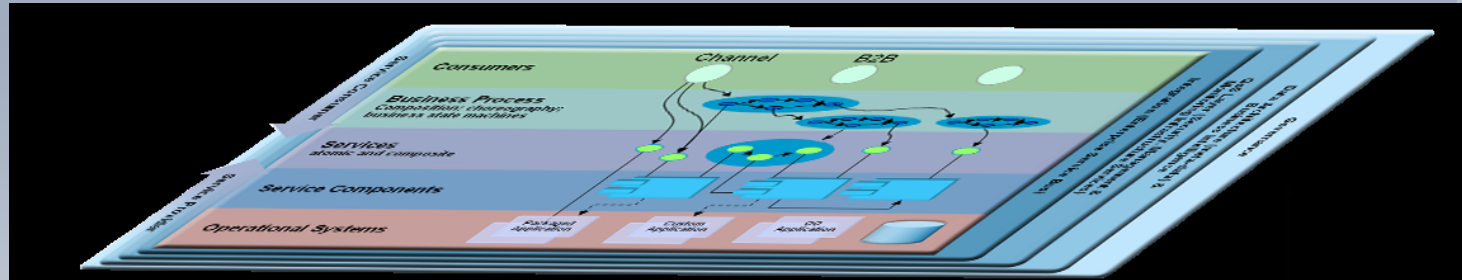IT *delivers* **services** designed to meet business **goals**
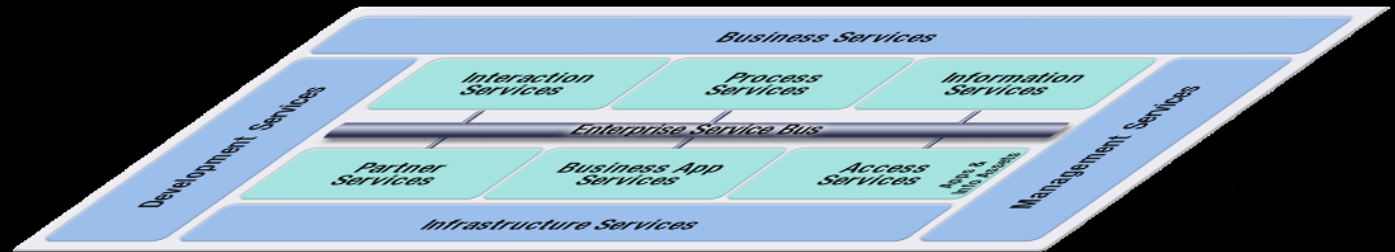
From Silos …

… to Services

IBM

SOA and Layers of Abstraction

Processes Services Applications

SOA Infrastructure

Physical Infrastructure

How Does SOA Impact Infrastructure and Management?

SOA Characteristics

- Applications reused in new dynamic ways

- Services combined from multiple sources

- Rapid deployment

- Services route to any available resource

- Distributed access

Key Infrastructure and Management Considerations

IT Infrastructure

- Strategy, Architecture and Design
- Integration
- Implementation and Migration
- Testing
- Performance
- Virtualization
- Security
- IT Service Management and Governance

Architectural Model for Dynamic Infrastructure®

SECURITY

RESILIENCE

SERVICE REQUESTORS

END USERS

DEVELOPERS

SERVICE CREATORS

OPERATORS

CUSTOMER SERVICE ADMINISTRATION

SERVICE MANAGEMENT

APPLICATION ARCHITECTURE

INFORMATION INFRASTRUCTURE

VIRTUAL IT INFRASTRUCTURE

SERVERS

STORAGE

NETWORK

PHYSICAL IT INFRASTRUCTURE

SERVERS

STORAGE

NETWORK

FACILITIES

BUSINESS INFRASTRUCTURE
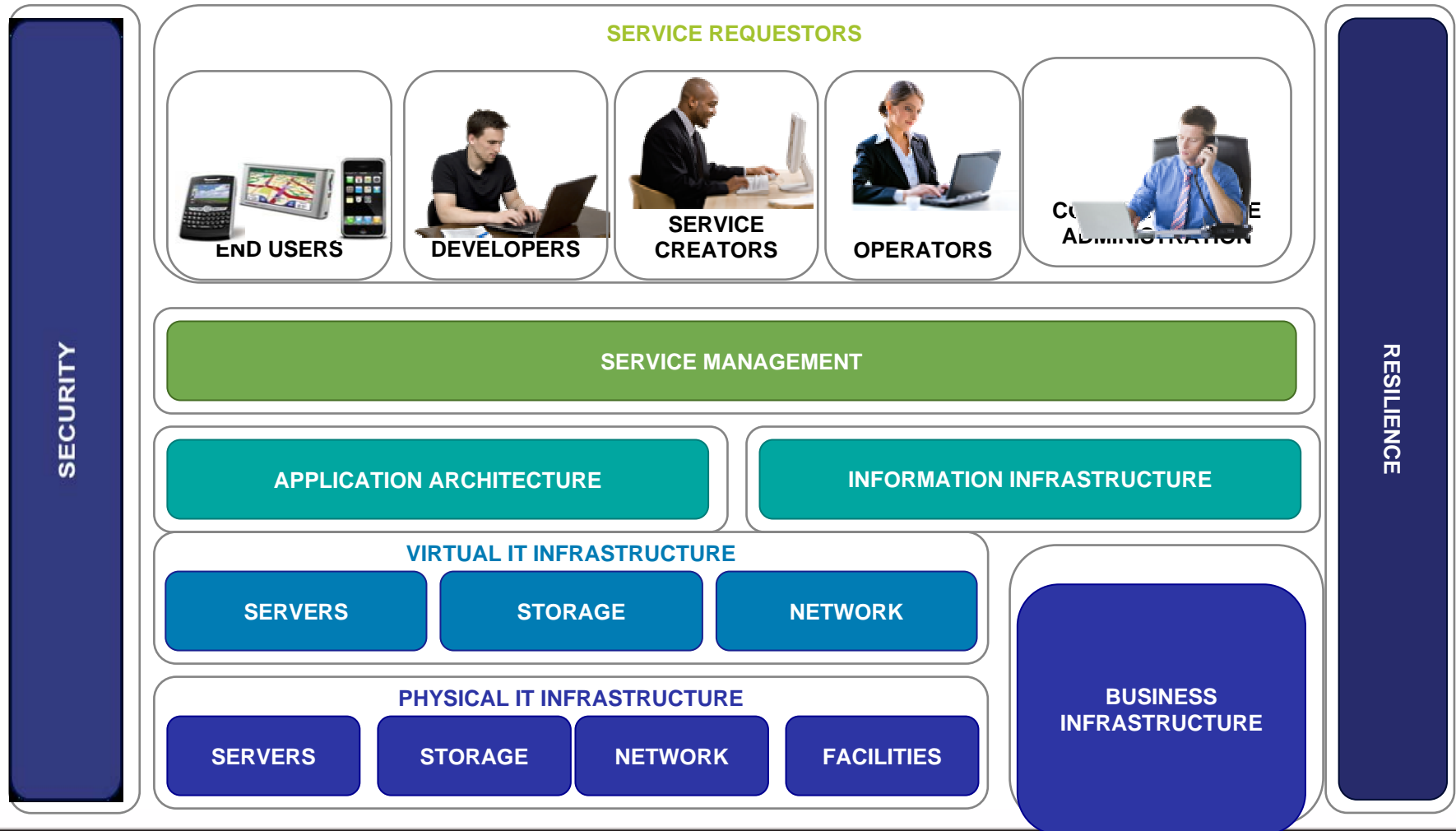
SOA-related concepts & challenges must be well-understood before starting the IT transformation

End-user

Partner

Mashup

Portal platform

Service desk

▸ Service definition (WSDL)
▸ Service contracts mgmt

Security layer

- Usage description
  . *#accesses / month*
  . *throughput*
- Security level
  . *rights, encryption*
  . *anonymity*
- Service level
  . *response time*
  . *availability rate*

Portal

Business logic

ESB access point

Technical mediations

▸ XML transcoding

▸ Delivery assurance

▸ Non repudiation
▸ Key management

Security management

Capacity & perf. management

Avail mgmt & continuity mgmt

Service level management

Financial management

Enterprise

Bus

Exchange platform

Network security layer

Internet

ESB access point

Inbound   Outbound

Technical mediations

Local directory

▸ Routing
▸ Identification
▸ Authentication
▸ Authorization
▸ Throttling
▸ Ramping-up
▸ Choking

Service delivery platform (xn)

ESB access point   *Exposed services*

Technical mediations

Functional mediations

▸ Transforming
▸ User aliasing…

Local directory

▸ Protocol transformation

Adapter   Adapter

Legacy SC / SP

Distributed enabler SP / SC

Choreographer SP / SC

Service design & management

Multi-layered network

Central operations & governance p

Functional meds

ESB access point

Dual Site (Active or Passive)

Global service namespace

Logging, Auditing & Accounting

Systems mgmt & Decision support

Change & Configuration management

Release management

Service Execution

Event, Incident & problem management

Agenda

- SOA Requires New Thinking About Infrastructure

- **Infrastructure Considerations for SOA**
  - Performance
  - Availability
  - Service Management
  - Security
  - Virtualization
- IBM Capabilities to Support SOA Infrastructure Architecture
- Summary

SOA Introduces Performance Challenges

- Measuring performance across organizational boundaries can be more difficult than in siloed applications
- Response time estimation is more challenging in a more distributed environment
  - Performance costs can be difficult to predict
  - Performance testing an SOA application requires the use of new techniques
- Increased requirement for XML processing may impact performance

- Don't forget about security overhead
  - Authentication, Authorization, Encryption

Performance Should Not be an Afterthought
It Should be Engineered into the Solution

- Performance in SOA systems should be a combination of performance engineering and performance management

- SOA-based applications can change the way an infrastructure performs
  - XML message transformation, location, message size, frequency
  - More complex applications and transactions

- Each of the components should be used to build a performance budget, transaction models and use cases

- Middleware and server sizing need to be done with the application teams
  - How many, how available, virtualized, system platform

- Don't forget about security overhead
  - Authentication, Authorization, Encryption

SOA Performance Testing Concepts

- Test SOA applications throughout the development lifecycle

- Test tools must be separate and external to the SOA environment

- Use multiple diverse datasets that are representative of an SOA workload

- Stress test the solution to detect trouble areas

- Run tests in a comparable environment to the deployment environment

- Use multiple test tools – similar results from multiple test tools using identical data sets validates the tests

SOA Performance Testing and Problem Analysis Tools

- Validate system scalability
  - Workload modeling for automated generation of test clients
  - Automated generation of performance tests
  - Real-time reporting of server response time and throughput

- Isolate performance bottlenecks and resolve problems
  - Monitoring support for services across multiple platforms
 - Collection and visualization of server resource data – root cause analysis

Service response time

Visualization of server resource data
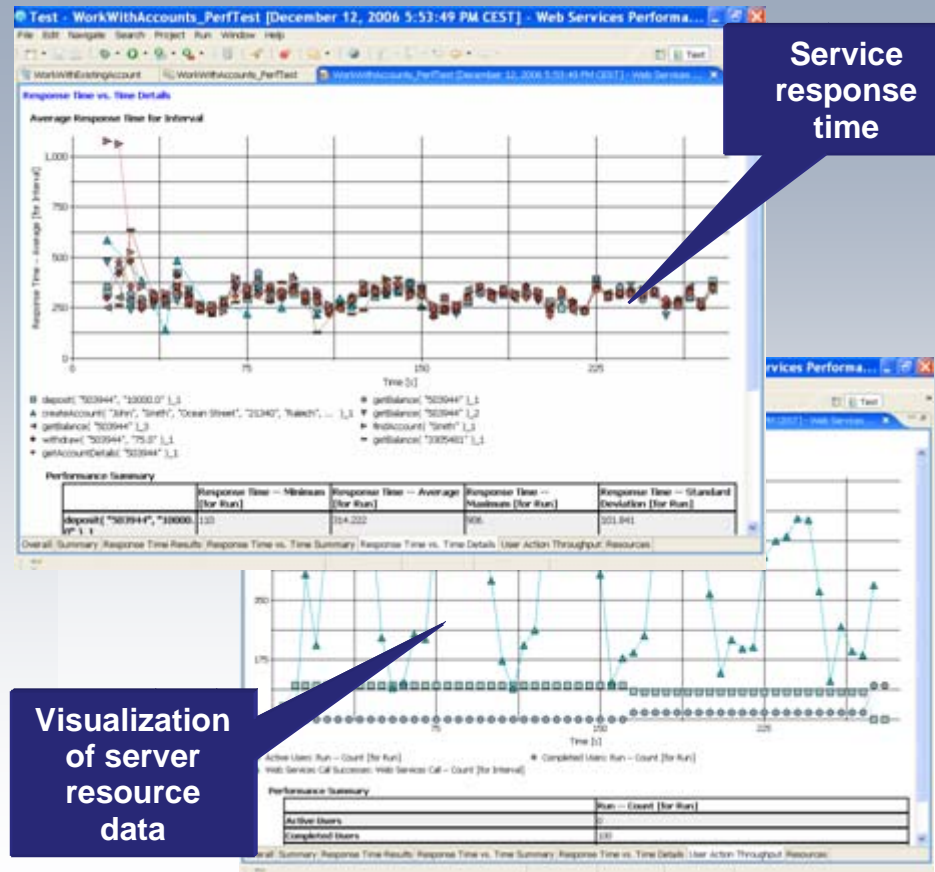
Monitoring Transaction Performance in SOA
Response Time Metrics in a Distributed Environment

- Composite applications span technology and platform boundaries

- Can be difficult to identify and isolate performance bottlenecks

- Use lightweight instrumentation that can be dynamically configured to proactively identify performance problems

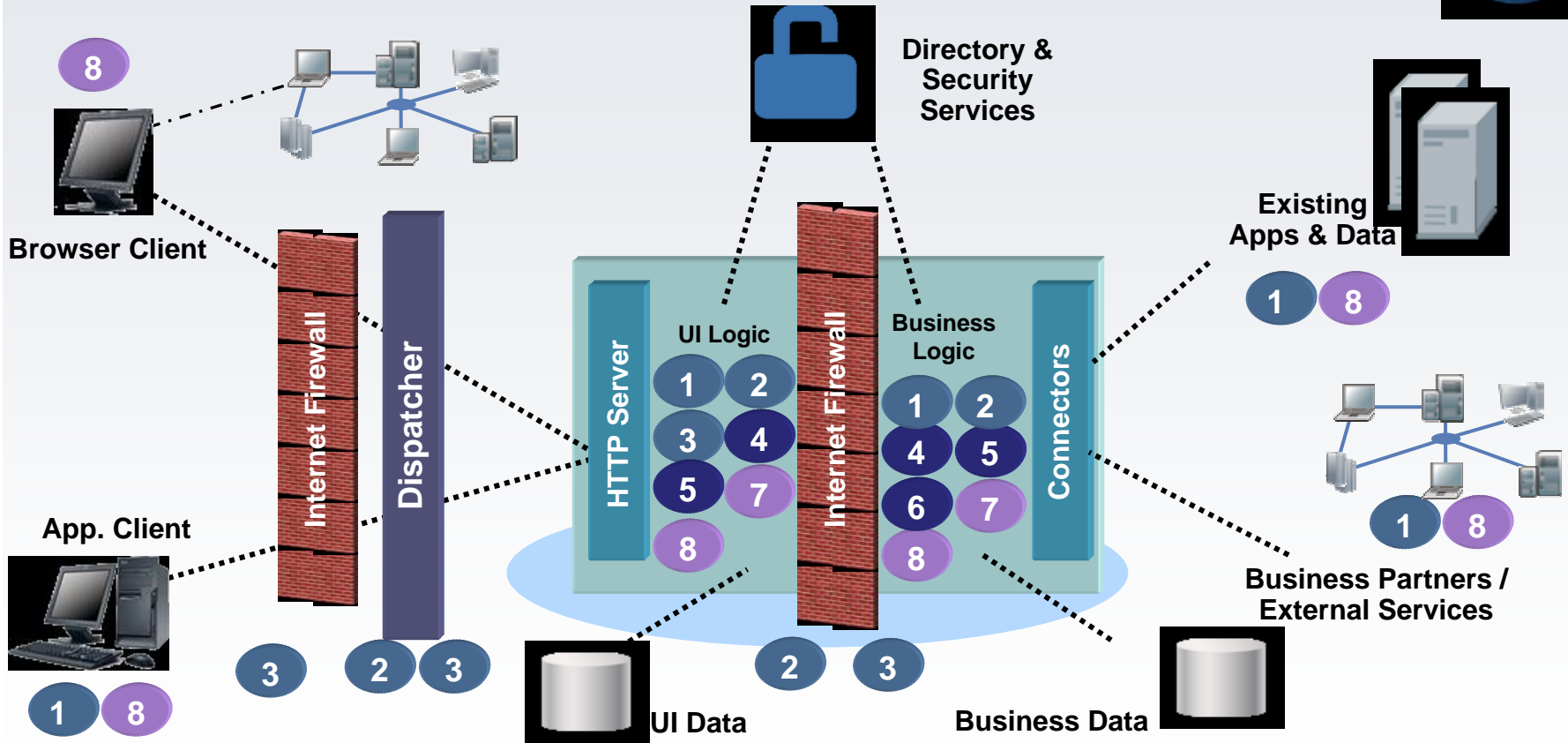- Use industry-standard ARM-based instrumentation to isolate the problem

IBM
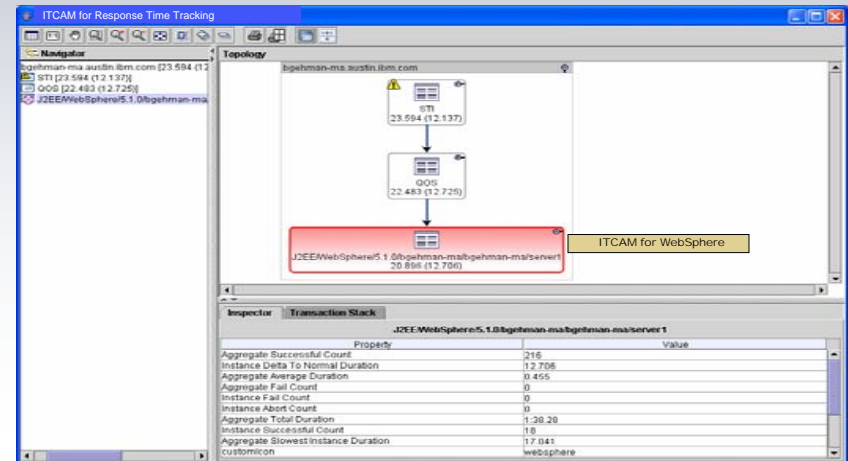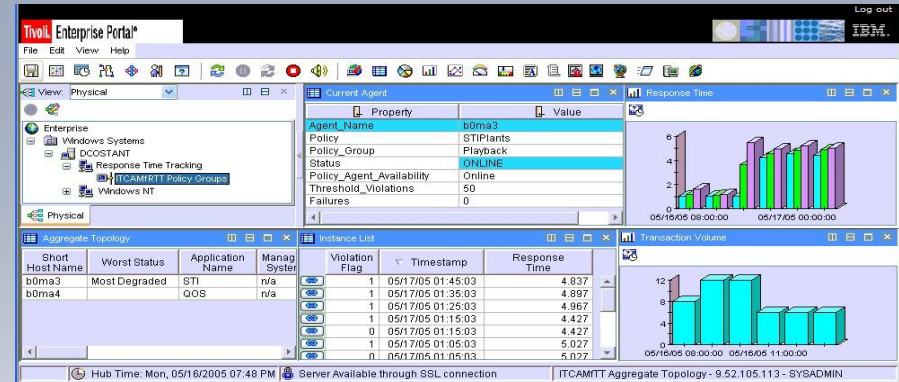
Guidance for SOA Performance

- The SOA performance model should be created and maintained throughout the lifecycle as the application is built

- Performance testing needs to obtain sufficient metrics to validate that services meet performance expectations

- Use established techniques to meet SOA performance requirements

- Design, test, and retest to confirm that non-functional requirements are met

- Implement an integrated solution that will automatically monitor, analyze and resolve response time problems

- Consider dedicated network appliances to optimize and accelerate XML parsing and security processing

Techniques for High Availability and Scalability

Browser Client

App. Client

Internet Firewall

Dispatcher

HTTP Server

Internet Firewall

Connectors

Directory & Security Services

UI Logic

1 2
3 4
5 7
8

Business Logic

1 2
4 5
6 7
8

Existing Apps & Data

1 8

Business Partners / External Services

1 8

UI Data

2 3

Business Data

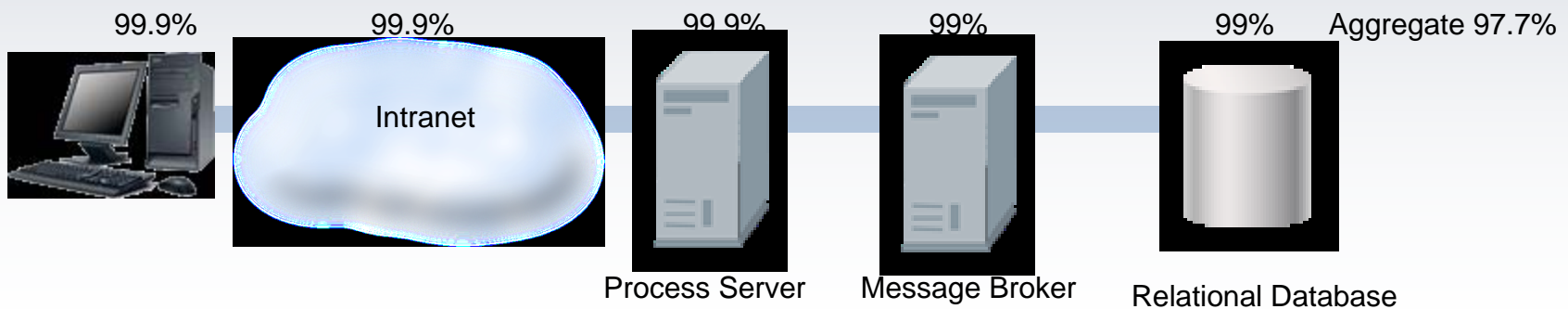|		
1 Faster Machines	**4** Segmented Workload	**7** Connection Management
2 Replicated Machines	**5** Request Batching	**8** Caching
3 Specialized Machines	**6** Data Aggregation	

High Availability in the SOA World

- An application may exist on multiple servers in different locations
    - Applications need to be "availability" aware in case a service within the workflow is unavailable

- SOA applications impact service availability levels
    - SOA introduce new application dependencies, including externally provided services
    - Need to understand the end-to-end view

- Monitoring, management and reporting is required to achieve predictable availability in an SOA environment

- Plan for the unexpected
    - What are the non-functional requirements? What systems are you using? Distributed? Mainframe? Where are they located? How will they be accessed?
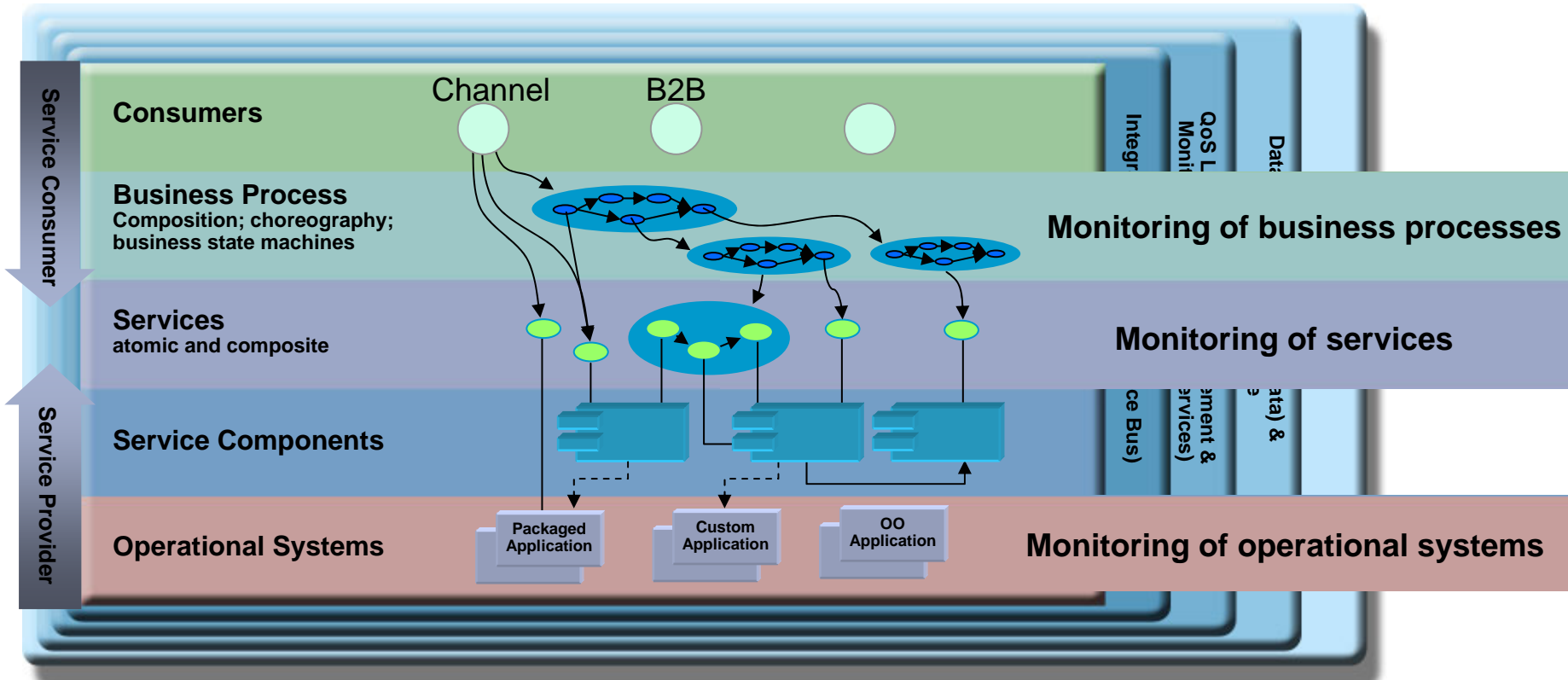   - The more components in the transaction, the greater the risks for failure or human error

Guidance for SOA Availability

- There are an increased number of components in an SOA infrastructure, so test rigorously for availability
- Create failover plans based on criticality of applications and services
- Take advantage of established availability techniques
  - Each component requires its own availability architecture
  - Leverage capabilities like Workload Management, High-Availability Manager, Deployment Manager, etc.
- Some components may require both hardware and software clustering
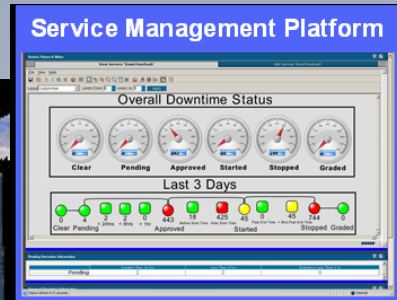 - Databases, enterprise messaging infrastructure, SOA appliances

99.9%	99.9%	99.9%	99%	99%	Aggregate 97.7%
	Intranet	Process Server	Message Broker	Relational Database	

The Challenges of Managing SOA

Service Management
Requires a Closed-Loop Approach

Service Management Platform

How does this relate to the business service?
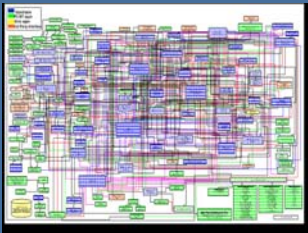
What's happening with the infrastructure?

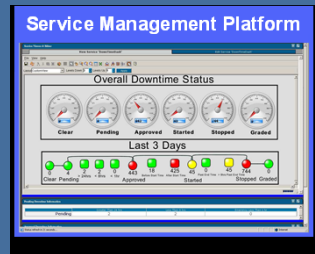**What actions do we take to correct the problems?**

IBM Service Management

What's happening with the infrastructure?

- Infrastructure and application discovery
- Server monitoring
- Storage monitoring
- Network monitoring
- Data monitoring
- Application monitoring
- Service monitoring

How does this relate to the business service?

- Dashboard
- Application dependency mapping
- Business service management
- Service level management
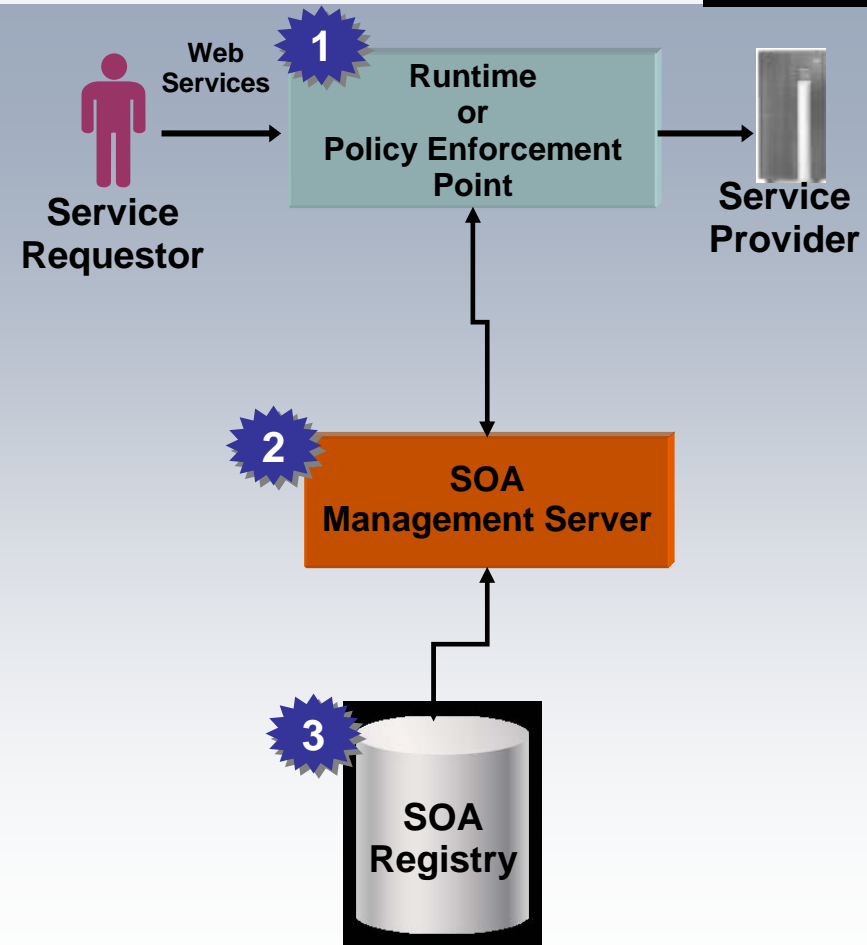
What actions do we take?

- System reconfiguration
- Data restore
- User identity provisioning
- System and application restart
- Infrastructure deployment
- Service mediation

Key Elements for Managing Services

There are 3 key components in services management:

1. The runtime environment – this is where messages are routed, secured, transformed, filtered and logged

2. The management server – aggregates the data from all of the endpoints and runtimes and sends configuration changes based on policy

3. The registry – stores meta data about services and policies

Service Requestor

Web Services

1

Runtime or Policy Enforcement Point

Service Provider

2

SOA Management Server

3

SOA Registry

Integrated Visibility of SOA Resources

Integrated Console

Service Consumer

Service Provider

Consumers

Business Process
Composition; choreography; business state machines

Services
atomic and composite

Service Components

Operational Systems

Channel   B2B

Service Management

Application Monitoring

Resource Monitoring

Resource Monitoring

Transaction Tracking

Integrated Reporting
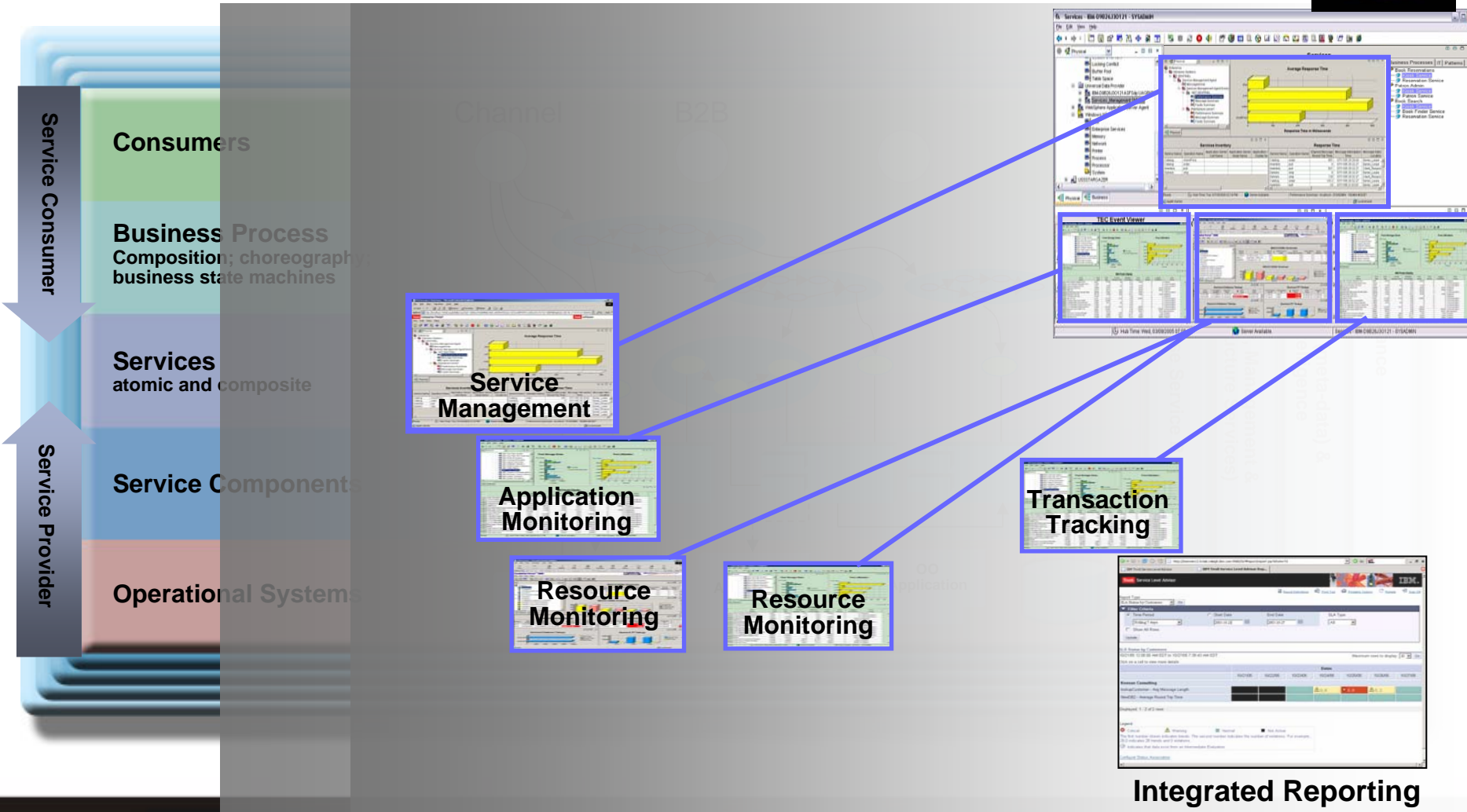
Guidance for Service Management

- Establish operational and business-focused management and monitoring perspectives

- Monitor the end-to-end solution to isolate and fix problems

- Automate provisioning and control of services to meet SLAs

- Make use of tools to improve application availability

- Track/predict change to reduce costs and downtime

SOA Security Considerations

- SOA introduces raise additional security issues
  - How do we identify and authenticate the service requester?
  - How to we identify and authenticate the source of the message?
  - Is the client authorized to send this message?
  - Can we ensure message integrity & confidentiality?
  - How do we audit the access to services?
  - How do we leverage Web services security standards?
  - How do we propagate identities with trusted service providers?

- XML Web services may expose backend systems in unintended ways

- SOA security may require multiple layers of enforcement – perimeter, gateway, app server, application

- Traditional security devices do not secure XML/SOAP

SOA Security – Trust Model
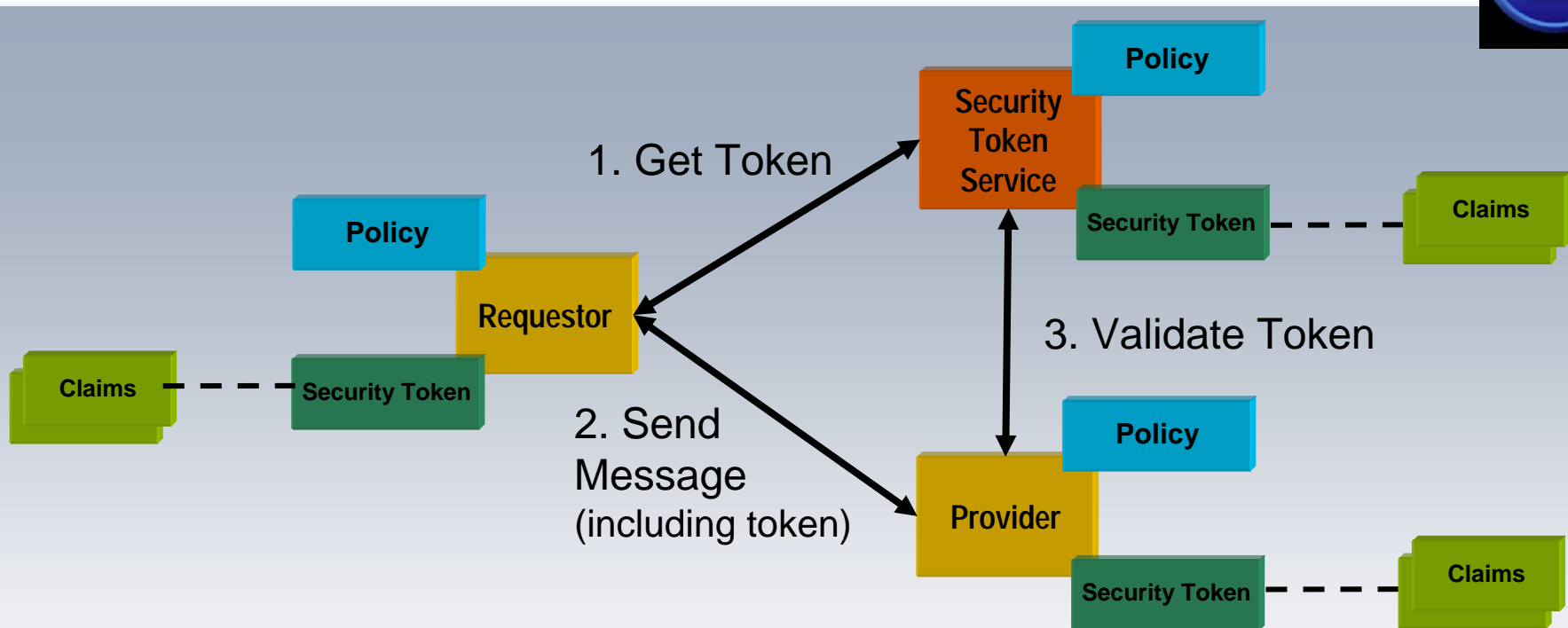
- Identity Federation and Web Services requires trust
  - This trust is based on agreements between partners & expressed as policies
- Trust can be enabled by technology
  - Trust requirements expressed as infrastructure policies and requirements
  - Security tokens include identity information; Cryptographic keys used to sign Security Tokens
- Technology needs to be standards based
  - Standard ways to express and exchange policies that reflect trust relationships
  - Agreed token format, information content, signing and encryption methods

XML Security Appliances
Can Simplify and Accelerate SOA Security
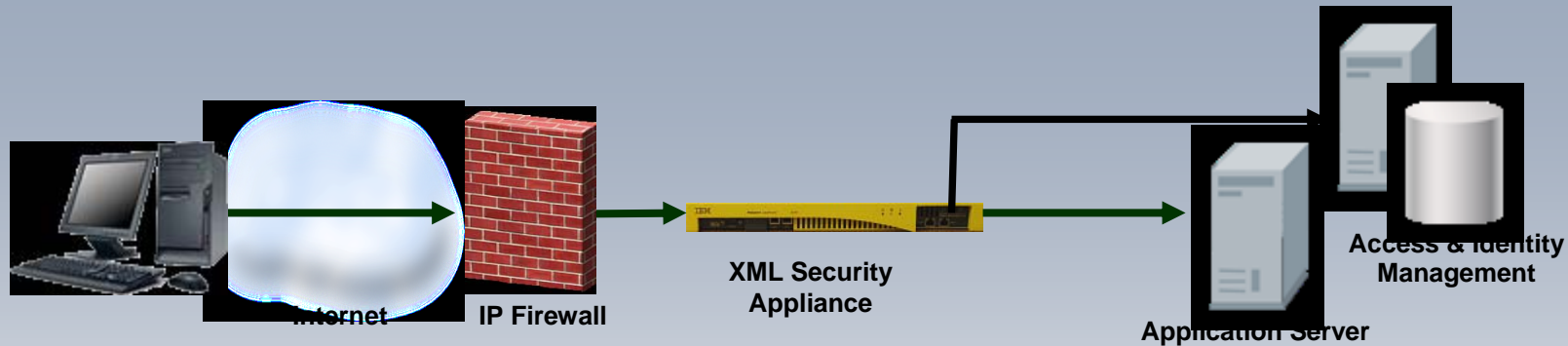
- XML/SOAP firewall enables filtering on any content, metadata or network variables

- Incoming and outgoing XML and SOAP is validated at wire speed

- Security can be performed at the field level
  - WS-Security
  - Encrypt & sign individual fields
  - Non-repudiation

- Provides XML/Web services access control

Guidance for SOA Security

- Security authorization needs to be granular at the service level

- Understand existing corporate security policies (especially approval and audit process) and apply them in the SOA environment

- Work with the SOA application teams to understand the requirements

- Understand the trade-offs of security, performance and cost

- Choose policy-based over programmatic approaches to allow security decisions to be implemented at service invocation

- Evaluate performance implications of security implementations

- Consider XML appliances to accelerate security processing

Virtualization Decouples IT Infrastructure from Applications
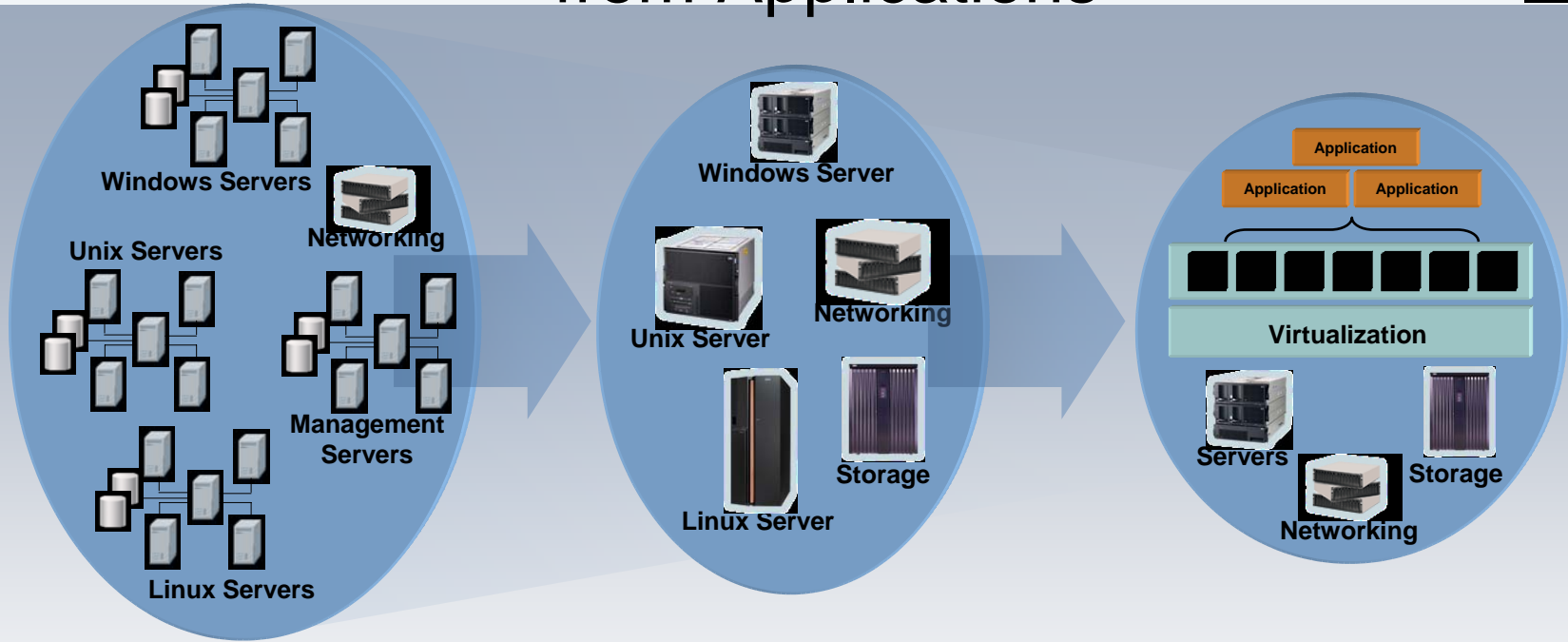
Complex

- 👎 Islands of computing and data
- 👎 Physical resources are bound to applications
- 👎 Disparate management tools
- 👎 Manual provisioning

Consolidated

- 👍 Fewer devices and licenses
- 👍 Increased utilization
- 👎 Physical resources still bound to applications
- 👎 disparate management tools
- 👎 Labor intensive provisioning

Virtualized

- 👍 Pools of resources
- 👍 Logic and physical resources decoupled
- 👍 Standardized, automated infrastructure management
- 👍 Automated provisioning

Infrastructure Optimization & Virtualization

Optimize infrastructure investment and prioritize applications and users in a mission-critical manner

- Provide high availability and redundancy for business-critical applications
- Increase server utilization to optimize capital & administration costs
- Ensure that the most important applications and users are given priority according to business and IT policies
- Flexibly respond to unforeseen application demand

Resource Optimization
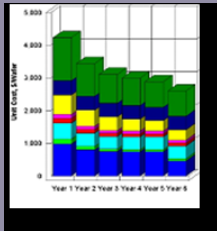
Utilization

Application Prioritization

Importance

High Availability

Assurance

Guidance for Virtualization

- Consolidate servers, storage & network assets for greater efficiency & reduced complexity

- IT resources should be used across applications without regard to where they physically reside

- Replace error-prone manual tasks & repetitive IT resource/capacity management tasks with automated capabilities

- Dynamically allocate IT capacity to meet business goals for increased infrastructure agility and readiness for growth
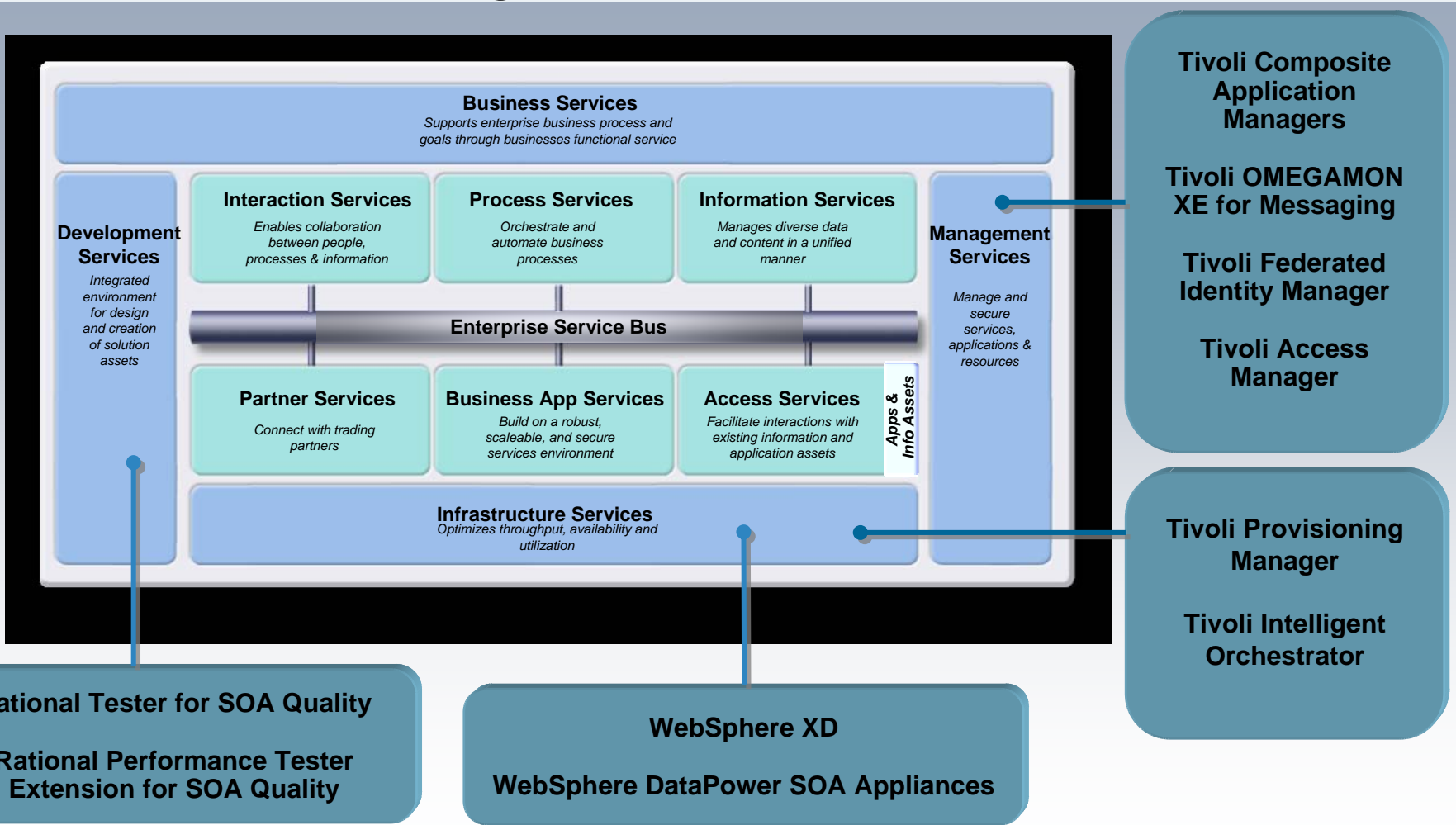
Agenda

- SOA Requires New Thinking About Infrastructure
- Infrastructure Considerations for SOA
  - Performance
  - Availability
  - Service Management
  - Security
  - Virtualization
- **IBM Capabilities to Support SOA Infrastructure Architecture**
- **Summary**

Mapping to the IBM Products

Business Services
Supports enterprise business process and goals through businesses functional service

Development Services
Integrated environment for design and creation of solution assets

Interaction Services
Enables collaboration between people, processes & information

Process Services
Orchestrate and automate business processes

Information Services
Manages diverse data and content in a unified manner

Management Services
Manage and secure services, applications & resources

Enterprise Service Bus

Partner Services
Connect with trading partners

Business App Services
Build on a robust, scaleable, and secure services environment

Access Services
Facilitate interactions with existing information and application assets

Apps & Info Assets

Infrastructure Services
Optimizes throughput, availability and utilization

Tivoli Composite Application Managers

Tivoli OMEGAMON XE for Messaging

Tivoli Federated Identity Manager

Tivoli Access Manager

Tivoli Provisioning Manager

Tivoli Intelligent Orchestrator

Rational Tester for SOA Quality

Rational Performance Tester Extension for SOA Quality

WebSphere XD

WebSphere DataPower SOA Appliances

IBM

The Keys to Architecting an SOA Infrastructure

- In the real-world, SOA-based applications put a lot of stress on a typical infrastructure

- From a business view, the application layer is geared towards simplification but the infrastructure can become complex

- The IT Infrastructure/Middleware Architect cannot let the SOA application become a *"black box"* within the infrastructure

- Visibility of quality of service metrics within the SOA application is crucial to achieving performance and availability goals

- As an IT Infrastructure Architect, one needs to know what is in the toolbox and how to build the best infrastructure for the SOA application

Thank You