Architecting the Ultimate Control-Point-Advanced Cyber-Threat Mitigation

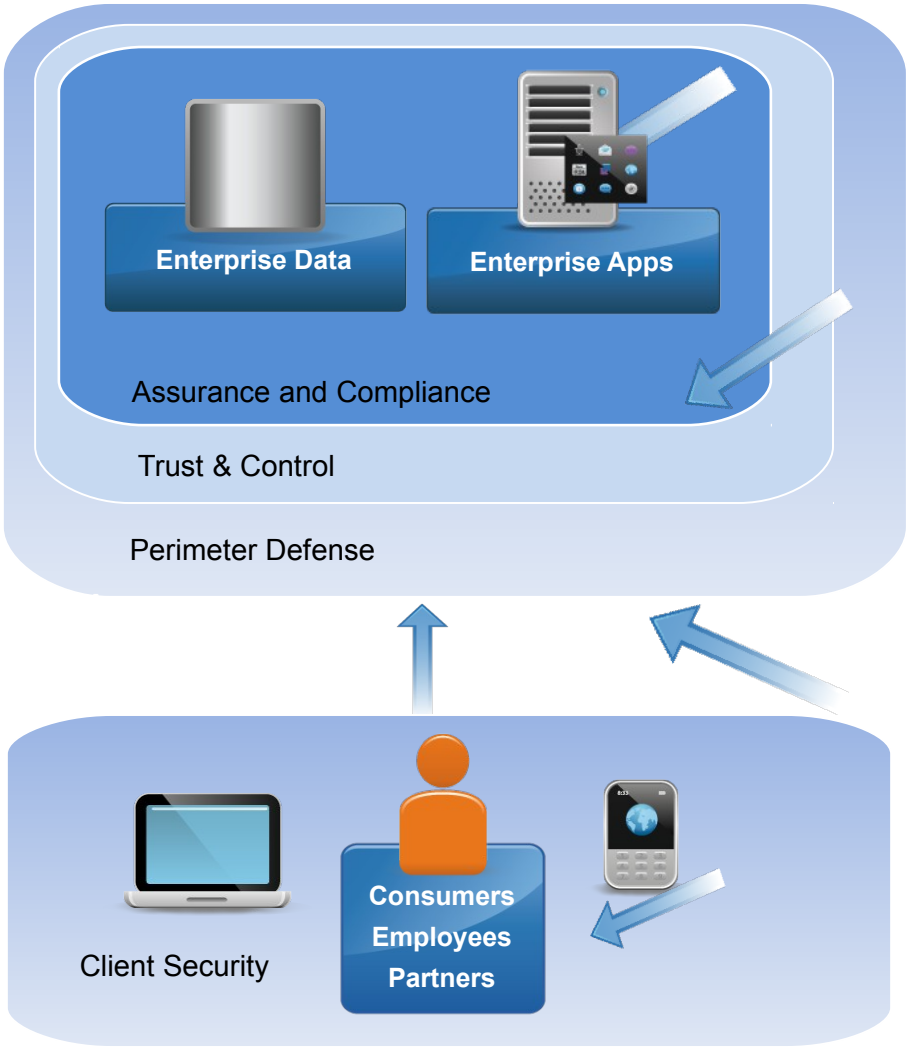
Presented by:

SOA Expressway Product Manager
Blake Dournaee

Agenda

- Part 1 Enterprise Security Overview
- Part 2 Threat Mediation Approaches
- Part 3 Gateway's Role in Policy Enforcement
- Part 4 Significance of Audit Logging
- Part 5 Live Gateway Demonstration

Enterprise/Cloud Security Layers to Address



Assurance and Compliance: How do I protect my data and ensure compliance?
- Data Loss Prevention
- Compliance (PCI/PII/SOX)
- Auditing

Trust and Control: How do I know who to trust and why?
- Authorization and access control?
- Usage?
- Trust for partner apps and services?
- Data confidentiality?

Perimeter Defense: How do I keep threats out of my datacenter?
- Intrusion Prevention and Detection
- Anti-Virus and Malware protection?
- Content threat protection?
- Protection against DoS attacks?

Client Security: How do I ensure trusted client access? How do I protect clients from malware and content threats?

STRIDE Threat Model Examples

Threat	Description	Example
Spoofing	Assume identity of client, server or request/response	Phishing attack to fool user into sending credentials to fake site
Tampering	Alter contents of request or response	Message or data integrity compromised to change parameters or values
Repudiation	Dispute legitimate transaction	Illegitimately claiming a transaction was not completed
Information Disclosure	Unauthorized release of data	Unencrypted message sniffed off the network
Denial of Service	Service not available to authorized users	System flooded by requests until web server / app fails
Elevation of privilege	Bypass authorization system	Attacker changes group membership

Threat Model + Countermeasure Examples

Threat	Security Service
Spoofing	Authentication
Tampering	Digital Signatures
Repudiation	Audit Logging
Information Disclosure	Encryption
Denial of Service	Throttling, Metering, Blocking
Elevation of privilege	Authorization

Where does SAML fit in?

SAML = Security Assertion Markup Language

Threat	Security Service	Data	Method	Channel
Spoofing	Authentication	SAML	SAML	
Tampering	Digital Signature	SAML		
Dispute	Audit Logging			
Information Disclosure	Encryption	SAML		
Denial of Service	Throttling, Metering, Blocking			
Elevation of privilege	Authorization, Input validation	SAML		

Where does Audit Logging fit?

Threat	Security Service	Data	Method	Channel
Spoofing	Authentication			
Tampering	Digital Signature			
Dispute	Audit Logging	Audit Logging	Audit Logging	Audit Logging
Information Disclosure	Encryption			
Denial of Service	Availability			
Elevation of privilege	Authorization, Input validation			

What We've Seen So Far – Just a Taste...

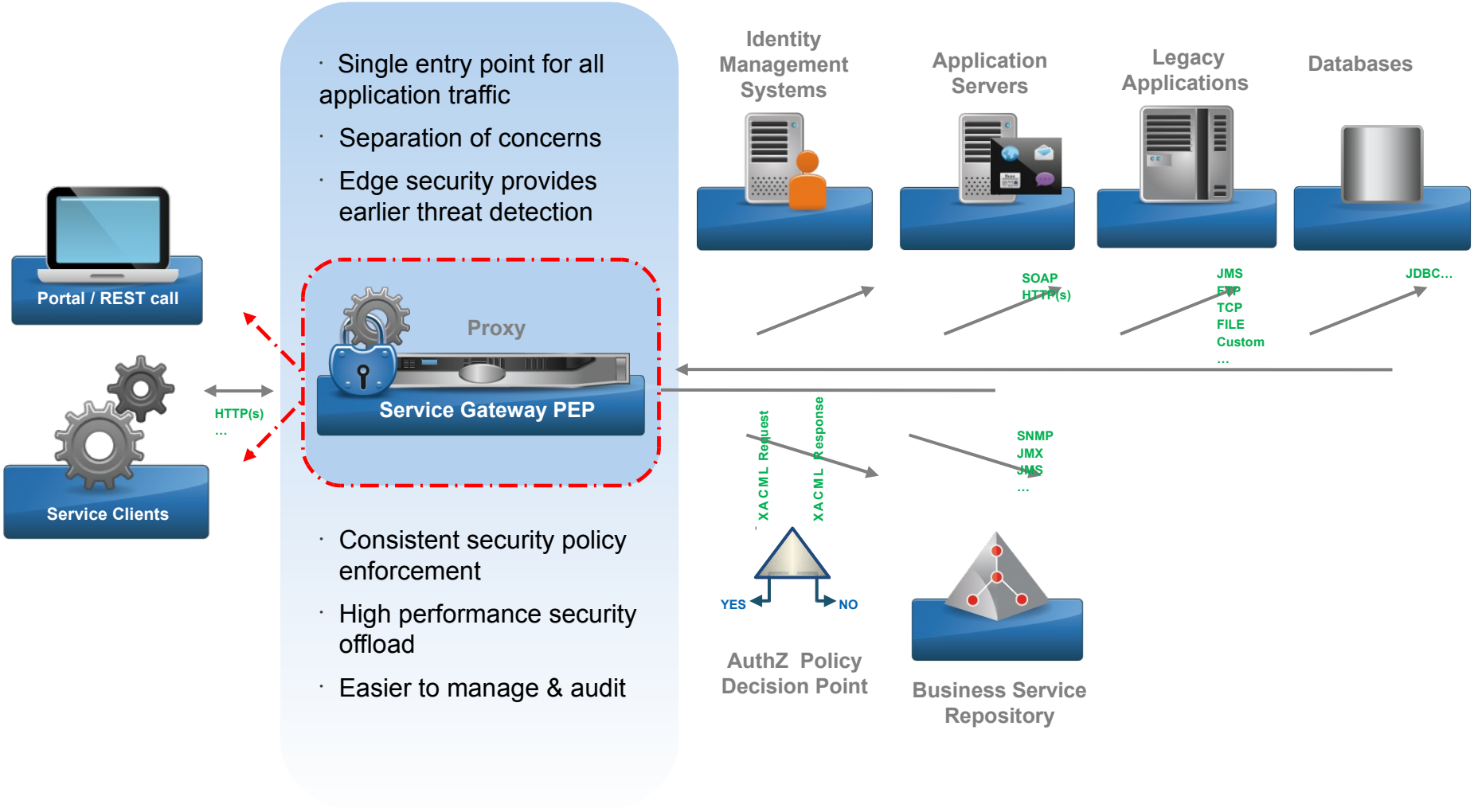
Threat	Security Service	Data	Method	Channel
Spoofing	Authentication	SAML	SAML	SSL/TLS
Tampering	Digital Signature	SAML	WS-Security	SSL/TLS
Dispute	Audit Logging	Audit Logging	Audit Logging	Audit Logging
Information Disclosure	Encryption	SAML	WS-Security	SSL/TLS
Denial of Service	Availability	Security Gateway	Security Gateway	Security Gateway
Elevation of privilege	Authorization, Input validation	SAML	XACML	SSL/TLS

Bottom Line: Implementing these standards and pre-cautions in code is a challenge – is there a better way?

Externalizing Security Policies with a Service Gateway

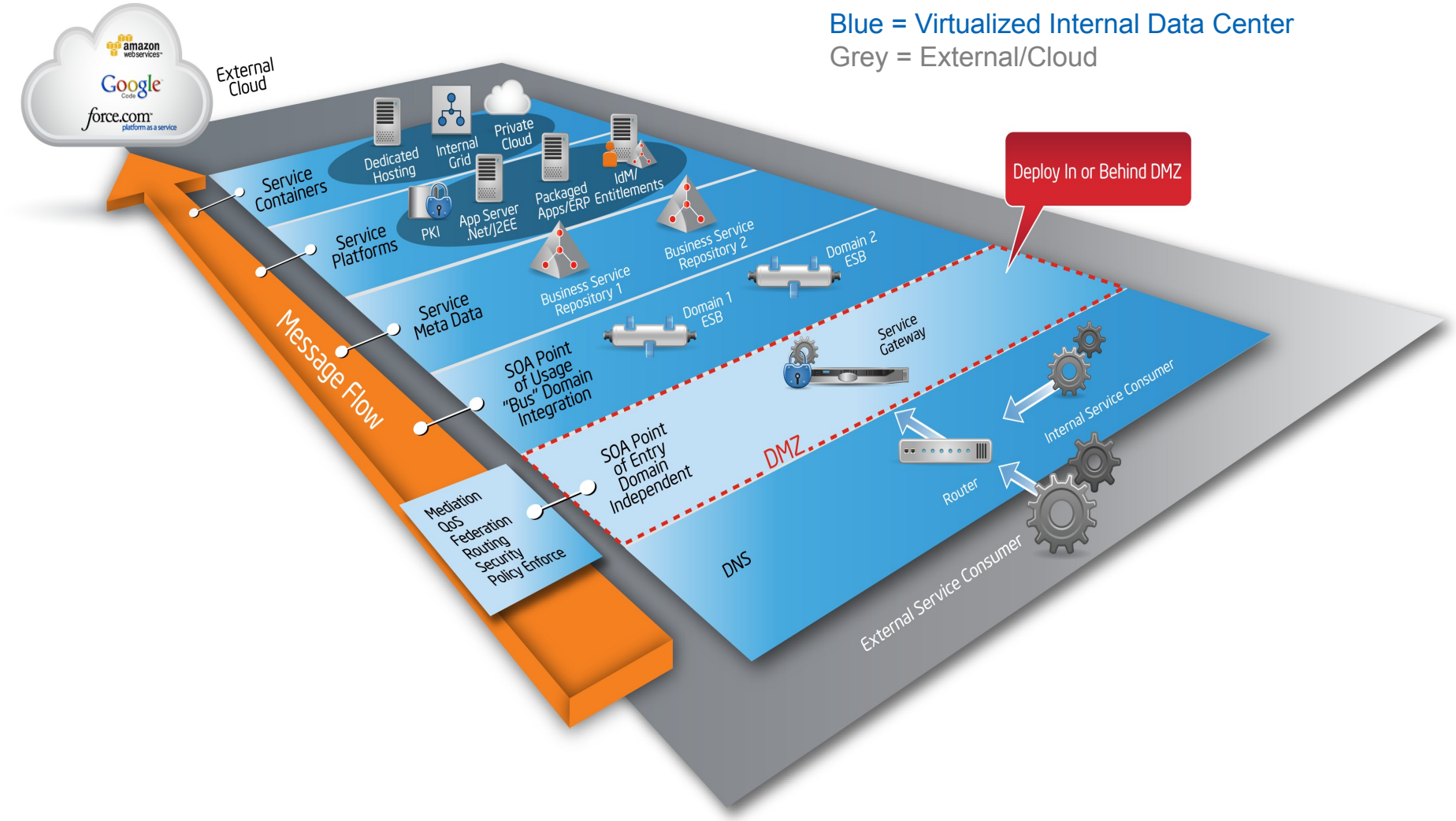
- A *service gateway* is a high-performance multi-form factor appliance for application level security
- E.G. an application level *proxy* for services
- Implement security policies outside of code
  - Ability to review & audit outside of application
  - Ability to version security independent application
  - Virtual patching – Where's the control point? If a major attack is found or launched against your system where can you defend from?
  - Enforce Separation of Privilege
  - Code is easier to maintain over time
  - Free yourself from being a security developer

Inter-domain or Edge Gateway: Technical Usage Model



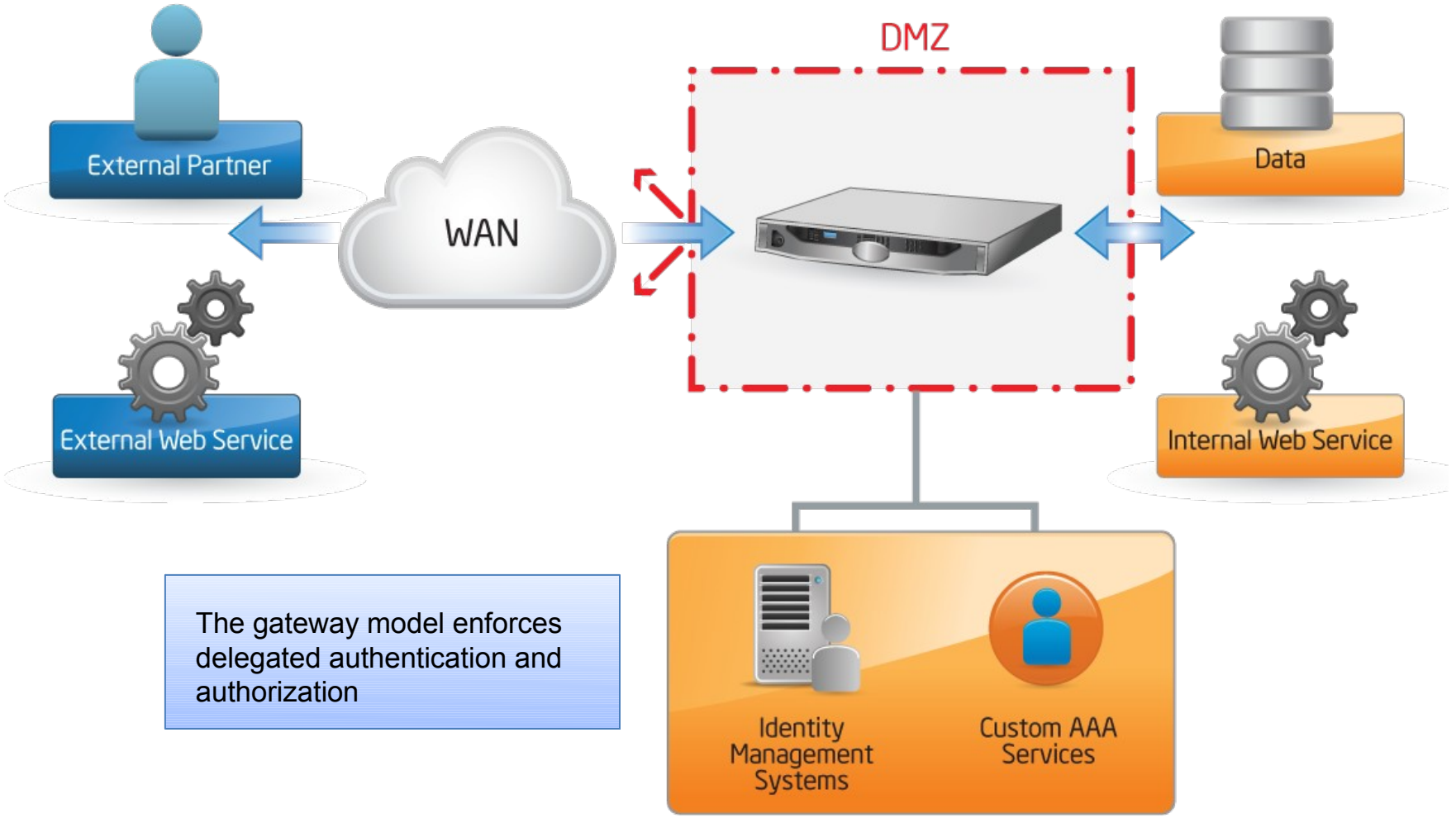
Externally facing security layer and central proxy that connects domains, middleware & identity infrastructure

Service Gateway…From the Data Center to the Cloud



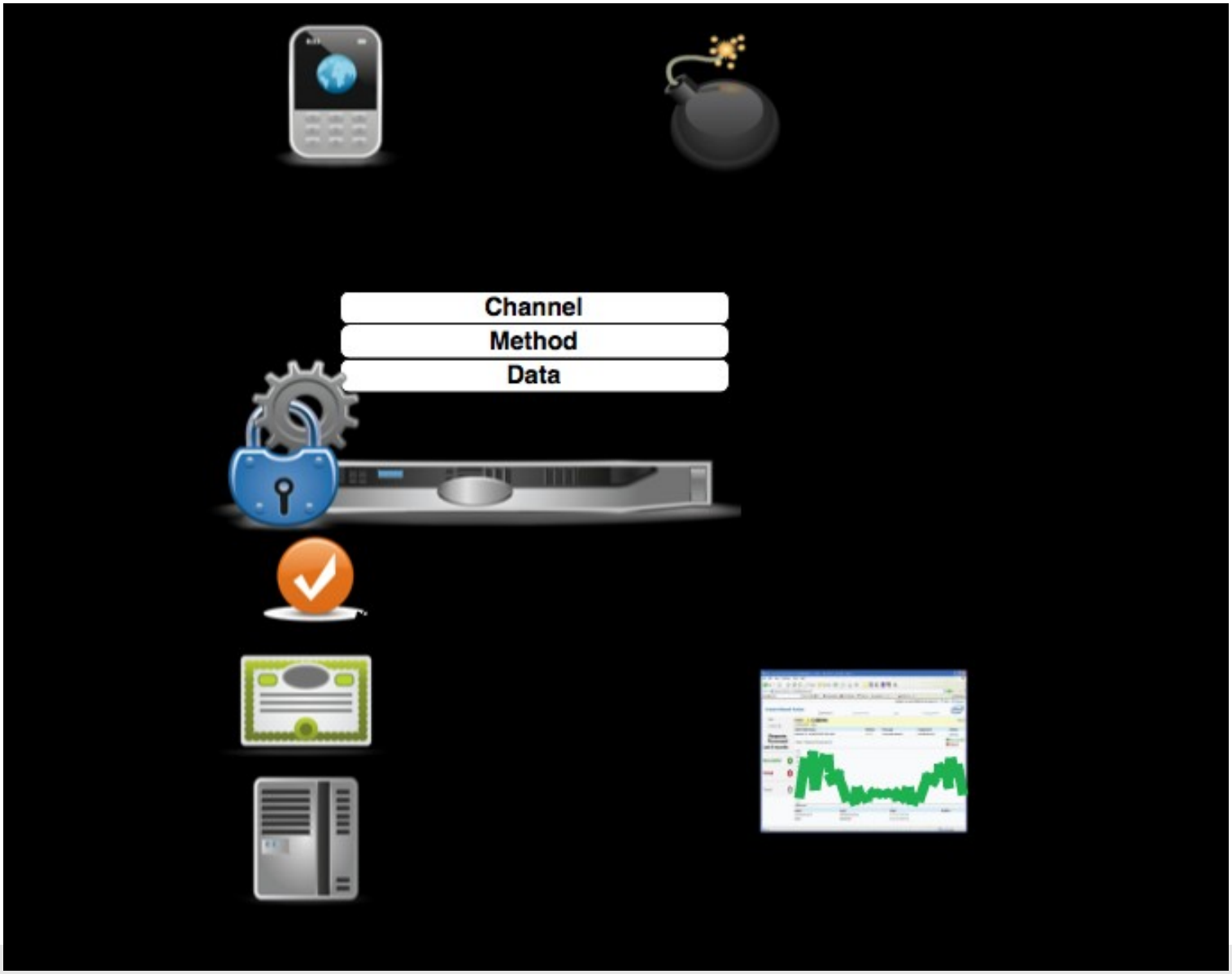
Point of Entry for Private, Public, Hybrid Environments

Policy Enforcement Point

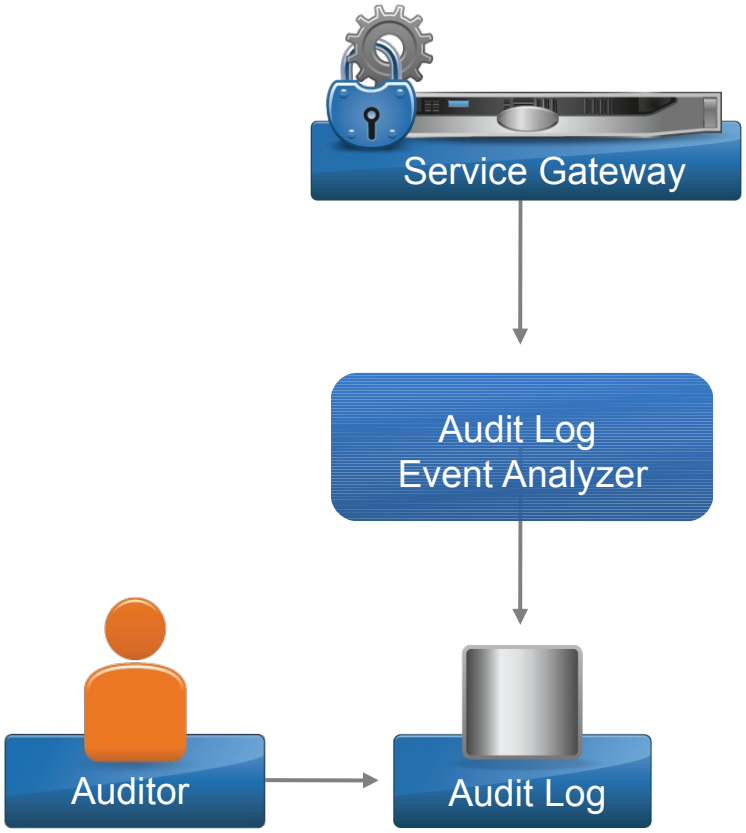


The gateway model enforces delegated authentication and authorization

Using a Gateway for Defensive Programming



Audit Logging



Who was involved?

What happened?

Where did it happen?

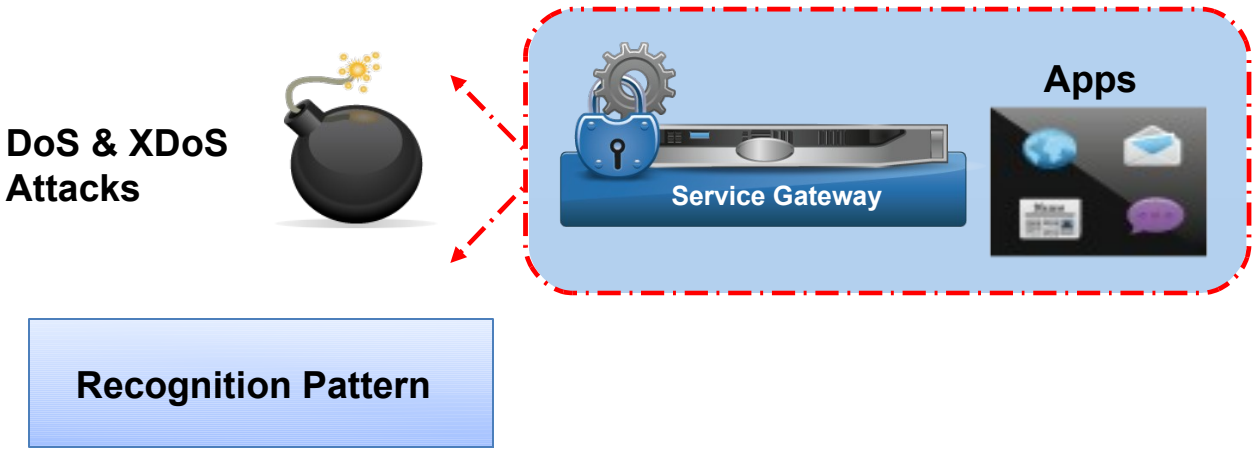
When did it happen?

Why did it happen?

How did it happen?

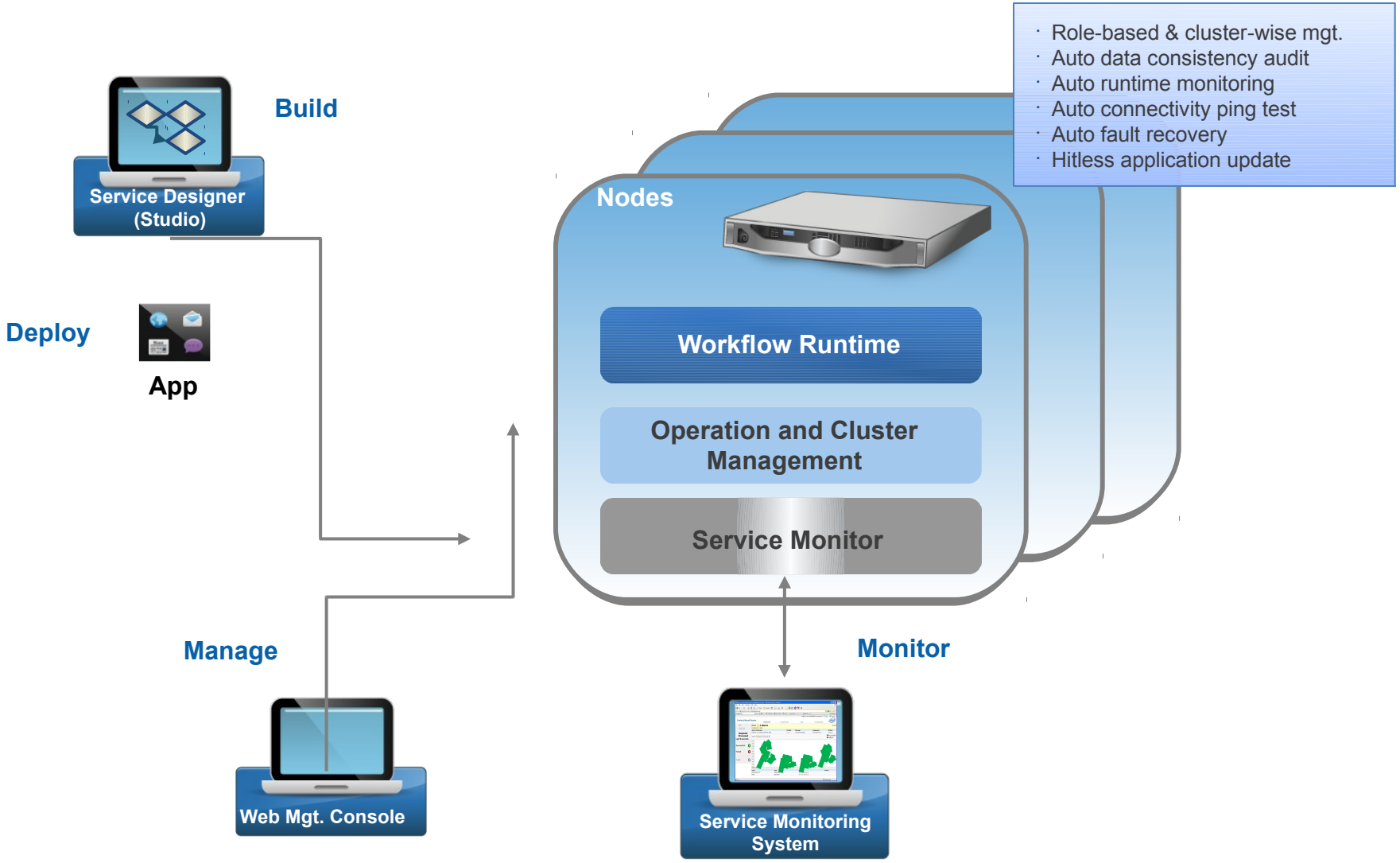
Service gateways can capture every detail

DoS Protection



- In addition to network-based DoS, Web services are vulnerable to XML Denial of Service attacks, such as:
  - Parser exhaustion: target DOM, Sax processing power
  - Large documents and binary blobs
  - XML Structural attacks

SOA Expressway System Architecture



Intel® SOA Expressway

SOA Soft-Appliance

or

Virtualized Appliance

or

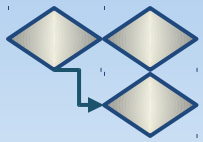
Tamper Resistant Hardware Appliance

Protocol Agnostic
- REST.,SOAP
- XML, Non-XML
- HTTP, FTP, TCP

Performance
- 2x hard appliances
- Tie-in to chip roadmap
- Efficient XML parsing at machine level

Secure
- Tamper proof appliance
- Common Criteria
- XML Firewall
- AAA integration

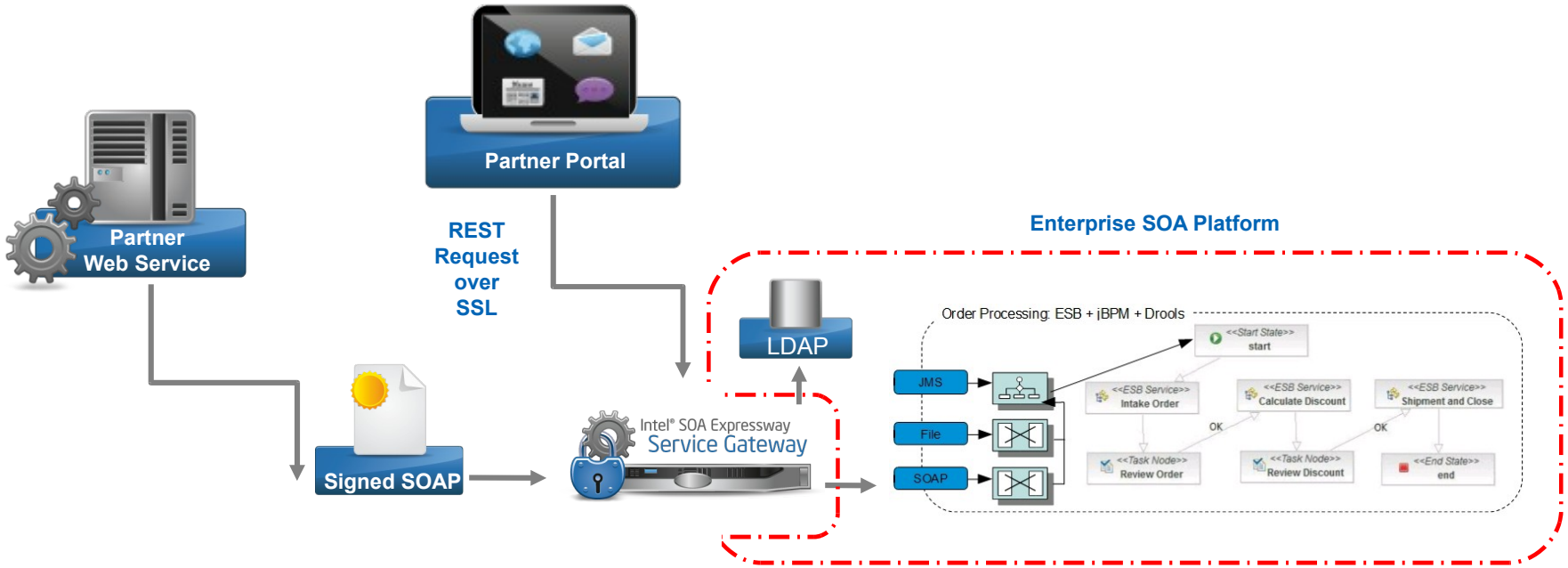
No Programming
- Simple visual environment



Flexible
- Routing
- Transform
- Validation
- Service Call-outs
- Firewall Rules

Available on all major operating systems

Demo: Enterprise SOA Middleware Platform



- SOAP Firewalling
- DoS Protection
- Runtime Policy Enforcement
- REST to SOAP Mediation
- Authentication
- Throttling, Auditing and Logging
- Separation of Concerns
- Massive Scalability

SOA Expressway securely exposes Jboss SOA 5 to all types of business partners

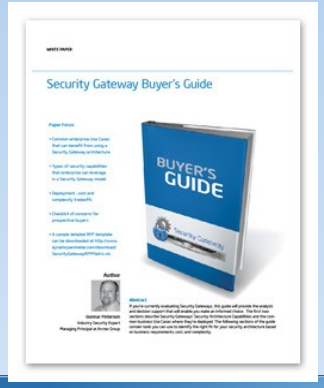
Part 4 - Live Gateway Demonstration

Perimeter Security Scenarios

- Security Policy Construction
- Web Services Security
- Content Attack Prevention
- AAA – SAML
- Denial of Service Prevention
- REST Security
- Content Attack Prevention
- REST-to-SOAP Mediation
- Digital Encryption
- Token Exchange

Regain Control...Secure the Dynamic Perimeter

Additional Information



Buyers Guide

"Advanced Threat Mitigation" Webinar

www.dynamicperimeter.com