



Identity-Driven SOA

The Yin and Yang of SOA and IdM

Anne Thomas Manes
VP & Research Director
Burton Group
atm@burtongroup.com

10 January 2008





Identity-Driven SOA

Thesis

- SOA environments are complex ecosystems
 - Security threats and requirements are equally complex
- Requires a comprehensive strategic approach
 - Combination of perimeter-based and identity-based protections
 - Layered defenses
 - Policy-driven
- Externalize security to infrastructure whenever possible
 - Don't leave security to the whim of the developer
- BTW – it requires a solid IdM solution to be in place



Identity-Driven SOA

Agenda

- Problem statement
- Recommendations



Problem Statement

Security is really hard

- Threats:
 - Message integrity, confidentiality, falsified messages, man in the middle, principal spoofing, forged claims, message replay, denial of service, content-borne threats, schema poisoning, code/content injections, fraud
- Requirements:
 - Entity authentication, data authentication, authorization, auditing, data protection in motion, data protection at rest, message uniqueness, message validation, content scanning, monitoring, management and administration, client provisioning, trust management, federation, compliance, and eDiscovery
- Can't expect every developer to understand it all
 - Requirements change at a different pace than the applications

What's different about SOA?

- Services aren't constrained to a single point of entry
- App-to-app communications (no humans)
- Heterogeneous authN and authZ mechanisms
- Mediation and loose coupling expose more vulnerabilities
 - Adds complexity to the trust relationship
- Need to capture multiple identities for auditing
 - Original requestor, data provider, intermediaries, etc



Problem Statement

Big challenges

- Administration and management
- Authentication and credential mapping
- Auditing
- Client provisioning
- Trust management and federation
- Threat and fraud detection
- Governance
- Compliance and eDiscovery



Identity-Driven SOA

Agenda

- Problem statement
- Recommendations



Recommendations

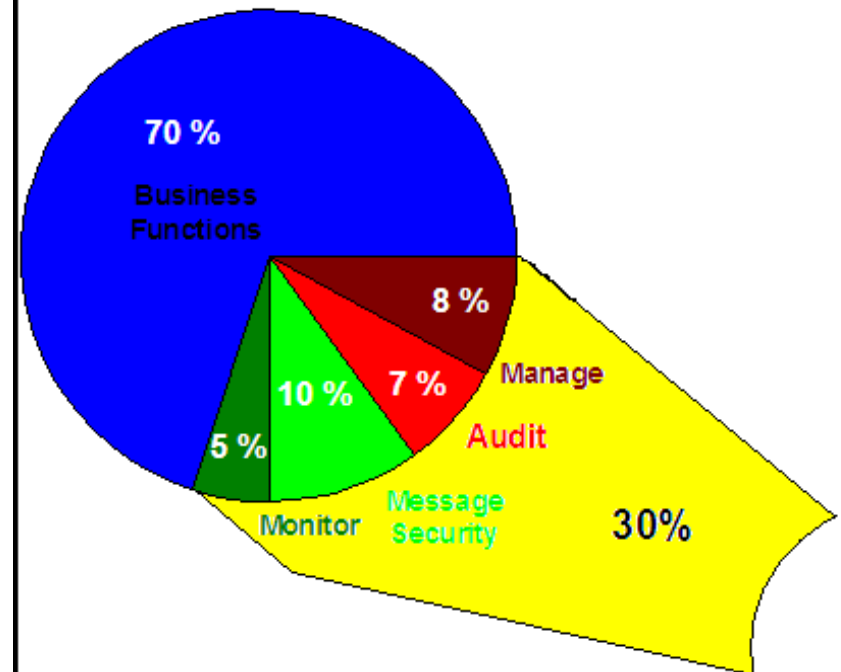
Adopt a strategic approach to SOA security

- Externalize security to the infrastructure
 - Let the infrastructure manage communications
- Configure security protections using policy
 - Centralized administration
- Use layered defenses
 - Perimeter and identity-based protections

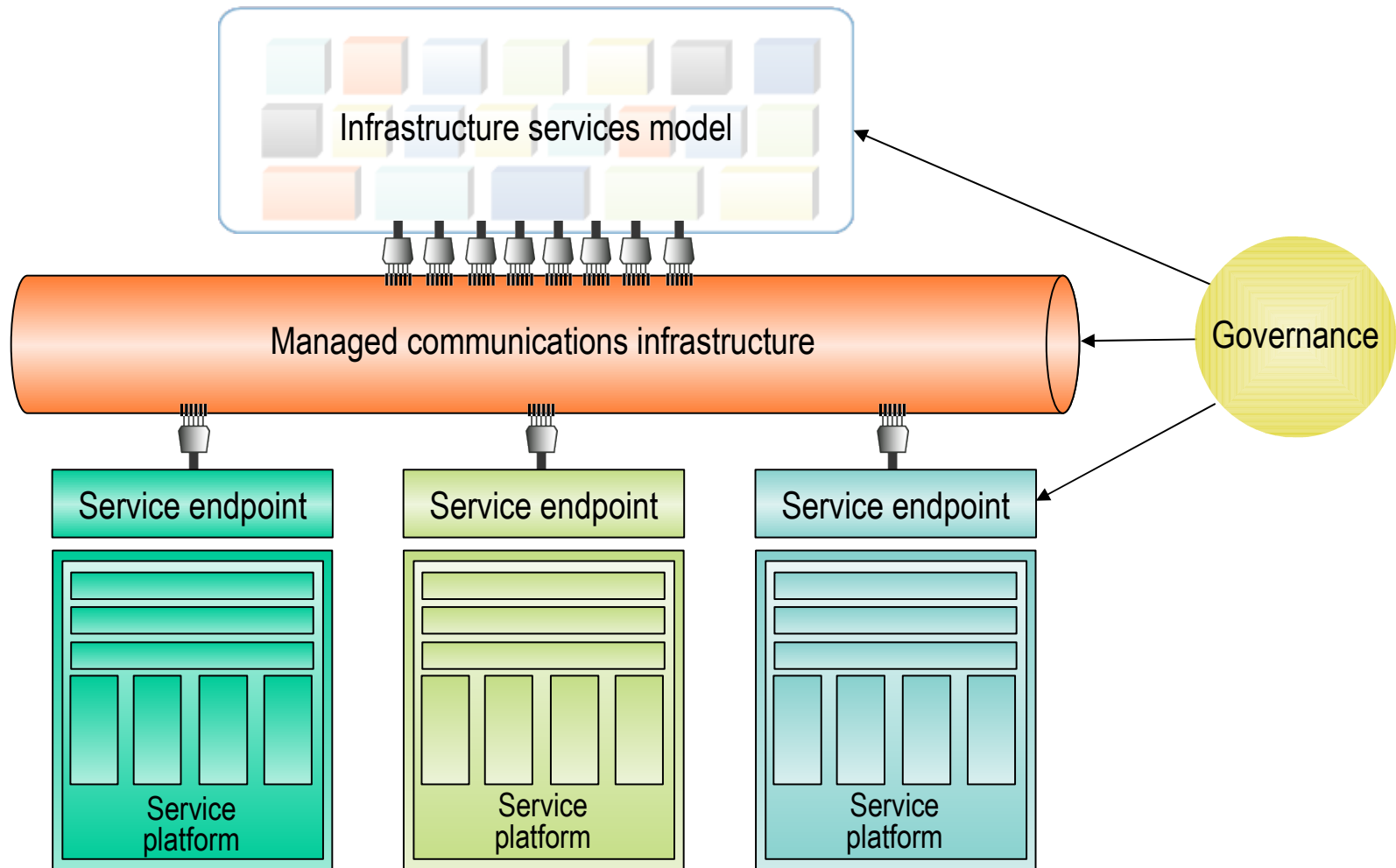
Externalizing security

- A F50 financial conglomerate estimates it can save up to 30% of annual IT budget by standardizing and externalizing security
- Extra benefit: improves consistent enforcement of corporate security policies

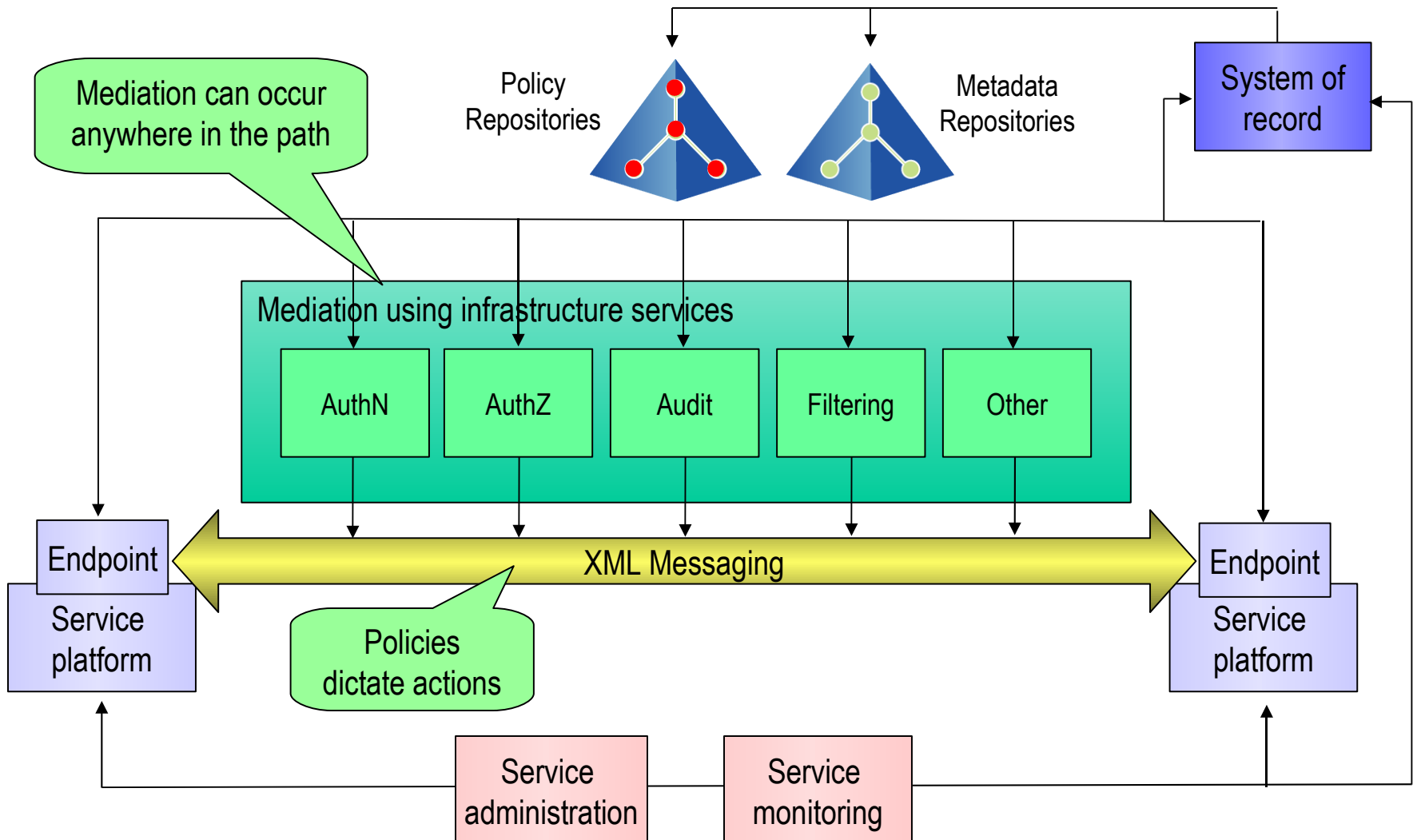
Total Cost of ownership for developing and operating our automated business processes



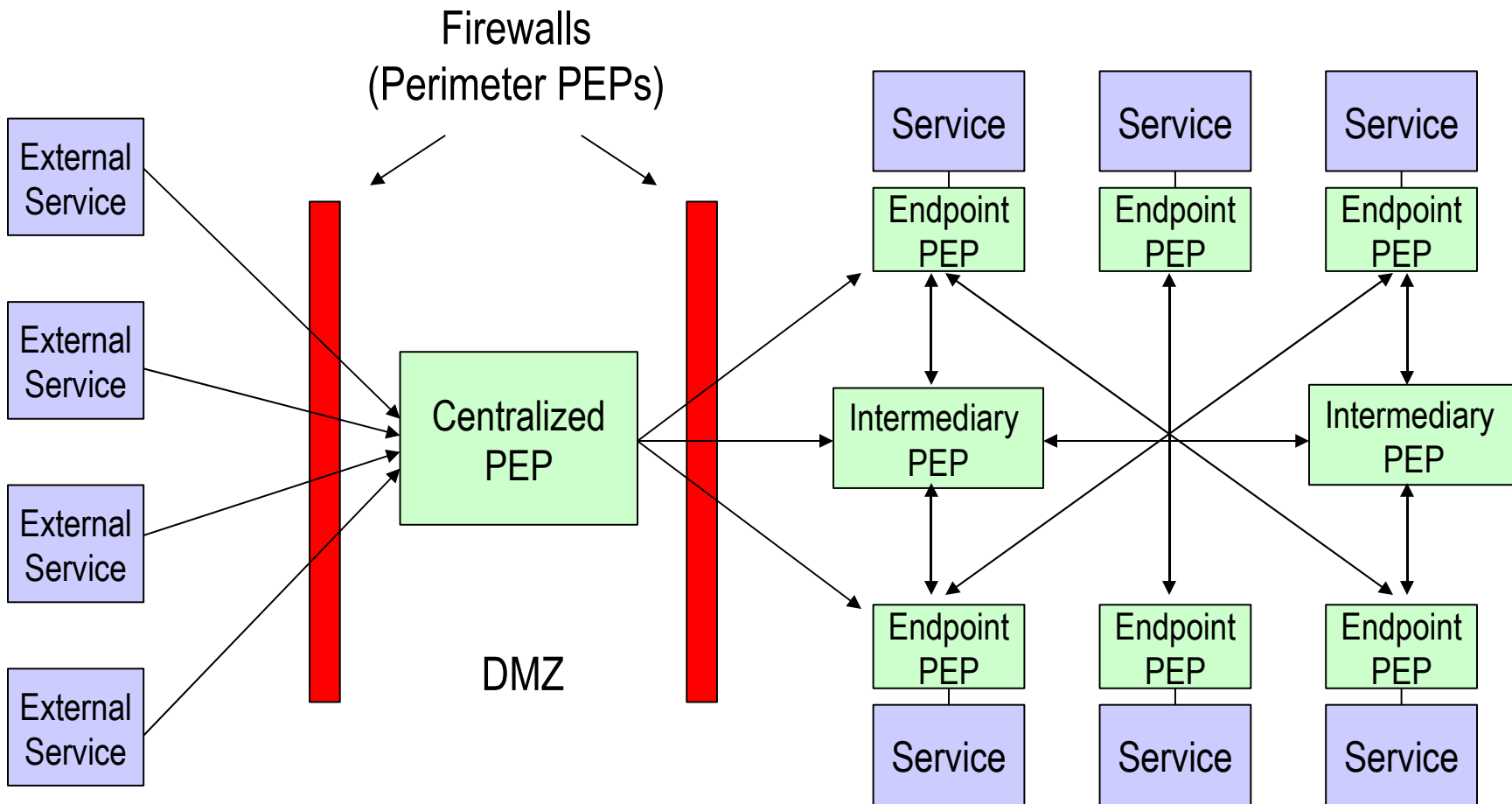
Conceptual model



Functional model: Managed communications infrastructure



Layered Defenses





Conclusion

- SOA environments are complex ecosystems
 - Security threats and requirements are equally complex
 - Don't leave security to the whim of the developer
- Externalizing security increases flexibility and consistency
 - Also reduces costs and time-to-market
- Adopt a comprehensive strategic approach to security
 - Combination of perimeter-based and identity-based protections
 - Layered defenses
 - Policy-driven
- SOA protections depend on a solid IdM strategy