

# Security for Service Oriented Architecture (SOA)

## Effective Security Policy Management for Modern Agile IT Architectures

### Service Oriented Architecture (SOA)

Service Oriented Architecture (SOA) is based on the idea that all IT assets are made available across a network as reusable “services”, which can be accessed via standard protocols and interfaces, and platforms (e.g. Web services and eXtensible markup Language, XML). Moreover, ownership of individual SOA IT services can be directly traced to a business owner and the overall enterprise architecture. One main goal is to be able to flexibly “plug together” services to meet changing business demands, using business-workflow based Business Process Modeling (BPM) suites.

Benefits of SOA include increased IT agility / flexibility and sustainable IT reuse, while maximizing IT cost-saving and return-on-investment. SOA also improves business / IT alignment and business-led ownership of IT assets. Furthermore, it can help consolidate IT assets, reduce complexity, and simplify IT & process changes.

### SOA Security

Unclear security implications are often high on the list of SOA issues that slow down SOA rollouts.

Some of the security concerns are:

- **Systems Get Opened-Up** Services are “opened up” to the outside world, which makes them an easier target for attacks than traditional siloed IT systems.
- **Security & Agility** Many traditional approaches to IT security are not well-suited to protect agile SOA IT landscapes. SOA landscapes involve potentially many services and many complex service interactions. that interact in complex, dynamically changing ways.
- **Expertise Gap** Many organizations today lack the expertise about agile SOA, how they affect security, and what security methods and tools are available. Due to this expertise gap, SOA is sometimes still wrongly perceived as relatively new, unpredictable and unmanageable.

As a leading SOA security expert, ObjectSecurity offers an in-depth study about SOA security (see website for more information) to help you close this expertise gap.

The two SOA security challenges that are perceived most significant today are:

- **Security Policy Management** Traditional security policy management tools and methods have been designed for static, siloed / stove-piped IT environments and do not support agile SOA landscapes well. ObjectSecurity’s OpenPMF has been specifically designed for low-maintenance, trustworthy security management of agile SOA landscapes.
- **Security Certification & Accreditation** Many government agencies (esp. defense agencies) face particular SOA security challenges because traditional assurance certification/accreditation practices assume relatively static IT environments, and therefore cannot easily be applied to agile SOA (e.g. Common Criteria). ObjectSecurity’s OpenPMF can help with SOA accreditation thanks to its “model-driven security” approach.



ObjectSecurity OpenPMF lets you intuitively select business-centric security & compliance policies, which are then automatically enforced across your IT landscape (using a “model-driven security” approach). You can conveniently manage your policies at run-time, and even change your software applications and workflows without extra administration. OpenPMF reduces costs, improves security, and enables agility. Available as a packaged product and as an integrated turn-key solution.

### Products & Services

- OpenPMF (packaged product & turn-key solution)
- SimulateWorld 4D synthetic environment toolkit
- SecureMiddleware: secure open source middleware
- Services: security policy management, Web 2.0 / SOA / Cloud / SaaS Security, middleware security, training workshop, tech. support, R&D
- Studies: in-depth documents about hot topics in security, e.g. model-driven security & SOA

[www.objectsecurity.com](http://www.objectsecurity.com)