

# Security for IT Managed Services Providers

## Security Policy Management for Customer Trust in Outsourced IT Managed Services

### IT Managed Services

Many organizations today are using or considering managed services to replace or complement their in-house IT services. Some of the main drivers include IT cost optimization, avoiding up-front set-up and hardware / software costs, reduce procurement risks, transfer of some of responsibilities, and reduced in-house training requirements. Examples of managed services include backup services, storage services, and the management of networks, users, and systems. Cloud services and Software-as-a-Service (SaaS) are managed services that go further by offering rich applications across the network with little or no installation needed on the client machine.

### Customer Trust is Critical

Security and trust are frequently mentioned as a show-stopper for the use of IT managed services. Building that trust requires state-of-the-art security controls and the ability to demonstrate security compliance to customers:

- **Building Trust & Confidence** Customers need to be confident that they can trust the managed service provider to handle their potentially sensitive information according to the agreed Service Level Agreements (SLAs).
- **Isolate Customer Information** Customers also need to be assured that their information is reliably separated from other service users, who could be potential competitors.
- **Legal requirements & jurisdiction** Customers need to be assured that their information is handled in line with legal requirements and jurisdictions. One example is the handing of privacy related information, which is regulated in many jurisdictions (including transmission between jurisdictions). For customers, outsourcing to a IT managed service does not automatically mean that the legal responsibilities are outsourced as well.
- **Service Availability** Customers are outsourcing control over their information and the services. It is important to ensure service availability at all times. Security plays part in this, for example to prevent or

mitigate denial of service attacks, data loss, and malicious data manipulation.

- **Service Delegation** In Cloud computing scenarios, IT managed services can themselves be composed from a number of other Cloud services from other providers. It is critical to ensure the security controls and SLAs extend through the entire service chain at all times.

### Security Policy Management

Many mature security mechanisms are available to protect information, segregate processing, segregate storage etc. However, one of the main challenges for IT Managed Services is how to reliably configure and enforce correct security policies across the large, interconnected, and ever-changing IT landscapes and datacenters. ObjectSecurity's unique OpenPMF security policy management technology helps solve this challenge:



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)