

Security for IT Management (CISO/CIO/CTO)

Align IT Security Policy Management, Enforcement & Audit Logging With Business & Technology Priorities

Aligning IT Security with Business Priorities

CIOs and CTOs need to ensure that processes, practices, and technology infrastructure support the flow of information throughout the organization as best as possible. This involves optimizing processes, architectures, and technologies, as well as the identification and development of new technical capabilities. Two main goals are IT cost & efficiency optimization, and the improvement of the organization through the use of technology. Several of today's CIO & CTO priorities revolve around real-time information sharing and fusion (e.g. business intelligence, business activity monitoring), IT consolidation, IT agility, and IT-business alignment. On a technical level, these priorities can be achieved through modern architecture approaches that allow the flexible, dynamic sharing of information across many interconnected users and "opened-up" systems and applications, e.g. using Service Oriented Architecture (SOA), Cloud Computing, SaaS / PaaS, and Web 2.0 / Enterprise 2.0.

New Security Risks

While significant productivity improvement and cost-saving can be expected using these modern approaches, they can also cause increased security risks due to the ever-increasing amount of sensitive information that is shared and which the business critically relies on.

Need for New Security Systems

Traditional security technologies and methodologies are frequently not suitable to meet those new challenges, mainly because they:

- only work within individual technology silos,
- do not allow for dynamic changes (agility & reuse),
- are unmanageable due to the scale and complexity of today's new IT landscapes.
- cannot easily be used in alignment with business priorities.
- make it expensive or infeasible to demonstrate security compliance to external auditors

Making Policy Management Manageable

Enterprise security policy management for today's complex, interconnected IT environments is a major challenge and cost factor in the form of manual labor, as

well as loss of productivity and functionality. This is because of a high degree of policy duplication across technology silos, and because policies need to be manually specified in vendor proprietary, technology-driven ways for many different silos. Moreover, policies need to be updated whenever systems change.

Improving policy management is therefore one of the most significant IT cost optimization opportunities: Using ObjectSecurity's OpenPMF, security policy management can be unified across silos and centralized external to applications, which results in significant cost savings, while at the same time improving security. OpenPMF's "model-driven security" approach enables security managers to define and maintain security control objectives in alignment with business thinking (i.e. alongside business process and enterprise architecture models) and with traceable IT security enforcement and incident monitoring across the operational IT landscape:



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