

Security for IT Modernization / Redevelopment

IT Cost Optimization & Simplified Security Management Across IT & Security Silos

IT Modernization

Many organizations today are faced with the need to close the gap between yesterday's IT implementations and tomorrow's IT demands, while planning, controlling and anticipating change due to generational shifts in technology, business pressures and IT skills. The main goals are to achieve optimized value, while reducing cost and risk. There are numerous drivers for IT modernization, such as:

- **IT Cost Optimization** Legacy systems are becoming increasingly expensive to keep up and complex to manage due to their often siloed and closed nature.
- **Legacy Reuse** Resources provided by legacy systems are usually siloed and cannot easily be integrated with current IT applications.
- **Business Changes** Changing business requirements demand additional features for the legacy systems. For example, privacy or auditing regulations require features most legacy systems do not offer.
- **Technology Changes** Generational changes to IT architectures often demands redevelopment or wrapping of legacy applications. For example, legacy applications may need to be enabled for Service Oriented Architecture (SOA), Business Process Management (BPM), Cloud / SaaS, and Web 2.0.

IT modernization involves an overhaul of the IT environment and culture to manage the ongoing, coordinated evolution of business processes, applications and supporting technology landscape. Typical solutions involve re-architecting or extending legacy applications (legacy redevelopment, refactoring, wrappers) to run on modern platforms. A more drastic alternative is to replace legacy applications with cost-effective state-of-the-art software (e.g. open source software).

Meet Modern Security Requirements

IT Modernization often involves opening up legacy applications to make them available to other applications (sometimes even across the Internet), which can make them susceptible to a wide range of attacks. Most legacy applications have not been designed for this changed scenario, and often do not have sufficient security built-in. In addition, security relevant regulations and best practices can become relevant due to the changes in use. While modern platforms can provide some level of security enforcement mechanisms, additional functionality may be required.

A particular challenge for IT modernization project is the consistent security policy management across these opened-up silos to reduce cost and risks, and to allow for future agile changes. OpenPMF is ideally suited for this purpose thanks to its broad legacy support, and its ability to reuse the models produced by redevelopment tools for its unique "model-driven security" feature:



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