

Security for the Logistics Industry

Coordination, Situational Awareness, and Collaborative Decision Making

Optimizing Throughput & Efficiency

Logistics industries always strive to optimize throughput, efficiency, cost-effectiveness, quality, and responsiveness, while minimizing staff / equipment downtime.

Many efficiency improvements in the logistics industry today are achieved thanks to state-of-the-art IT landscapes, which enable better, faster, and more automated scheduling / coordination, situational awareness, responsiveness, information exchange and collaboration. As a result, logistics firms today are critically dependent on the uninterrupted and correct function of their IT applications and infrastructure.

Security – A Critical Enabler

Security is a critical enabler for these logistics IT environments. Without it, logistics firms leave their core business vulnerable to financial, reputational, and legal / regulatory damage:

- **Ensure Availability and Reliability** The entire logistics business critically relies on the uninterrupted and correct operation of the IT environments. Security controls need to be put in place to ensure the IT landscape is protected from denial-of-service attacks or malicious information modification / loss.
- **Protect Sensitive Information** Many logistics firms frequently handle and share of commercially sensitive information, such as credit card details, customer usage patterns, fleet tracking information, shipped items tracking information. Security controls need to be put in place to restrict access to this information to only be available to authorized third parties.
- **Legal & Regulatory Requirements** Logistics firms frequently have to handle information that is regulated, e.g. by financial, privacy, or auditing regulations. Security controls need to be put in place, because non-compliance can cause significant financial and reputational damage.

Security Policy Management

Many mature security mechanisms are available to secure information storage and transmission, and to regulate access to it. However, one of the main challenges today is how to reliably configure and enforce correct security policies across the large, interconnected, multi-organizational, 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