

Security for the Manufacturing Industries

Managing Secure Information Sharing Across Interconnected Supply Chains

Information Sharing for Increased Efficiency

Most manufacturing industries always strive to maximize manufacturing efficiency, quality, and responsiveness, while minimizing staff / equipment downtime unnecessary stock-keeping etc. (e.g. Just-In-Time supply chain management and real-time mass product customization). Examples include the automotive, aerospace, semiconductor industries.

Often business process and supply chain efficiency improvements are achieved thanks to state-of-the-art IT landscapes, which enable better, faster, and more automated information exchange and collaboration.

Security – A Critical Enabler

Security plays a critical role in IT-enabling tightly interconnected supply chains. Without it, companies will not be prepared to rely on information from third parties for their own organization's success:

- **Ensure Availability and Reliability** The entire interconnected supply chain critically relies on the uninterrupted and correct operation of their 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** Manufacturing industries frequently handle and share of commercially sensitive information, such as confidential manufacturing specifications, release dates, lot sizes, and safety-related 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** Manufacturing industries frequently have to handle information that is regulated, e.g. by 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