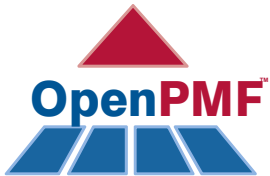


OpenPMF™

Making Application Security Manageable Through Automation



OpenPMF™ application security policy automation is key to reducing cost and improving security & compliance. OpenPMF™ offers manageable authorization policy automation for today's agile, interconnected applications – including those running on Service Oriented Architecture (SOA) and cloud computing platforms.

Why you need security policy automation

Most organizations today need to reduce cost and improve IT security & compliance at the same time, which is practically impossible without increased security automation. Manually translating security policy & compliance requirements into effective technical implementation is difficult, expensive, and error-prone - esp. for interconnected, agile applications (for example, built using SOA & cloud platforms):

- ▶ Where does the policy come from?
- ▶ Who can write the matching technical policy rules?
- ▶ Who can maintain them despite dynamic changes?
- ▶ Who can verify policy correctness & compliance?

OpenPMF automates policy management

With OpenPMF, you can automate managing application security policies for access control & auditing: automate the process of turning human-understandable security & compliance requirements into the matching numerous and ever-changing technical security policy rules and configurations. In addition, proactively enforce ("whitelisting"), and continuously monitor security the application layer. OpenPMF involves five steps: Configure, generate, enforce, audit, and update.

OpenPMF is critical for enterprise security

OpenPMF ("Open Policy Management Framework") makes application security manageable through automation. Its security automation forms a critical part of any authorization management, entitlement management and identity & access management (IAM)

strategy. OpenPMF also enables a secure application development lifecycle at development time right from the beginning – dealing with policy abstraction, externalization, authoring, automation, enforcement, audit monitoring & reporting, and verification.

OpenPMF offers unique automation

Unlike any other application security policy management product in the market, OpenPMF offers unique automatic policy generation (whitelists) and update from intuitive business security requirements - including least privilege and workflow policies, which protect from insider attacks. OpenPMF automates policy management even for agile SOA and cloud application platforms. OpenPMF automates security using unique award-winning and patent-pending model-driven security, advocated by ObjectSecurity's thought-leading founders since 2000.

OpenPMF has many benefits

OpenPMF helps develop, operate and maintain secure applications. It makes application security proactive, manageable, intuitive, cheaper, and less risky:

- ▶ Save time and money
- ▶ Adopt security easily & flexibly
- ▶ Align business, security, compliance, developers
- ▶ Improve proactive security & agility
- ▶ Adopt across many new & legacy technologies
- ▶ Proven technology since 2000

OpenPMF has many benefits:

1. Save time and money

- ▶ Security professionals focus on security
- ▶ Application professionals focus on the application
- ▶ Automatically generate & update application security policies

2. Adopt security easily & flexibly

- ▶ Development tool integration out of the box (Eclipse & Intalio)
- ▶ Multiple licensing alternatives and gradual adoption options
- ▶ No security expertise required

3. Align business, security, compliance, developers

- ▶ Allows business-centric security & compliance requirements to be captured in human/business "domain specific languages"
- ▶ Compliance with requirements can be demonstrated with confidence
- ▶ Removes technology and security silos, and reuses legacy
- ▶ Security & development separated, but linked via policy
- ▶ Comprehensive, fine-grained security auditing & reporting capabilities (white-listing prevents false-positives/negatives)

4. Improve proactive security & agility

- ▶ Security is enforced using whitelisting and blocking on the application layer
- ▶ Technical policies are updated at the click of a button whenever SOA/cloud application & interactions change
- ▶ Monitoring is continuous and based on whitelisting (no false-negatives/positives)

5. Adopt across many new & legacy technologies

Many technology integrations pre-built, others developed as needed for your deployment:

- ▶ XACML export: OpenPMF automation for other tools
- ▶ IDE: Eclipse IDE & modeling framework
- ▶ BPM SOA orchestration: Intalio BPMS
- ▶ Cloud PaaS mashup: Intalio Cloud
- ▶ Web app servers: Weblogic, Glassfish, Axis2
- ▶ Data Distribution Service: RTI DDS
- ▶ CORBA: Qedo CCM, MICO C++, JacORB Java
- ▶ Message brokers & MOM: ActiveMQ, XMLBlaster
- ▶ Firewall: IIOOP ObjectWall ("network PEP")
- ▶ IDS: Promia Raven
- ▶ Public Key Infrastructure (PKI): X.509
- ▶ Privilege Management (PMI): OMG ATLAS
- ▶ Directory Services: LDAP
- ▶ Databases: PostgreSQL (under dev.)

6. Proven technology since 2000

OpenPMF is proven, award-winning, patent-pending, and standards-based (incl. BPMN, XACML, Syslog, X.509, Ecore/MOF), with deployments including US Navy & Air Force, EU training systems for air traffic control & crisis management. ObjectSecurity is the leading company in the application authorization automation market since 2000, founded by renowned thought-leaders.

OpenPMF is used in 5 steps:

1. Configure intuitive business security requirements:

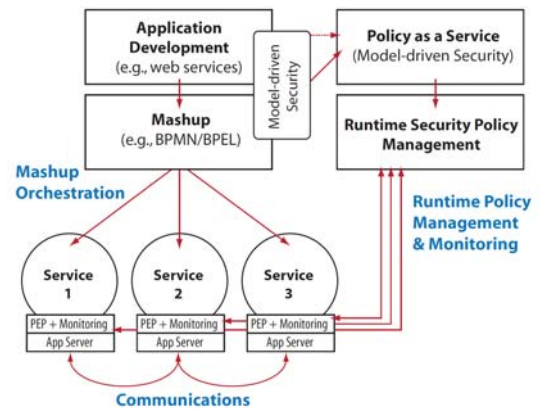
Security professionals can configure and audit generic application security requirements in OpenPMF, including access and monitoring policies. No need to be an application specialist.

2. Generate matching technical security policies automatically: Application developers can implement application specific technical application security at the click of a button. OpenPMF automatically analyzes your software as it is being written or updated, and generates fine-grained access and audit policies. No need to be a security specialist.

3. Enforce technical security policies transparently: At runtime, OpenPMF's local protection agents underneath all applications automatically intercept and check all application communications before they are forwarded to the application.

4. Audit technical security policies transparently: At runtime, OpenPMF also automatically monitors and collects information about security incidents for auditing purposes. The collected information can be configured through fine-grained audit policies.

5. Update technical security policies automatically: OpenPMF agile policy automation uniquely makes policy management and implementation manageable for today's rapidly evolving interconnected applications (e.g. agile SOA with BPM, agile cloud infrastructures).



Model-driven security: is the tool supported process of modeling security requirements at a high level of abstraction, and using other information sources available about the system (produced by other stakeholders). These inputs, which are expressed in Domain Specific Languages (DSL), are then transformed into enforceable security rules with as little human intervention as possible. It also includes the run-time security management (e.g. entitlements / authorizations), i.e. run-time enforcement of the policy on the protected IT systems, dynamic policy updates and the monitoring of policy violations.

Learn more: objectsecurity.com/download ▶