Whitepaper

ObjectSecurity OpenPMF™ 4.0 Security Policy Automation.

OpenPMF Security Policy Management Platform stops security breaches with powerful policy enforcement. OpenPMF™ makes security policy manageable through automation.

OpenPMF automatically bridges the semantic gap between human-intuitive, generic security policies and technical implementation: Author rich, generic, advanced policies. Automatically generate the matching technical rules & configurations.

Maximum security. Minimum effort.

This is why OpenPMF should be your overarching security policy management solution:

- OpenPMF is a security policy automation "umbrella" that lets you manage "one truth of the policy" in generic, expressive, intuitive terms
- OpenPMF imports existing information that makes policy automation easier, using its customizable importers
- OpenPMF generates and enforces the matching low-level policies across your IT landscape via its own enforcement infrastructure and via customizable exporters into third party products
- OpenPMF monitors security, and generates compliance documentation automatically.
- OpenPMF also lets you test policies before deployment.
- OpenPMF is robust and scalable regardless of the complexity of your IT landscape today and what it evolves to tomorrow.

Contents

objectsecurity.com
@objectsecurity
info@objectsecurity.com

Whitepaper

ObjectSecurity OpenPMF™ 4.0
Security Policy Automation.

Introduction: The future is now

Today's information age would have felt like out of a sci-fi movie to someone 20 years ago. More data has been created in the past two years than in the entire previous history of the human race. 1.7MB of data is created for every human per second. Within 4 years, we will have generated 44 trillion gigabytes of data, and will have 50 billion smart connected devices. Most of the data is managed by enterprise and governments. For example, a third of all data will pass through the cloud. Every angle of daily life of citizens, enterprise, and government is touched by IT.

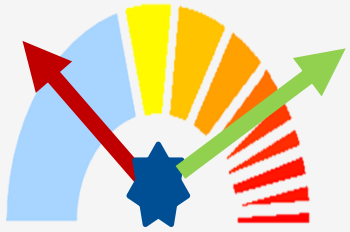
With that progress comes a great need to control access to data and IT systems. We increasingly rely critically on IT to work as expected and on data to be protected. Our physical safety, our health and well-being, our economy and business success, our national security and defense, and much more depend on it.

Conventional cybersecurity – not good enough anymore

Unfortunately, today's cyber security is simply not good enough to protect us, and our data and systems, from attack. This is shown by many high-profile hacks in recent times across pretty much all industries.

Because security is not good enough, many organizations cannot fully leverage the benefits of IT automation, and cannot protect well from breaches of their increasingly large and interconnected IT landscapes.

Incremental progress in the cybersecurity industry is not nearly fast enough to protect users and organizations from attack. To really 'move the needle forward', we need to change how we do security today.



Technical policy management – many challenges

Security policy management is hard

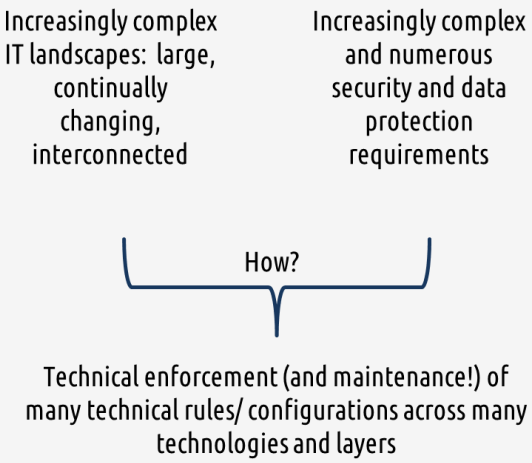
One of the key problems for enterprise (and governments) today is that it is difficult to figure out and manage security requirements. Once these so-called "enterprise security policies" are figured out, it is even harder to technically implement them so they actually protect today's complex, interconnected IT landscapes. There is a large gap between how human security professionals think about security policies, and how technical systems implement them. This is especially true for access control policies, which lie at the heart of cybersecurity.

When securing your organization, including both users and your interconnected IT systems, are you going to manually configure & maintain all security rules and configurations everywhere?

Access Control is hard to manage

In particular, it is hard to manage and implement access control that gives everyone (and every device) the access they need but no more, because this requires many complex, dynamic access rules. Historically, it has been terribly painful or just plain unmanageable. 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 and compliance?

There are too many overlapping rules and configurations in too many places, and too many changes to do this manually. Also, the security policies you actually want are too complex to maintain manually across many systems, and they often do not even support the implementation of the policies you wanted. For example, user identities, roles and privileges need to be configured and maintained with Identity & Access Management (IAM) systems. Additionally, firewalls rulesets and other network equipment, operating systems security, database security, application security, web security etc. all need to be configured and secured in their own right.



Too hard to do it manually

Today's overworked IT departments do not have the resources to author and maintain too many technical access rules, or manually integrate tools into their IT landscape. Security administrators are facing a "lose-lose" situation, especially for access control: Either, today's security tools help implement access control that is too simplistic to actually reflect the enterprise security policies. For example, today often inadequate access controls are implemented (often purely based on identities and roles). Or they try to manually implement enterprise security policies, which is unmanageable, especially because today's connected IT landscapes are ever-changing and evolving. It is also not auditable. And human configuration errors happen - the needed policies are too hard to author and maintain and too hard to technically integrate and implement. Multi-$bn are wasted every year world-wide in staff and consultants costs, and costs of security breaches and non-compliance.
Of course enterprises already have a bunch of tools available to manage access, especially identity & access management products. However, these are better at managing things like identities, roles, authentication, account provisioning and deprovisioning etc. Most of them are not so useful for managing access control policy rules. And the access control they can provide is usually not very adaptive, and cannot be enforced consistently across today's typical hodgepodge IT landscape. On the other end of the spectrum, there are some fine-grained access control vendors, but they are often unmanageably complex, requiring administrators to manage complex and numerous access policies.

What's needed: Policies for humans, and policy automation.

How humans 'do policy'

Access control needs to be human-manageable and adaptive, meaning decisions are based on dynamically changing context. Humans think of security policies in few concepts that are non-technical, concise, general, and rich. Machines, on the other hand, are good at processing the opposite: many detailed, specific technical rules and configurations.

At the core of the problem is that humans intuitively "think policy" differently. When you abstract away the underlying technical complexities, the policy that you wanted isn't usually all that complex and long if you author it in human-intuitive concepts and terms. Humans are usually better at expressing policies in intuitive, "undistorted", non-technical concepts, in general concepts, and in rich concepts (rather than in detailed technical terms). Policies get much simpler for humans this way.

How humans 'do policy'

- Non-technical, concise concepts
- Few policy rules
- Imprecise
- General concepts
- Rich concepts

How machines 'do policy'

- Technical
- Many rules in many places
- Precise
- Many details
- Specific, often simple concepts

The need for security policy automation

So what's the solution? Wouldn't it be logical to use an automated tool to bridge the gap between human-manageable, intuitive policies and the matching detailed technical rules and configurations. This would allow security administrators to author policies in very generic terms. The tool should then automatically fill in the technical details, and enforce the policy.

For example, administrators should be able to author policies such as:

- "only allow a selection of the detected information flows and block everything else"
- "all analysts can access all data about any suspect they are tasked to investigate, and about all other suspects that are within 3 hops social proximity of that suspect"

Such a "security policy automation" solution needs to automatically bridge the gap between such human-understandable, intuitive policies and the matching detailed technical rules and configurations. It should automatically generate technically enforceable technical rules and configurations (esp. for access control policies). It should also automatically test policies, produce documentation, and monitor security activity.

How would such a tool achieve security policy automation? By importing existing information sources, and using them to fill in the technical details. For example, it could import information about users, roles, applications, systems, networks, network traffic, and much more.

The remainder of this whitepaper describes how ObjectSecurity OpenPMF™ 4.0 security policy automation helps you achieve such powerful security policy implementation with effortless management.

ObjectSecurity OpenPMF™ 4.0 Security Policy Automation

Powerful security policy implementation, effortless to manage

OpenPMF is the "umbrella" for IT access control management. It allows organizations to implement powerful access policies with organization-wide consistency in a way that is easy to implement, manage, audit. It reduces risk/costs, improve security, improve compliance, and enable smarter organizations.

OpenPMF automatically bridges the semantic gap between human intuitive generic security policies and technical implementation. Author rich, generic, advanced policies. Automatically calculate the matching technical rules & configurations.

Unique features

ObjectSecurity OpenPMF lets you easily author generic and advanced security policies. It enables you to maintain "one truth" of the undistorted, feature-rich, expressive policies. OpenPMF automatically calculates the matching technical rules & configurations for the underlying IT landscape, integrating either via OpenPMF's own enforcement software agents, or via rapidly customizable exporters to configure third party products.

OpenPMF is powerful and scalable: such generic policies will not need to be changed often, even if your IT landscape changes! OpenPMF simply re-calculates the technical updates for you!

Unlike competing technologies, OpenPMF makes advanced access policies both manageable and implementable. It integrates out of the box with numerous standards and technologies, and automates much of policy authoring and enforcement.

Unique benefits

OpenPMF helps you implement and manage better access policies: you can robustly implement the necessary access control policies across your IT landscape based on rich, customizable attributes including location, time and context.

OpenPMF makes access control mode effective, auditable and manageable across your interconnected IT landscape for all stakeholders. It reduces cost, and improves security and compliance. It also speeds up and simplifies security implementation, maintenance, and testing. It is often implemented as part of Identity & Access Management (IAM) initiatives, which all major enterprises and governments have.

OpenPMF has been deployed for over a decade across several industry verticals. ObjectSecurity as a vendor is here to stay: The company has been in the market for 16 years. Our flexible "OpenPMF" product is available as an on-premises product and a flexible SaaS service. It can be customized, to import whatever information sources you have, and to export access control policy configurations into whatever applications and systems you have.

What you can do with OpenPMF™ 4.0 Security Policy Automation

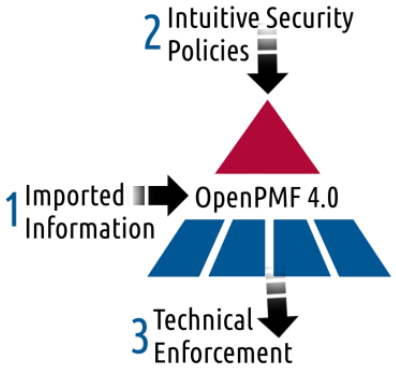
OpenPMF™ Makes Security Policy Manageable Through Automation.

ObjectSecurity's OpenPMF security policy management platform stops security breaches with powerful policy enforcement. It gives you powerful security policy implementation that is also effortless to manage.

It allows you to improve protection, monitoring, testing, and documenting – for your information, users and devices. OpenPMF™ turns human-manageable security policies automatically into the matching preventive technical implementation.

OpenPMF lets you manage security policies in customizable terms that matter to your organization. OpenPMF ensures policies are manageable even if IT landscapes are large and change dynamically. The result is a significant cost saving, especially with respect to maintenance.

How OpenPMF security policy automation works:



1. **Import information** about your organization, including systems/applications, data flows, users, alerts etc.

2. **Import** your existing technical **policies** as a baseline, for example access control configs

3. **Author** security policies that are intuitive, generic, rich, customizable

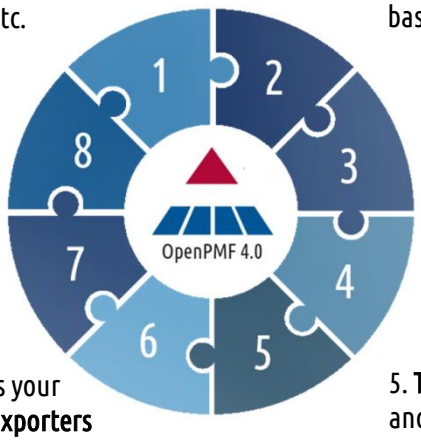
4. **Generate** technical enforcement rules & configurations, for example access control

5. **Test** using formal model checker methods, and **document** for audit & compliance

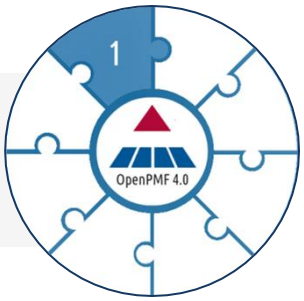
6. **Enforce** consistent "defense in depth" across your IT via **OpenPMF's enforcement** and **3rd party exporters**

7. **Monitor** policy enforcement alerts centrally to help policy management & remediation

8. **Update** technical enforcement automatically if your IT changes and **customize** OpenPMF



What you can do with OpenPMF™ 4.0 Security Policy Automation



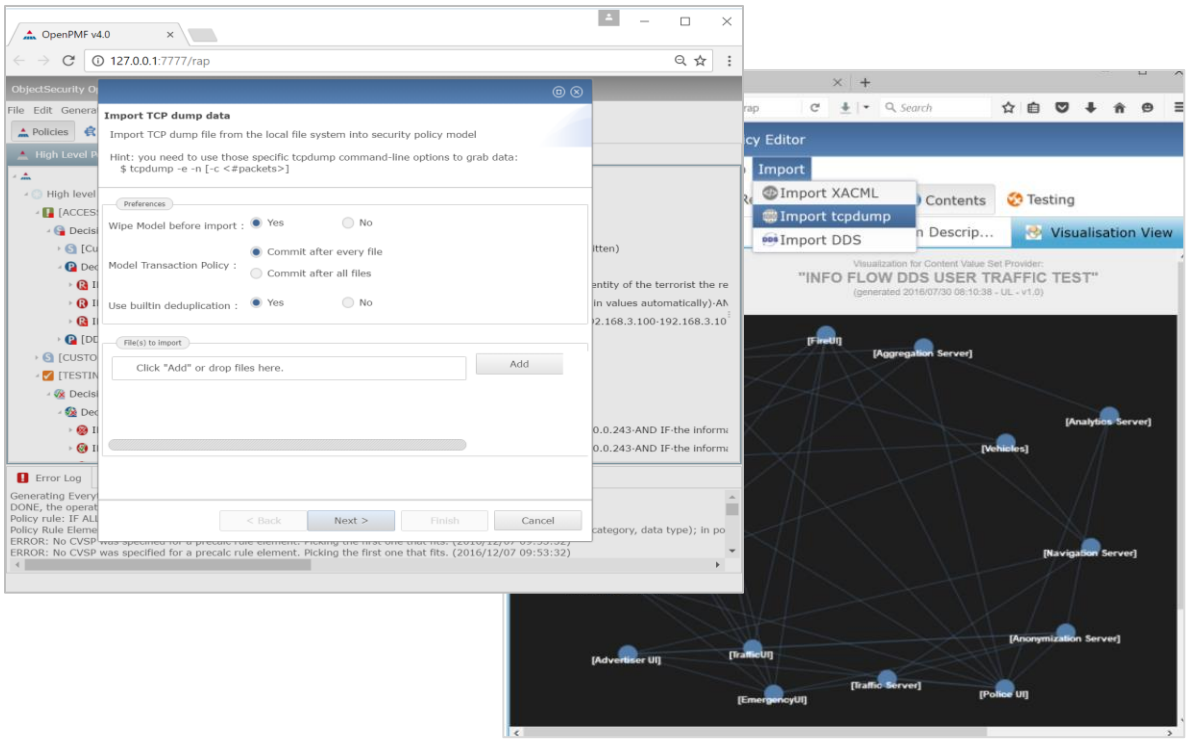
1. **Import information** about your organization, including systems/applications, networks, data flows, users, alerts etc.

OpenPMF has a rapidly customizable, standards-based importer interface that lets you import various information sources, which simplifies policy authoring: OpenPMF then lets you author policies in generic terms, referring to selections of imported data. For example, you can allow only certain information flows between certain applications, or between certain systems. Such rule elements can be combined with other rule elements, including user identities, roles, proximity, and more.

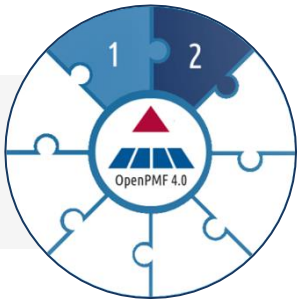
The crucial benefits are that the authored policies are simple and generic, and do not have to be changed if the imported information changes. OpenPMF simply detects the changes when re-importing and updates the policies accordingly.

OpenPMF supports many importers out of the box. For example, you can import information about your networks and applications using OpenPMF's network traffic log importer. Or you can import information from your identity management system via LDIF. Or import security alerts from Syslog. The imported information can be analyzed, selected, and visualized conveniently in a user-friendly UI.

OpenPMF's ingestion of those other information sources is also easily customizable so you can import your particular organization's information.



What you can do with OpenPMF™ 4.0 Security Policy Automation



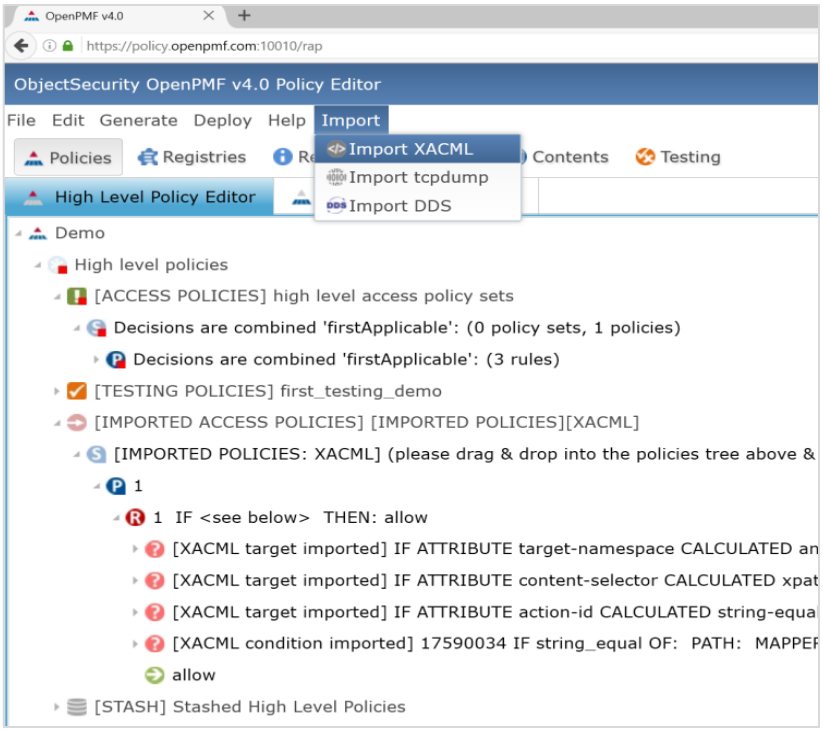
2. **Import** your existing technical **policies** as a baseline, for example access control configurations

As already described, OpenPMF has a rapidly customizable, standards-based importer interface that lets you import various information sources making life easier during policy authoring.

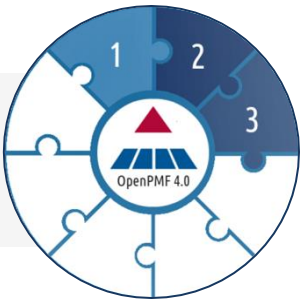
In order to ensure you do not have to start from scratch, OpenPMF allows you to import existing security policies that are in place throughout your IT landscape.

For example, you can import:

- access policies specified in OASIS XACML
- policy information from identity management systems (via LDAP LDIF)
- network security policies defined in host firewalls and domain boundary controllers (iptables etc.)



What you can do with OpenPMF™ 4.0 Security Policy Automation



3. **Author** security policies that are intuitive, generic, rich, customizable

OpenPMF lets you author policies in generic, intuitive, rich concepts, using terms you choose. Security professionals can easily edit "high-level" access control (and other) policies in OpenPMF's easy-to-use, flexible policy editors (graphical editor, and smart text editor). Users only have to author a few intuitive, generic "high-level" policies compared to the multitude of technically enforced "low-level" policies, making OpenPMF a solution that saves money and time.

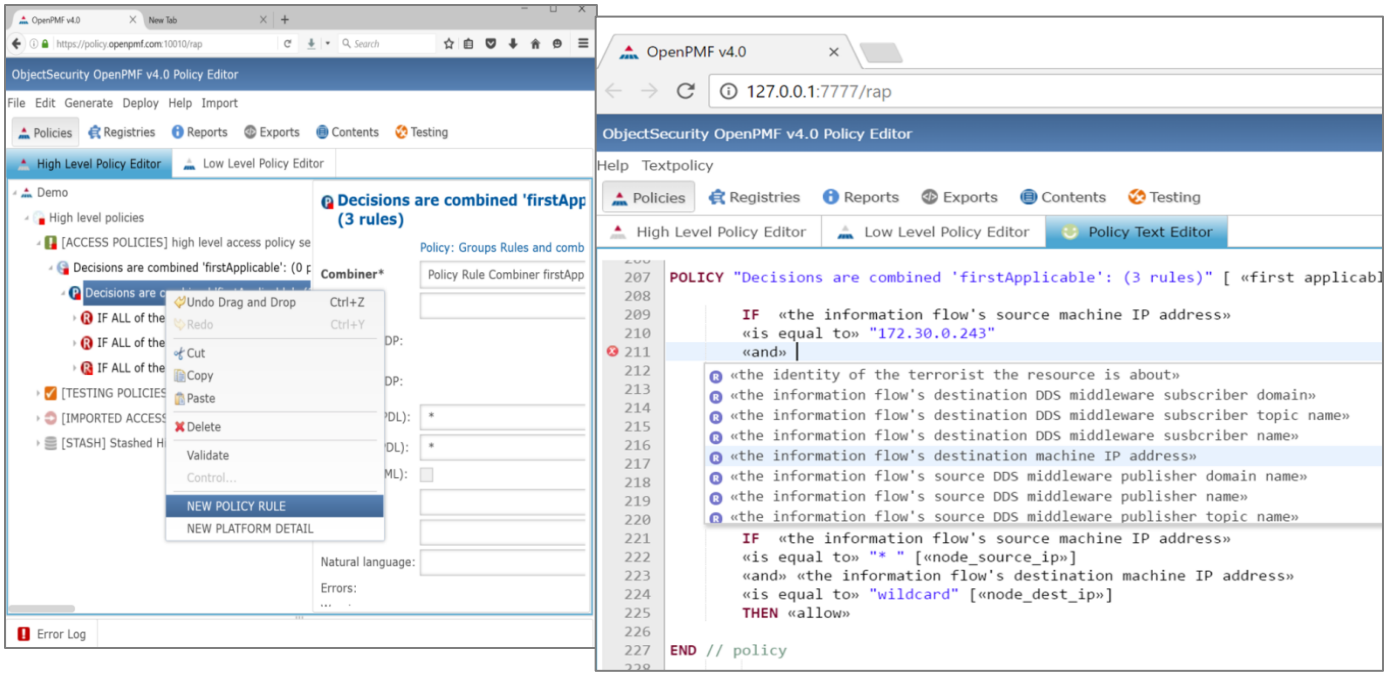
OpenPMF even allows you to write policies using attributes and rule elements that are not readily technically enforceable, and automatically calculates mappings to technically enforceable, available attribute sources, calculation sources, and mapper sources.

For example, if users want to author policies that grant or deny access based on whether the requestor's current location is in the US or EU (e.g. for privacy enforcement), but only the geolocation can be obtained from the request context, mappers can be integrated into OpenPMF that map between US/EU, country code, and geolocation.

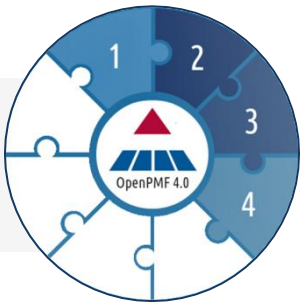
As another example, you can automatically "whitelist" application interactions that have certain characteristics and block anything else. This unique feature empowers users to author policies in more generic, intuitive terms without going near the complex, numerous low-level technical policies.

The 'vocabulary' used to author policies, such as attributes and calculations, is fully customizable, and the corresponding data can be flexibly imported from your organization's existing data sources (e.g. HR systems, logistics systems, task management systems).

The web-based editor and the underlying data models are standards based. The editor itself auto-configures after even a major customization of OpenPMF, resulting in a rapid and straightforward implementation.



What you can do with OpenPMF™ 4.0 Security Policy Automation



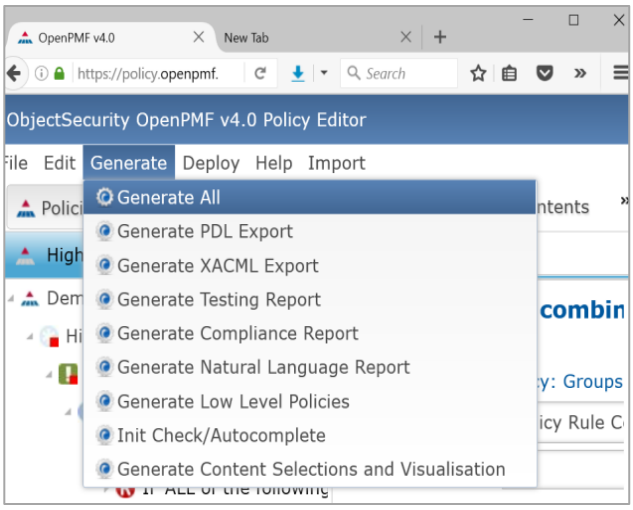
4. **Generate** technical enforcement rules & configurations, for example access control

OpenPMF automatically generates "low-level" technical policy implementation from the authored generic, intuitive expressive "high-level" policies and other - ideally already existing - information sources.

During the generation process, OpenPMF uniquely bridges a “semantic gap” between the human-intuitive high-level policies and the matching low-level technical policies.

The benefits are that the high-level policies:

- remain undistorted from the technical details of the underlying IT landscape; and
- do not have to be updated if the technical details of the underlying IT landscape change (such as. re-configuration of interactions, user role updates etc.)

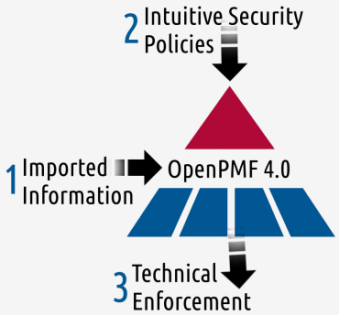


How OpenPMF security policy automation works:

The technical approach behind this process is called “model-driven security”, which applies the concepts behind model-driven development and semantic approaches to security.

“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.”

- Wikipedia



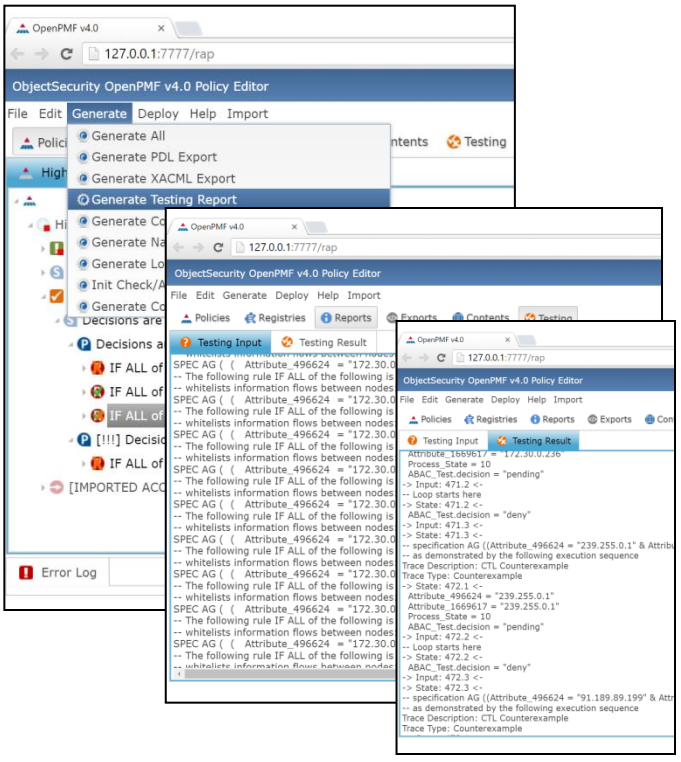
What you can do with OpenPMF™ 4.0 Security Policy Automation

5. **Test** using formal model checker methods, and **document** for audit & compliance

Test using formal model checker methods

OpenPMF includes an advanced policy testing feature based on formal methods (symbolic model checker, combinatorial testing). Users can simply author policy properties they would like to test for (in the context of imported information about systems, information flows, users etc.). Users can then simply run a test that proves/disproves whether policies will have the intended effect.

This feature uses a formal combinatorial model checker. It is based on years of scientific development by the National Institute of Standards and Technology (NIST). ObjectSecurity won Phase 1 and phase 2 of a NIST SBIR to develop, extend, and commercialize this feature (see objectsecurity.com/nist).



Document for audit & compliance

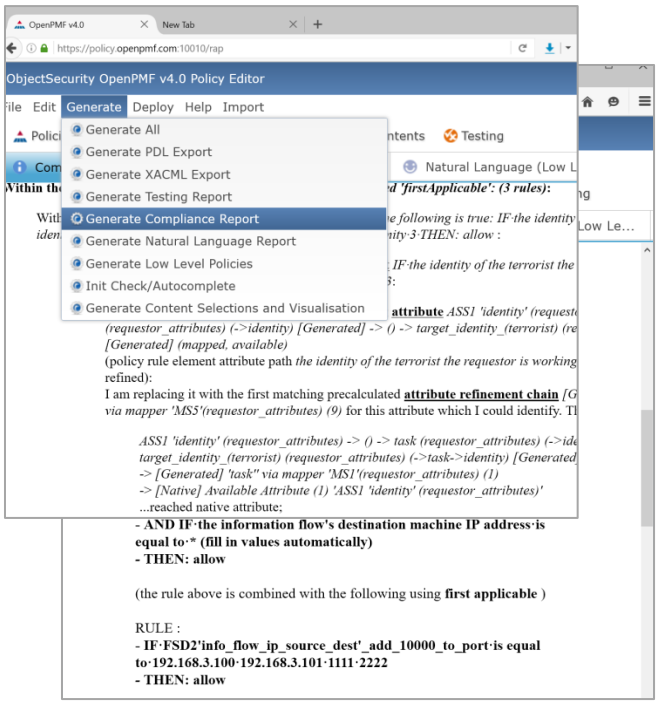
Regardless of their technical acumen, OpenPMF's documentation feature provides users with a straightforward and easily understood documents about the policy and its implementation.

Natural language documentation

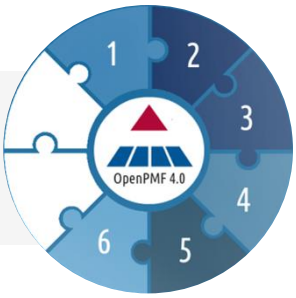
OpenPMF automatically generates a natural language document about your policy at the click of a button. This version of the policy is easy to read and understand, making it easier to understand the policy.

Compliance documentation

OpenPMF automatically documents every step its algorithms have taken in an a natural language report, which can be used by audit and compliance to understand how the technical policy was generated from the authored high-level policies.



What you can do with OpenPMF™ 4.0 Security Policy Automation



6. **Enforce** consistent "defense in depth" across your IT landscape – via **OpenPMF's enforcement –** and via **3rd party exporters**

OpenPMF's own enforcement infrastructure supports many technologies out-of-the-box, and other technologies on demand

OpenPMF comes with its own enforcement infrastructure, which includes a Policy Access Point (PAP) and local software agents (Policy Decision Points, PDPs and Policy Enforcement Points, PEPs) that can be installed on the to-be-protected systems or on network equipment. OpenPMF distributes technical rules to these software agents at the click of a button.

Each local software agent then intercepts information flows (e.g. all messages going in and out of its host system and applications), fetches the necessary information to make a decision, and enforces that decision. Decisions can be for access control ("allow"/"deny") decisions, monitoring ("log"), or customized actions.

OpenPMF supports manageable and effective Attribute-Based-Access Control (ABAC) security enforcement with push-button updating to protect systems that do not themselves provide adequate security features.

OpenPMF supports many technologies out-of-the-box, and other technologies on demand, including for example: host-based firewalls, OSGi middleware, web app servers, DDS, CORBA/CCM, SOA BPMS etc. (objectsecurity.com/supported-technologies).

Export & configure third party products and features using OpenPMF's rapidly customizable exporter

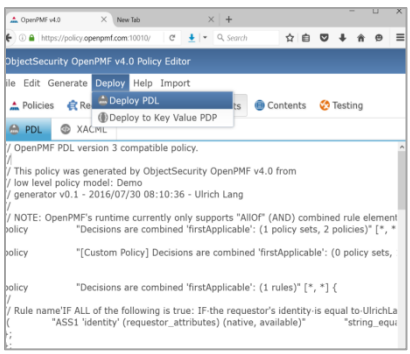
OpenPMF also has a flexible, rapidly customizable, standards-based export design that can be configured to export low-level policies into 3rd party security products and features.

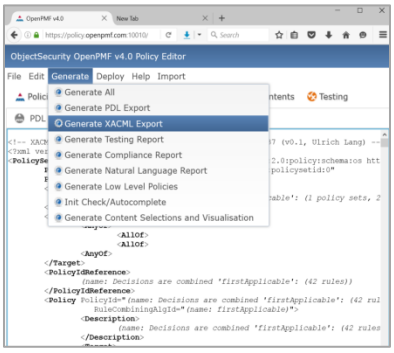
Thanks to this customizable exporter feature, OpenPMF can configure security of most systems and applications without the need to install software locally, thus saving time and money.

OpenPMF essentially becomes an overarching "security configuration management system" for the organization, which can be used alongside overarching Identity & Access Management (IAM) deployments.

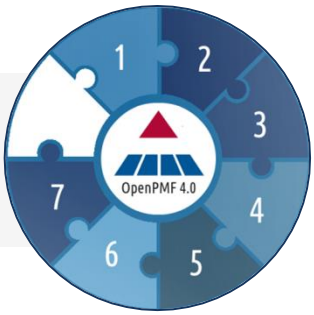
OpenPMF supports exporting configurations into many technologies out-of-the-box, and other technologies on demand, including for example:

- Host firewalls and network firewalls
- IDS/IPS (syslog)
- OASIS XACML
- Middleware security (e.g. OMG DDS Security)
- …





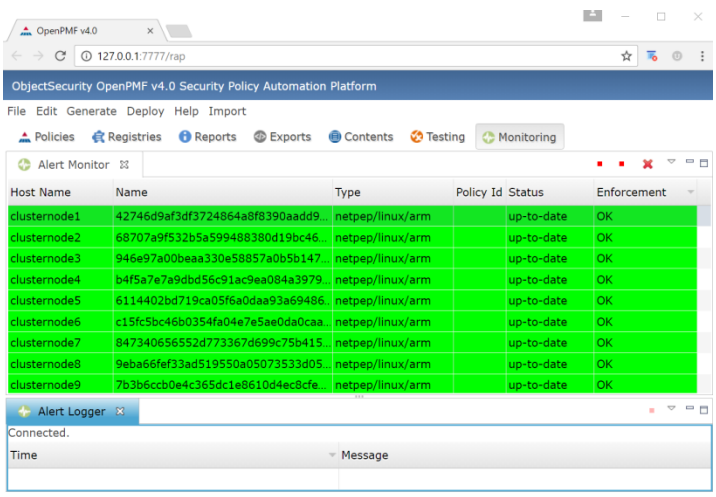
What you can do with OpenPMF™ 4.0 Security Policy Automation



7. **Monitor** policy enforcement alerts centrally to help policy management & remediation

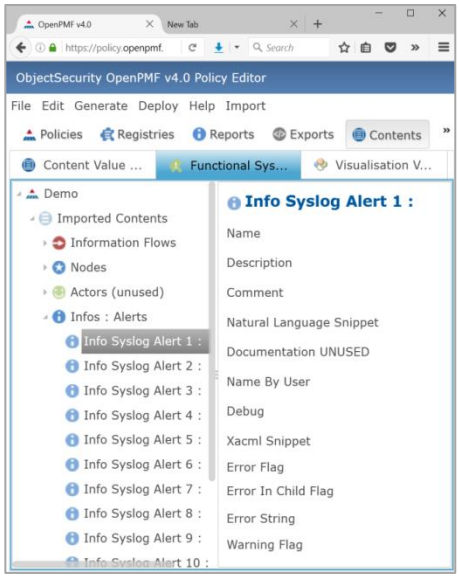
Monitor security via OpenPMF's own runtime.

OpenPMF allows the convenient monitoring of all running enforcement points in a monitoring dashboard. The dashboard shows the status of the enforcement point, as well as any alerts produced by the enforcement point. Alerts are caused by policy violations and by user-configurable logging policies.



Import security alerts

Furthermore, OpenPMF supports importing alerts from 3rd party tools using OpenPMF's rapidly customizable importers, for example Snort Syslog alerts.



What you can do with OpenPMF™ 4.0 Security Policy Automation

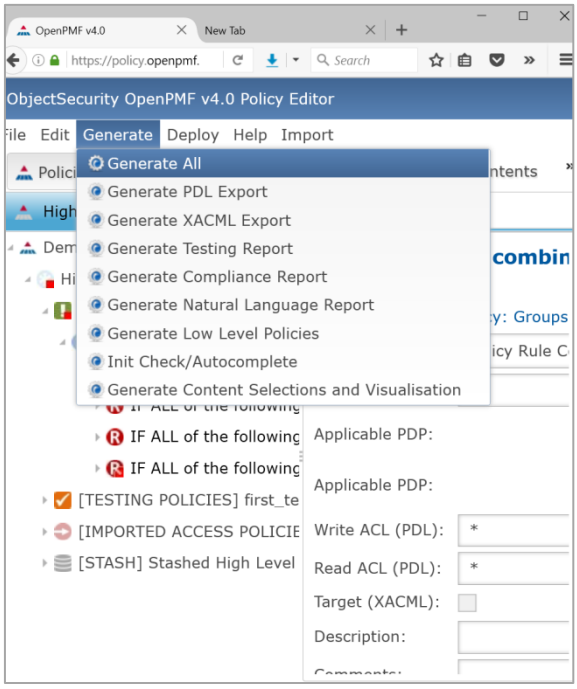
8. **Update** technical enforcement automatically if your IT changes and **customize** OpenPMF

Automatically update policies when your IT landscape changes

To update, just re-import information about the changed IT landscape, and simply regenerate the technical policy at the click of a button.

This capability to auto-update is a major simplification and significant improvement compared to manually implemented technical security policies.

It was originally developed to make security policy management easier for agile Service Oriented Architectures (SOAs), but is widely applicable today, as IT landscapes become increasingly dynamic and interconnected (e.g. IoT, microservices, …).



Rapidly customize policies and enforcement for your organization

OpenPMF is designed from the ground up to be flexible and rapidly customizable. Customization and flexibility are absolutely critical features because every organization has its own set of policies, use cases, and technologies. There is no "one-size-fits-all" when it comes to implementing an overarching policy management "umbrella" such as OpenPMF. Any "one-size-fits-all" products would just end up becoming point solutions themselves, lacking the critical edges of robustness and scalability.

You can customize most features of OpenPMF, including policy features, importers, exporters, enforcement.

Furthermore, OpenPMF is based on industry standards (XMI, XML, REST, Eclipse EMF, MOF, OMG QVT, Xtext, Xpand etc.), making the customization of the data models, importers, and exporters quite straightforward. For example, exporters can be developed quickly based on the specific security products available in your organization.

About the Author

Dr Ulrich Lang

Ulrich Lang is ObjectSecurity's founder & CEO; Ph.D. from University of Cambridge Computer Laboratory (Security Group) on access policies; Master's Degree (M. Sc.) in Information Security from Royal Holloway College (London) in 1997. Ulrich is a renowned thought leader in access control policy, model-driven security, and Cloud/SOA/middleware security, identity & access management. He is on the Board of Directors of the Cloud Security Alliance (Silicon Valley Chapter).

He is co-inventor and co-developer of ObjectSecurity's award-winning OpenPMF product. He delivers some of the professional services ObjectSecurity offers. He has published over 150 papers/presentations, and has previously worked as a proposal evaluator, project evaluator, conference program committee, panel moderator, consultant, book author, technical expert witness.

About ObjectSecurity

ObjectSecurity's mission is to simplify security for the complex, interconnected IT landscapes most organizations deal with today. The company's primary focus is simplified, automated security management and secure IT application integration, led by its core product -- OpenPMF 4.0, the leading security policy automation platform. OpenPMF 4.0 stops security breaches with powerful policy enforcement through patented "model-driven security" automation.

Launched in 2000 by CEO/Founder Ulrich Lang, the company has two independently operated entities: ObjectSecurity LLC in San Diego, CA, and its European company, ObjectSecurity Ltd., in Cambridge, UK. The employee-owned company works with partners and clients in more than 25 countries across the globe.

For more Information

- ObjectSecurity OpenPMF Security Policy Auditor™: objectsecurity.com/auditor
- ObjectSecurity OpenPMF™ 4.0 Security Policy Automation: objectsecurity.com

objectsecurity.com
@objectsecurity