VESPA: Multi-Layered Self-Protection for Cloud Resources

Marc Lacoste

Orange Labs

Self-protection has raised growing interest as possible element of answer to the cloud protection challenge. However, previous solutions miss flexible security policies, cross-layered defense, multiple control granularities, and open security architectures.

This talk presents VESPA, an open IaaS self-protection architecture and framework that overcomes such limitations. Key features are regulation of security at two levels, both within and across software layers; flexible coordination of multiple feedback loops enabling enforcement of a rich spectrum of protection strategies; and an extensible architecture allowing simple integration of commodity security components.

OW2Con'12, November 28-29, 2012
Orange Labs, Paris. www.ow2.org

Motivation

- **Security = #1 adoption stopper to cloud computing.**

- **Mushrooming threats:**
  - **From outside:** rootkits, malware, intrusions…
  - **From inside:** "honest-but-curious" legitimate users, over-privileged admins…

- **Heterogeneous defenses:**
  - **Vertically:** layer-specific mechanisms.
  - **Horizontally:** system. vs. network placement.

⇨ **Self-prote** **with promise of simpler, s** *ow*

But…
…How to design self-protecting clouds?

3 Major Challenges

Challenge #1: Multi-Layering

- Each cloud layer has its own security mechanisms, oblivious to other layers.
- **But attacks may span several layers at once!**

Challenge #2: Multi-Laterality

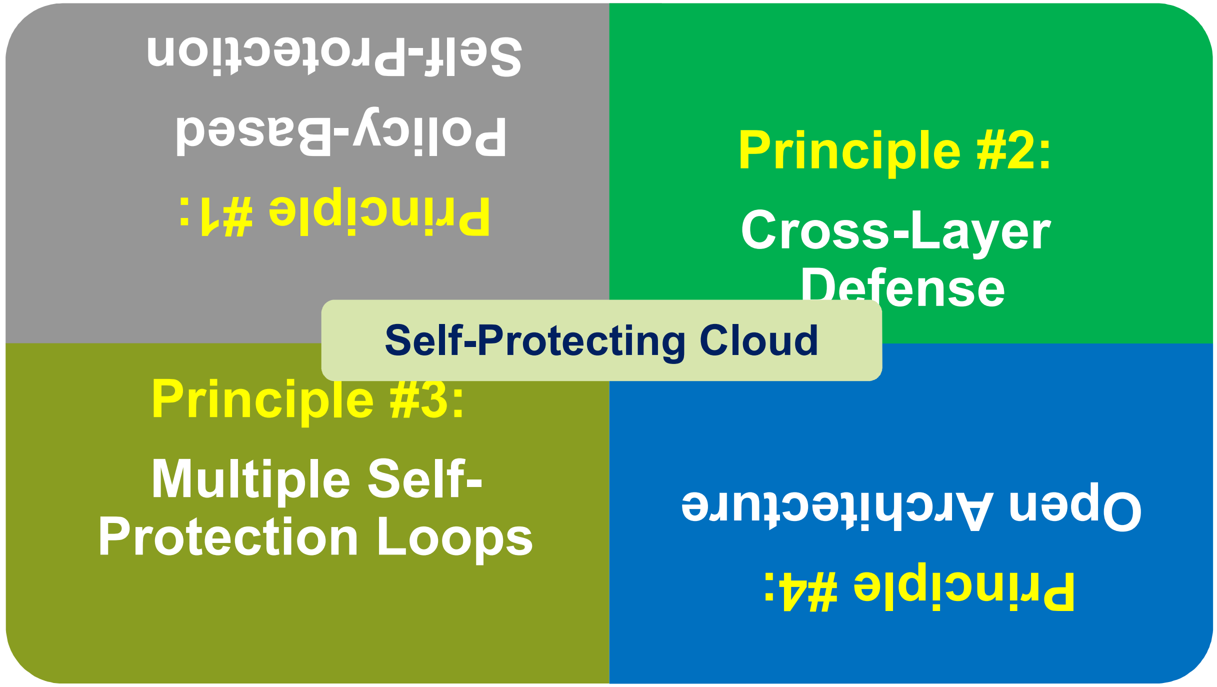
- Each cloud stakeholder has its own security objectives and policies.
- **Flexiblility is needed in monitoring granularity and security policies!**

Challenge #3: Openness

- Cloud stakeholder topology is dynamic, and threats may be unknown.
- **Interoperability is needed with 3rd-party security policies/components!**

- Principle

Cloud Self-Protection Design Principles



Principle #1: Policy-Based Self-Protection

Principle #2: Cross-Layer Defense

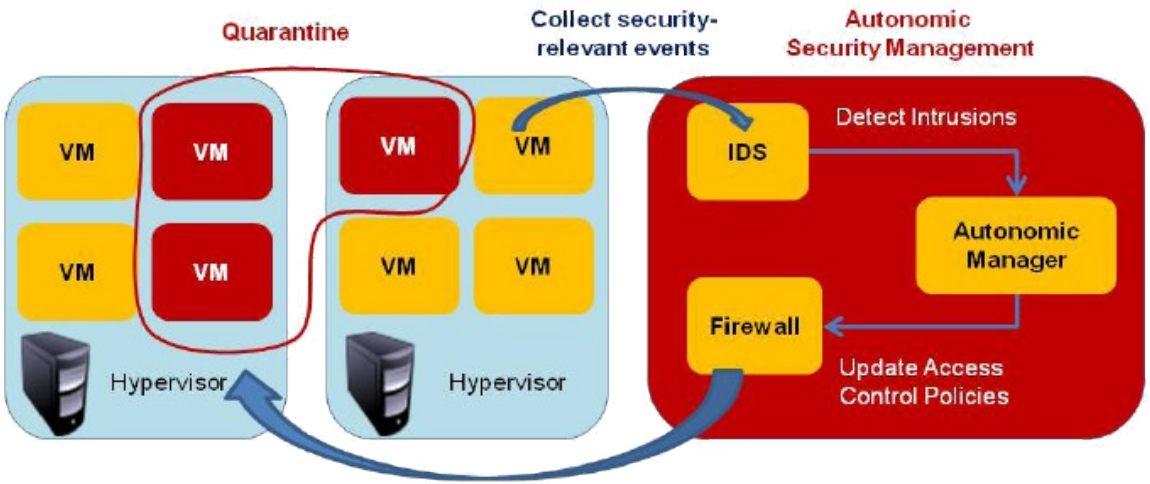
Principle #3: Multiple Self-Protection Loops

Principle #4: Open Architecture

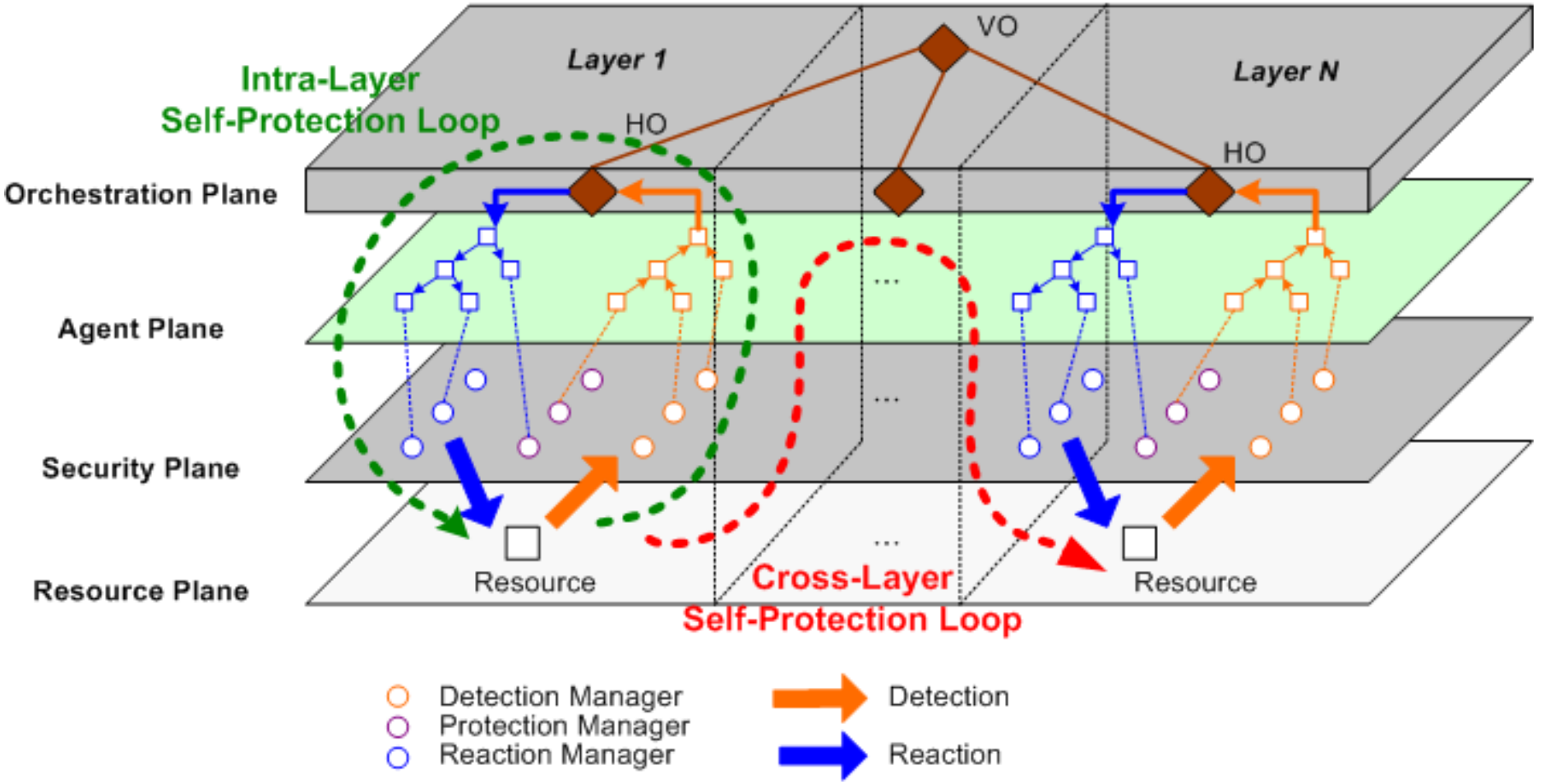
...integrated in the security architecture.

VESPA Goals

- **VESPA = Virtual Environments Self-Protecting Architecture:**
  An autonomic security framework for regulating protection of IaaS resources.
  1. Cross-layer approach to security.
  2. Multiple levels of supervision granularity.
  3. Open and flexible architecture for easy security interoperability.
- **Implementation:** KVM-based IaaS infrastructure.
- **Typical application:** risk-aware dynamic VM confinement.

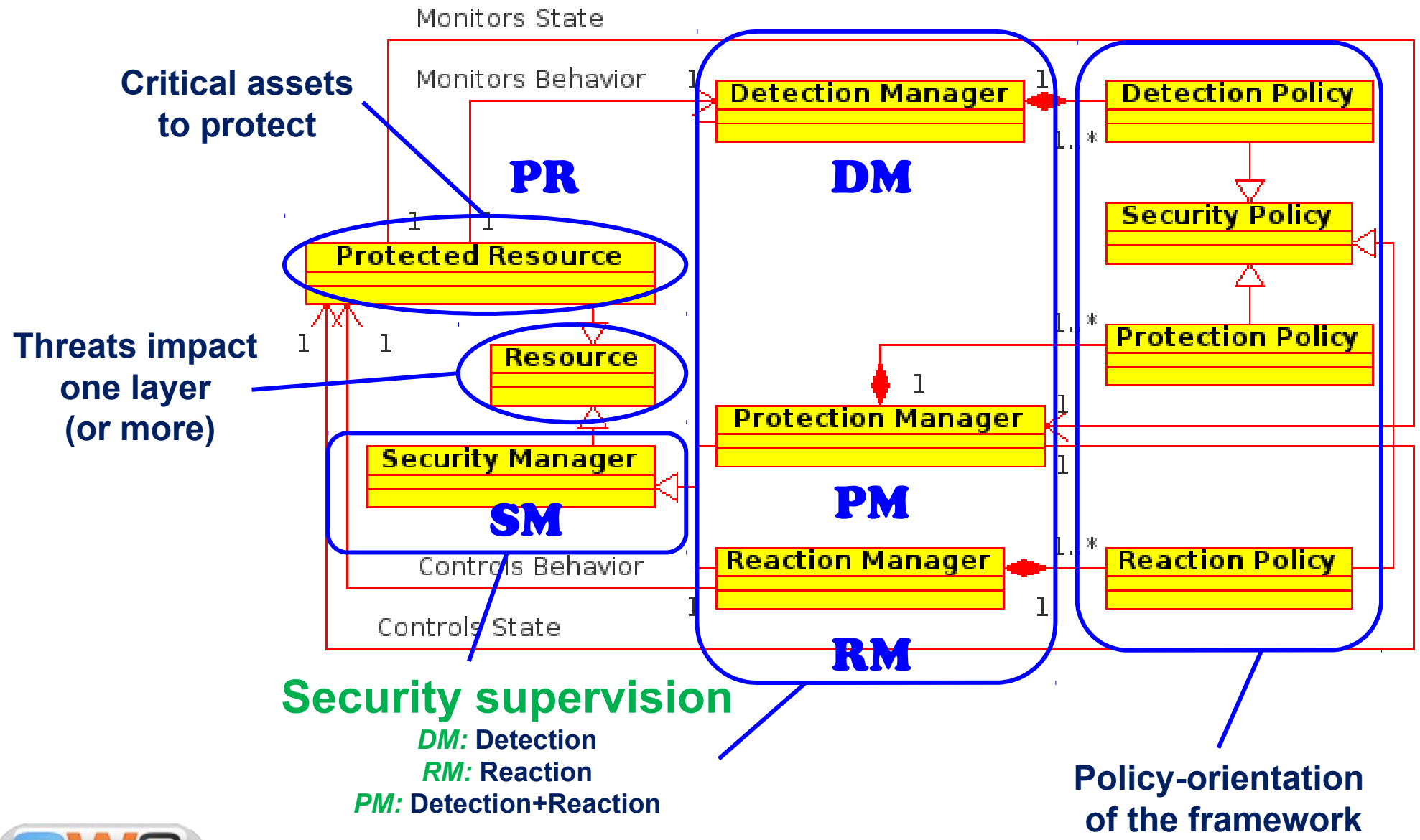


VESPA System Architecture



1. Policy-based security regulation, with well-defined SP model.
2. Automated protection at two levels, within and across IaaS layers.
3. Flexible orchestration of multiple SP loops, for rich defense strategy.
4. Layered, extensible architecture for easy security COTS integration.

Security Model

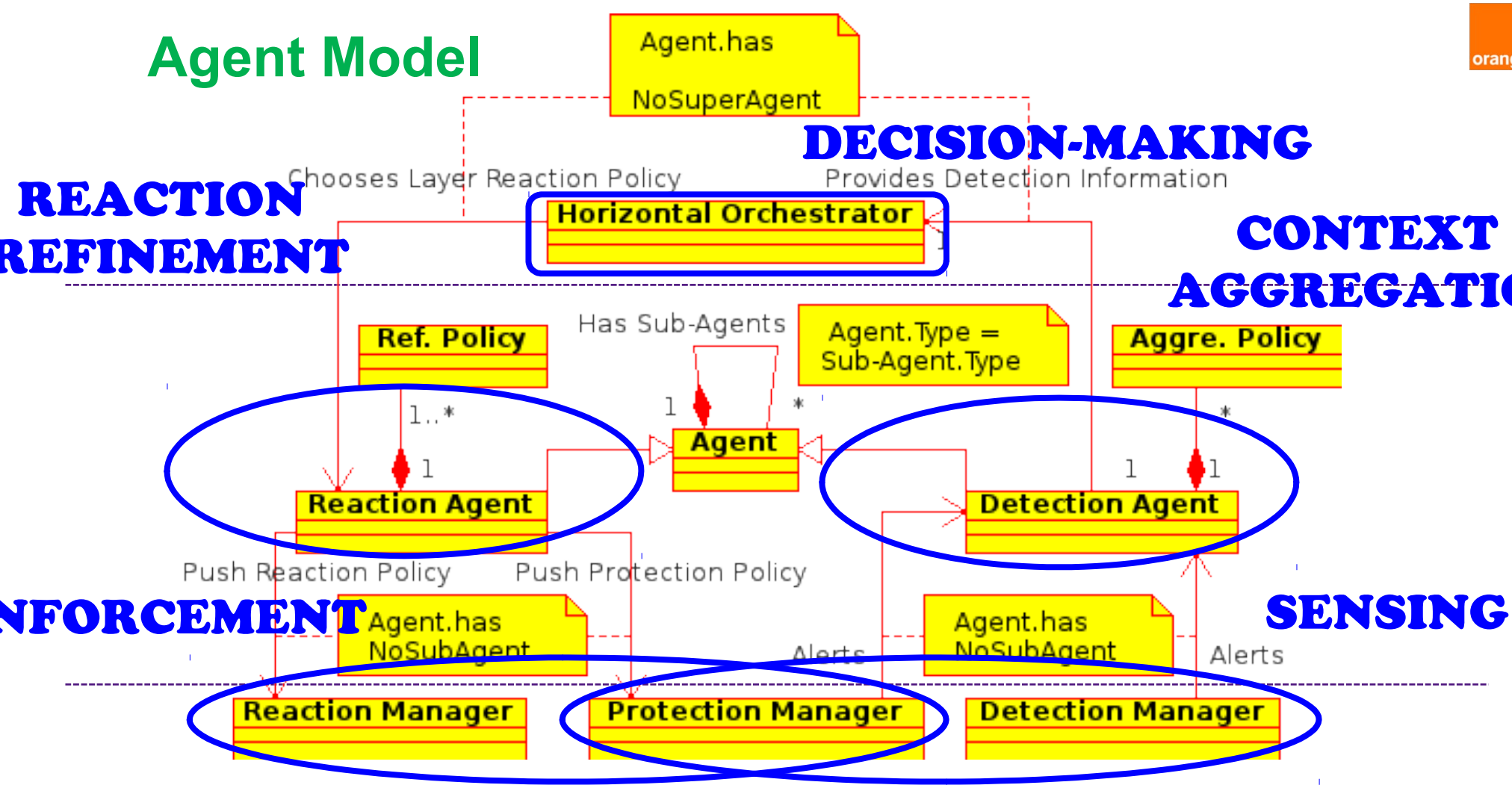


Security supervision

DM: Detection
RM: Reaction
PM: Detection+Reaction

Policy-orientation of the framework

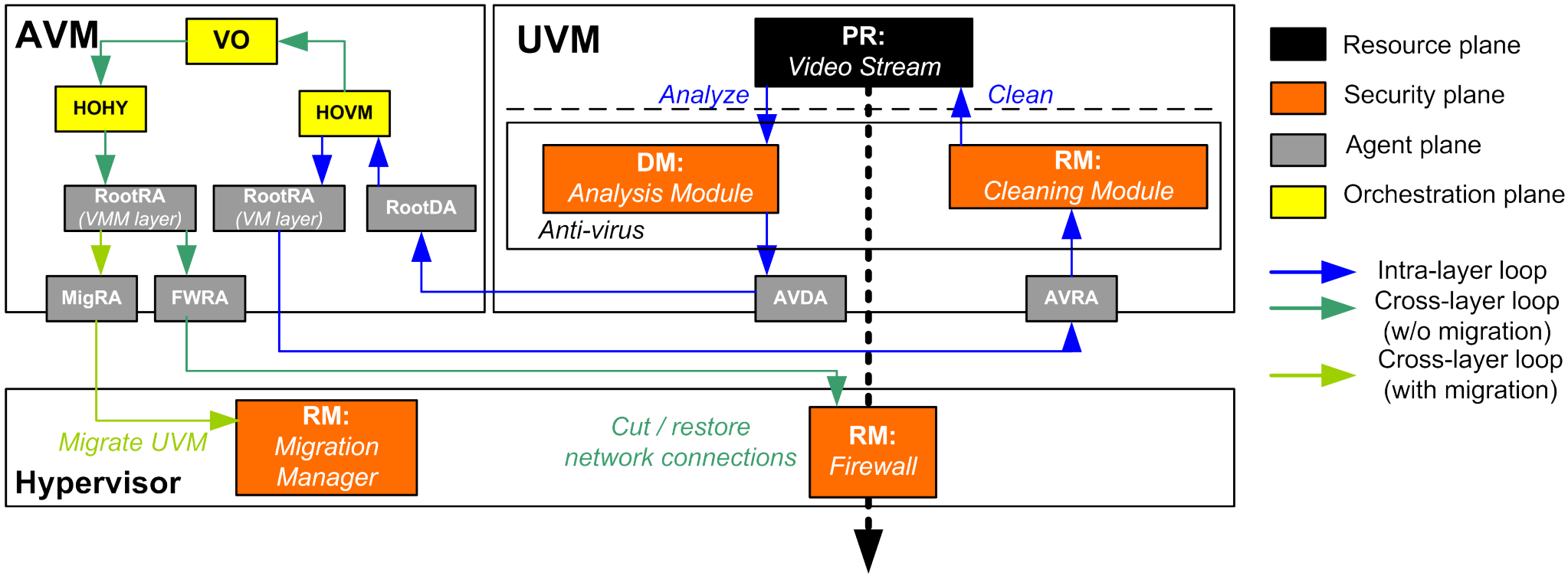
Agent Model



Agents **performs mediation between security and decision-making:**

- Security context aggregation.
- Reaction policy refinement.
- API adaptation for easy infrastructure integration of security COTS.

Implementing Risk-Aware VM Quarantine



Three levels of self-protection:

1. **Intra-layer** [VM-level]: anti-virus for analysis and cleaning.
2. **Cross-layer** [VM+hypervisor levels]: hypervisor firewalling for VM isolation.
3. **Cross-layer** [VM+hypervisor levels]: hypervisor migration manager to move VM to quarantine zone and back.

Conclusions

- **Key points:**
  - VESPA: architecture for effective and flexible SP of IaaS resources.
  - Two-level tuning of security policies, within and across layers.
  - Coordination of multiple loops allows rich spectrum of defense strategy.
  - Multi-plane open design for easy integration of detection/reaction COTS.

- **Ongoing:**
  - VESPA v0 = 8000 Python LoC. Underlying infrastructure = KVM.
  - C version under development using Fractal / Cecilia framework.

Security services: IDS, anti-virus, log analysis, firewall, MAC.

  - Extend VESPA to the **multi-cloud setting** using security domains.

- **More …**

Available soon in open source! Check-out our **ICAC 2012** paper!

[ICAC 12] Aurélien Wailly, Marc Lacoste, Hervé Debar.
VESPA: Multi-layered Self-Protection for Cloud Resources.
9th ACM International Conference on Autonomic Computing (ICAC),
San José, California, September 2012.


Thanks!
Contact:
Marc Lacoste
Senior Research Scientist
Orange Labs, Security Dept.
E-mail: marc.lacoste@orange.com