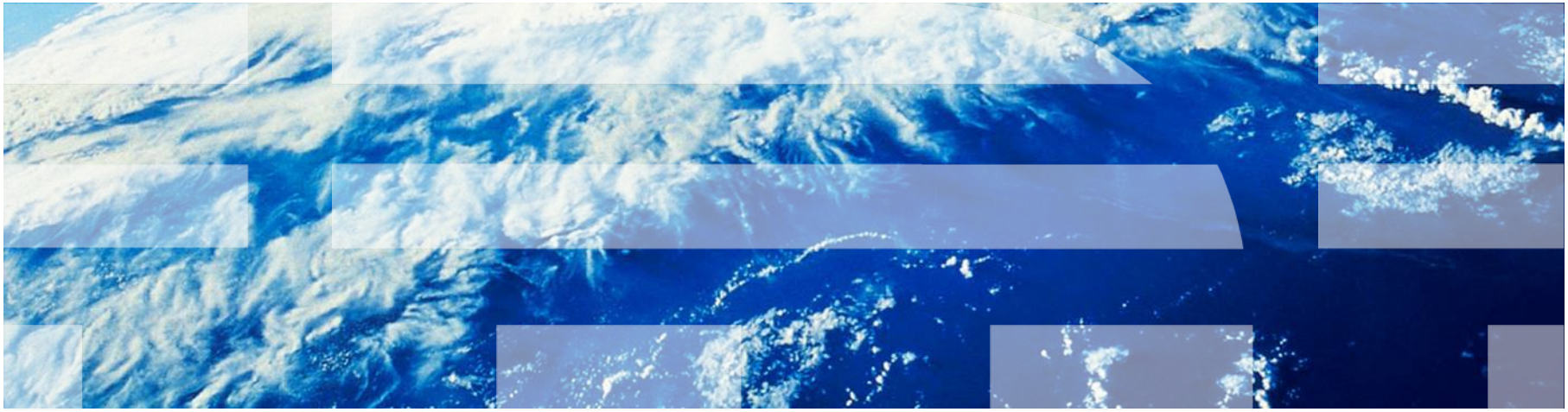
Security Analysis of Dynamic Infrastructure Clouds

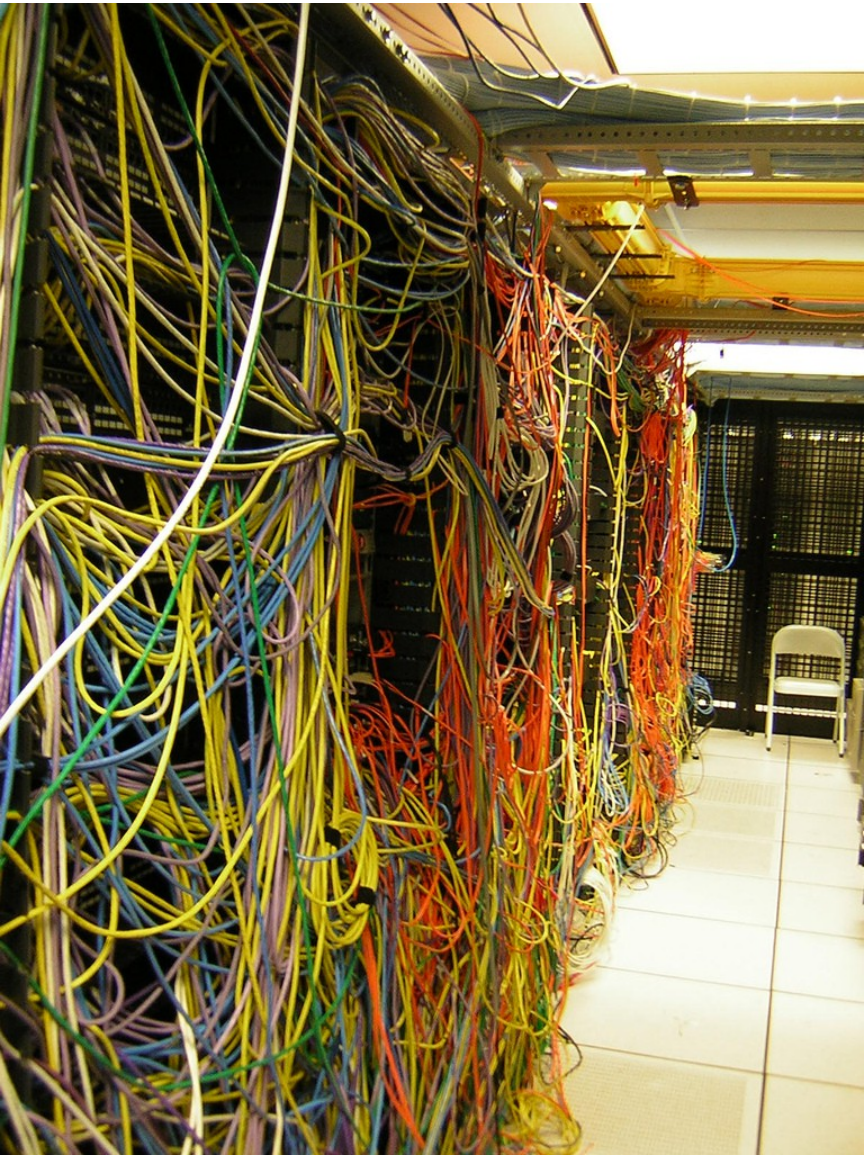
Sören Bleikertz, IBM Research – Zurich
Thomas Groß, University of Newcastle upon Tyne
Sebastian Mödersheim, DTU Informatics



What is this talk about?

- *What is the problem?*
  Complexity and insider attacks lead to misconfigurations and isolation failures.
- *How do we approach it?*
  Pro-active, model-based analysis of infrastructure changes.
- *What are the key insights?*
  Possible to model real-world infrastructure clouds and their changes using graphs and transformations of graphs.
  Efficient automated analysis in production-size environments.

Complexity/Insiders: Misconfigurations lead to Isolation Failures

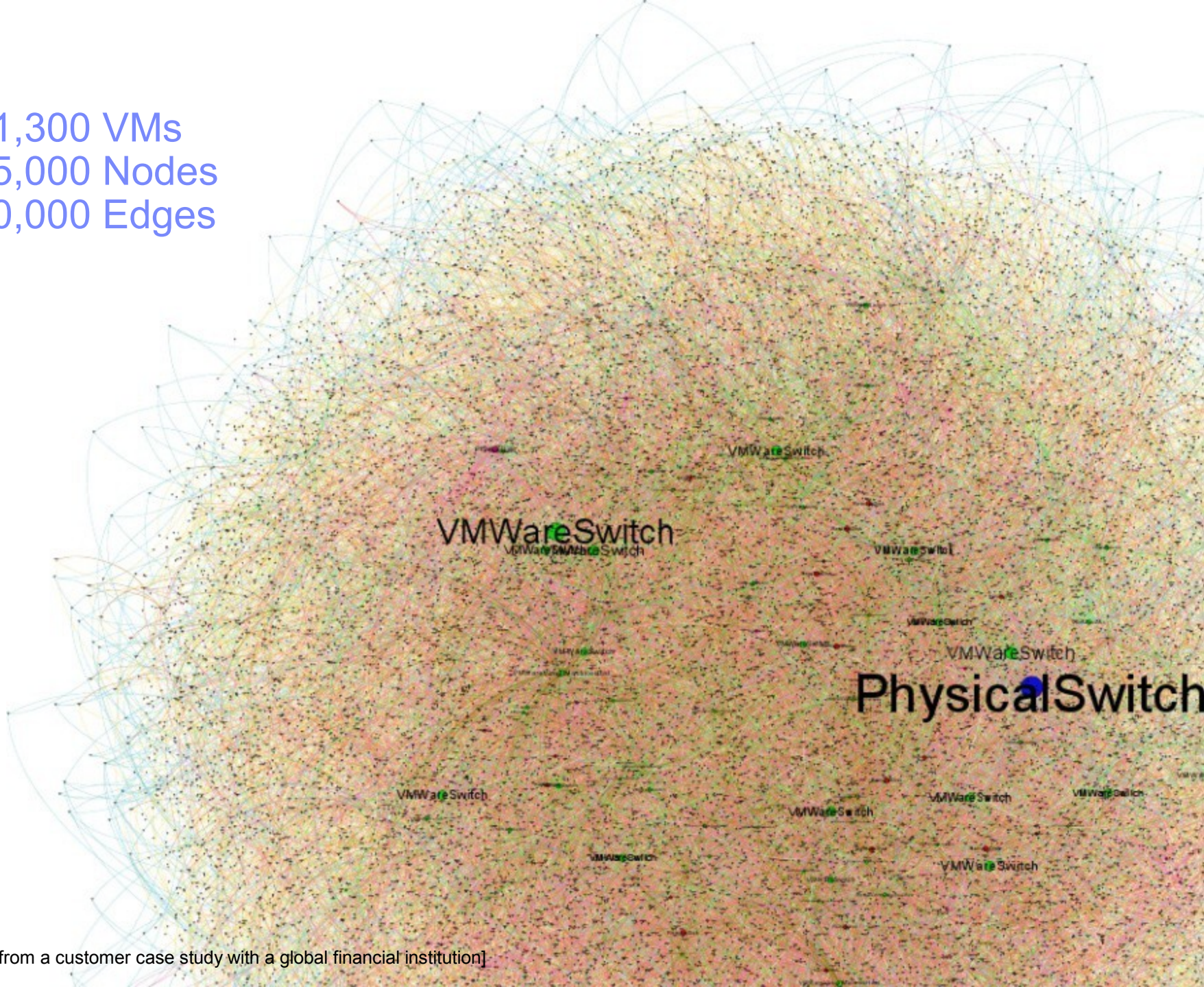


- Complexity → error-proneness
- Amplified by virtualization
- Multi-tenancy and shared resources

  → Isolation essential

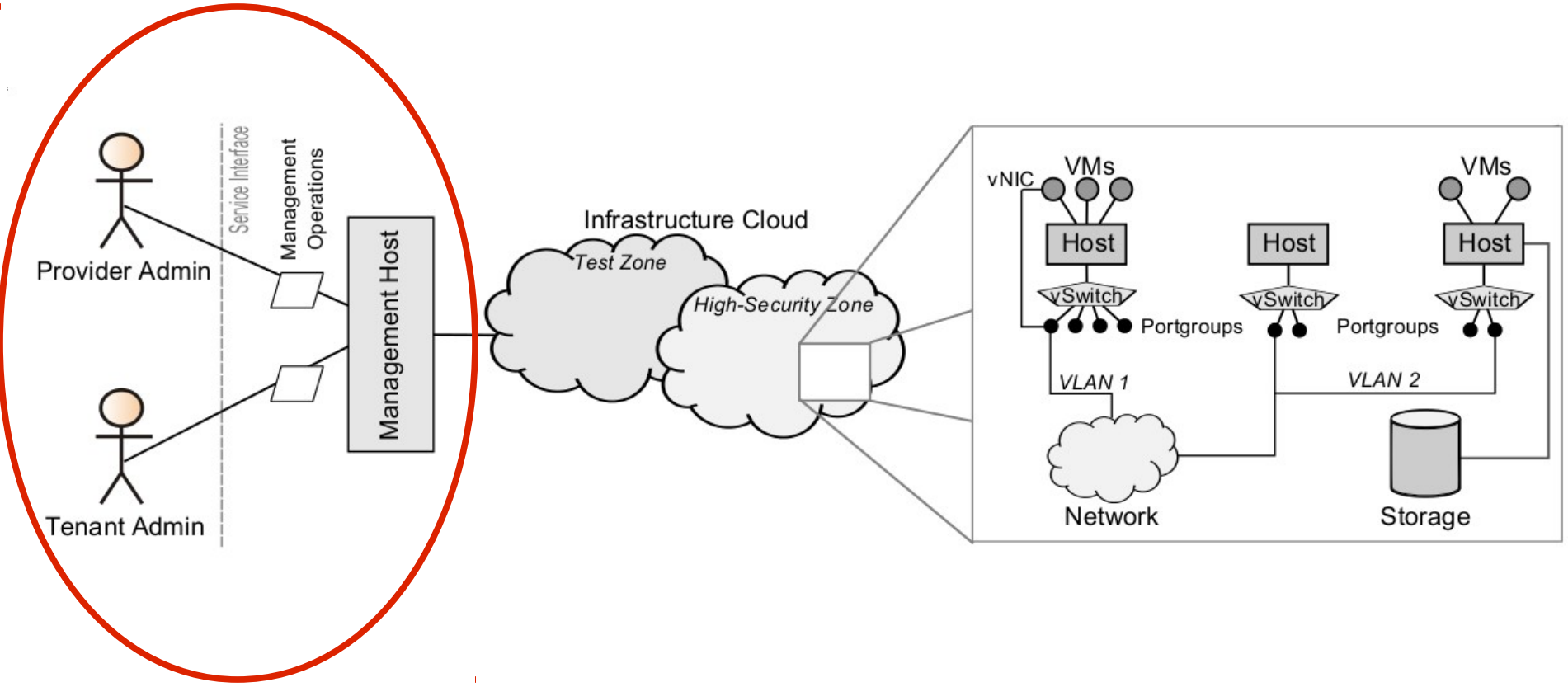
[Photo: http://www.flickr.com/photos/alonzo/113658733]

1,300 VMs
25,000 Nodes
30,000 Edges

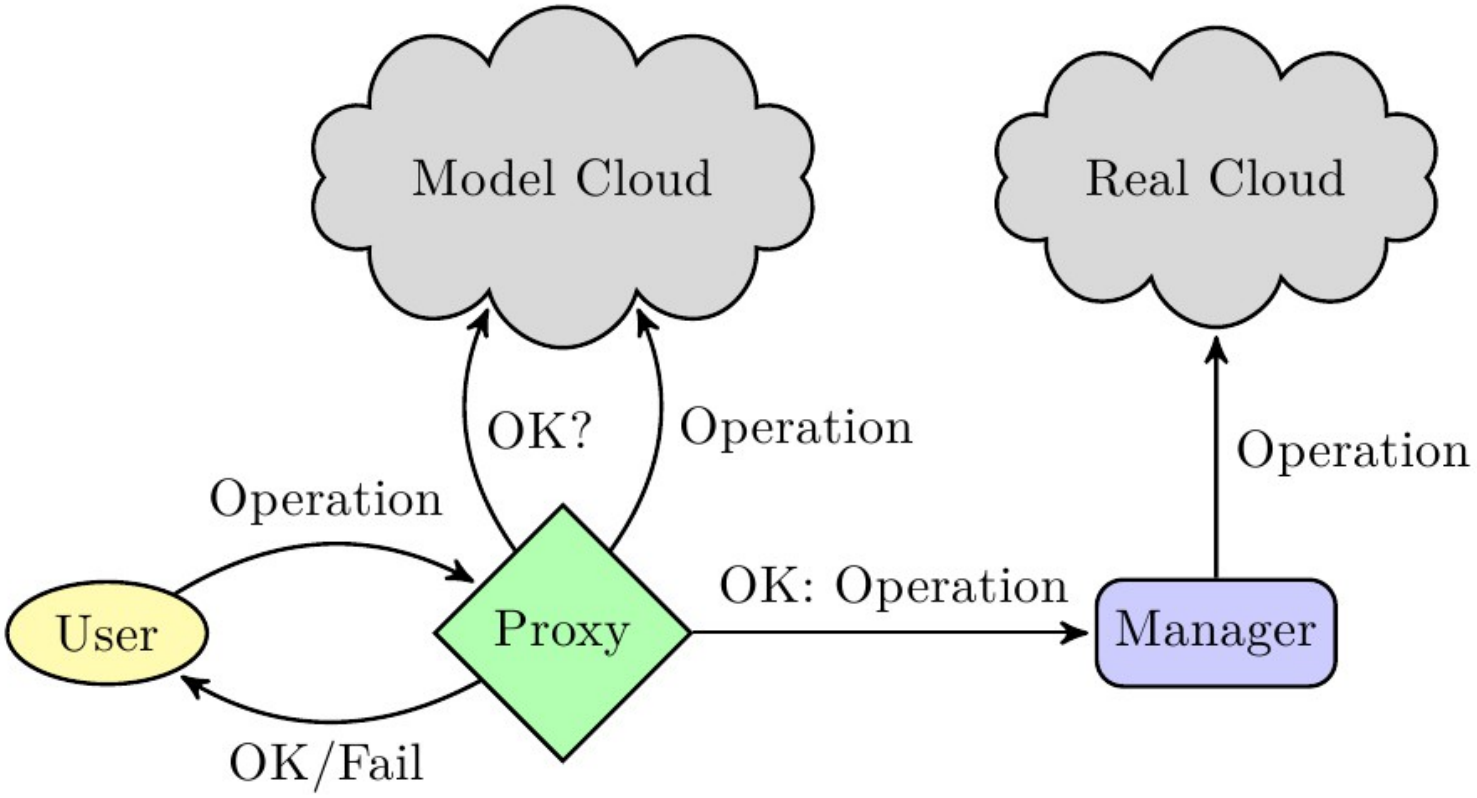


 [Data from a customer case study with a global financial institution]

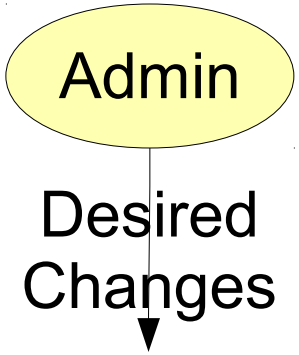
System Model of Infrastructure Clouds



Run-time Operations Analysis

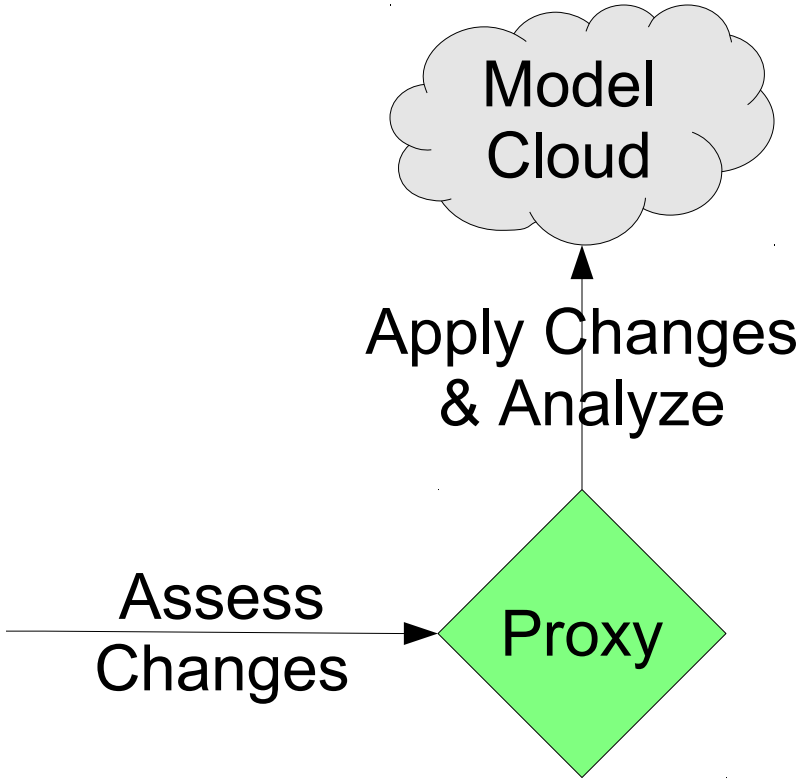


Change Plan Analysis

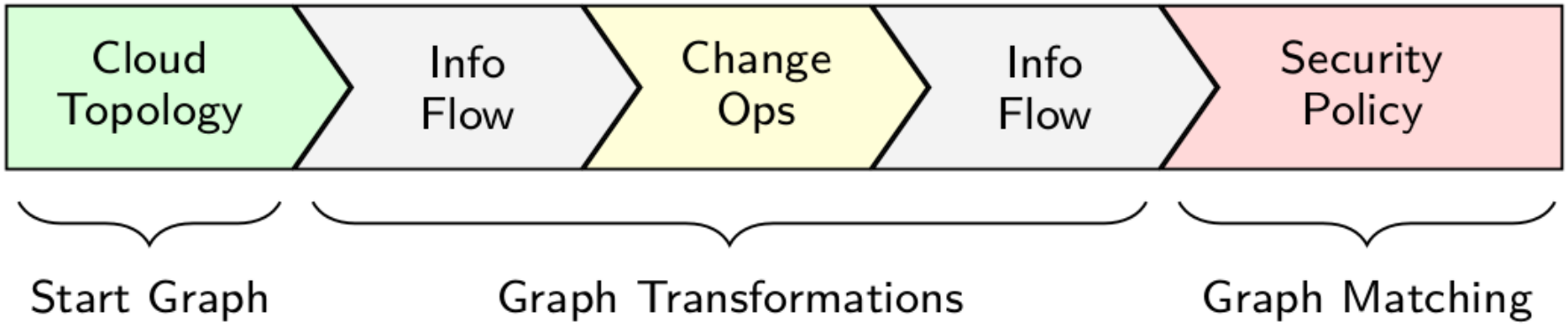



```
AddVirtualSwitch("host1", "vswitch2");
node PG;
AddPortGroup("host1", "vswitch2", "portgroup4", 23, ↩
    out PG);
string Dev;
AddVirtualNic("host1", "portgroup4", "127.0.0.1", ↩
    "00:FF:00:FF:00:FF", out Dev);

UpdateVirtualNic("host1", Dev, "127.0.0.2", ↩
    "00:FF:00:FF:00:AA");
UpdatePortGroup("host1", "portgroup4", 24, ↩
    "portgroup4");
```



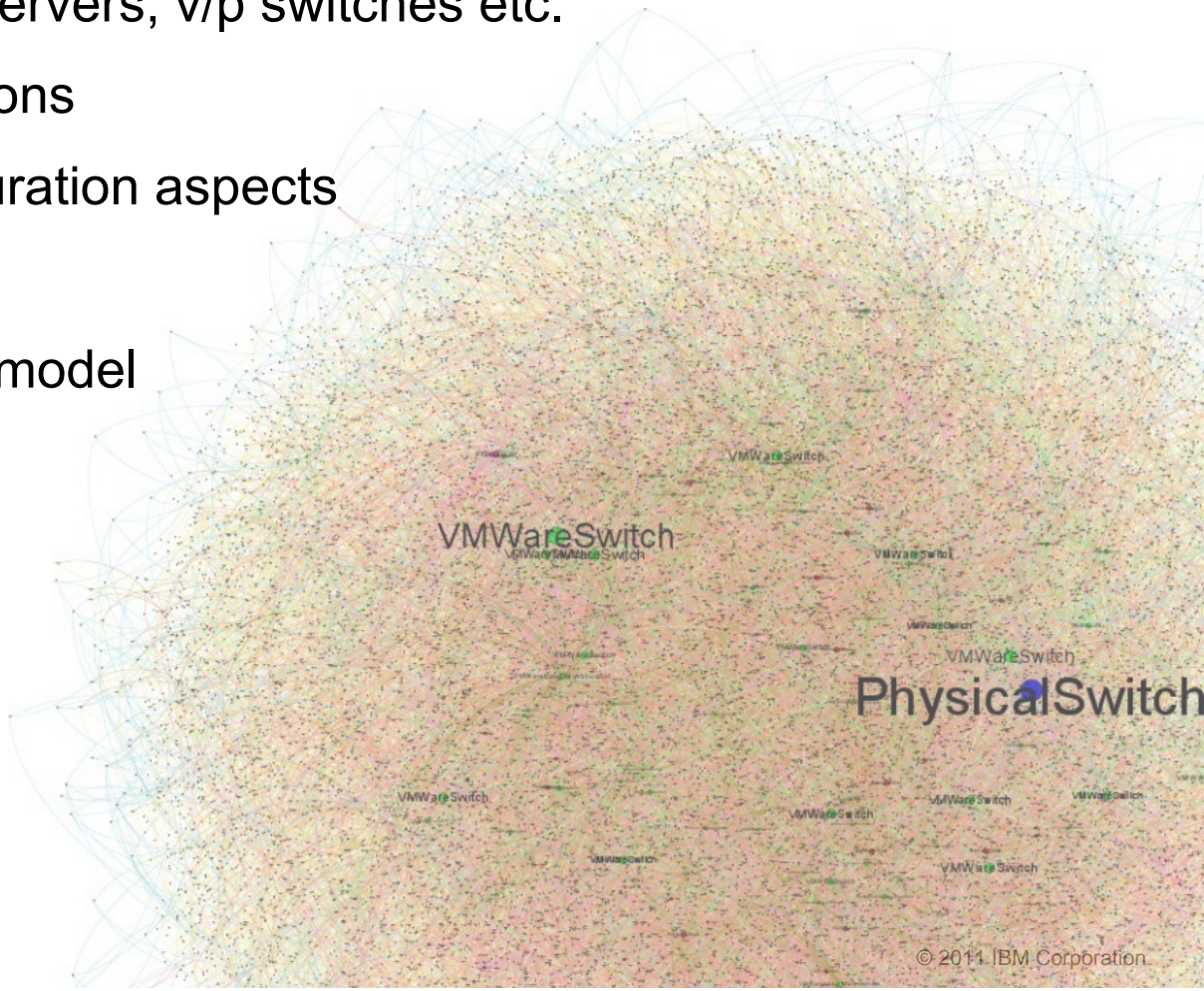
Overview of Analysis Process



Start Graph: Infrastructure Cloud Topology and Configuration

- Vertices: VMs, physical servers, v/p switches etc.
- Edges: Topological relations
- Vertex attributes: Configuration aspects

- Based on existing graph model
- Automatically populated

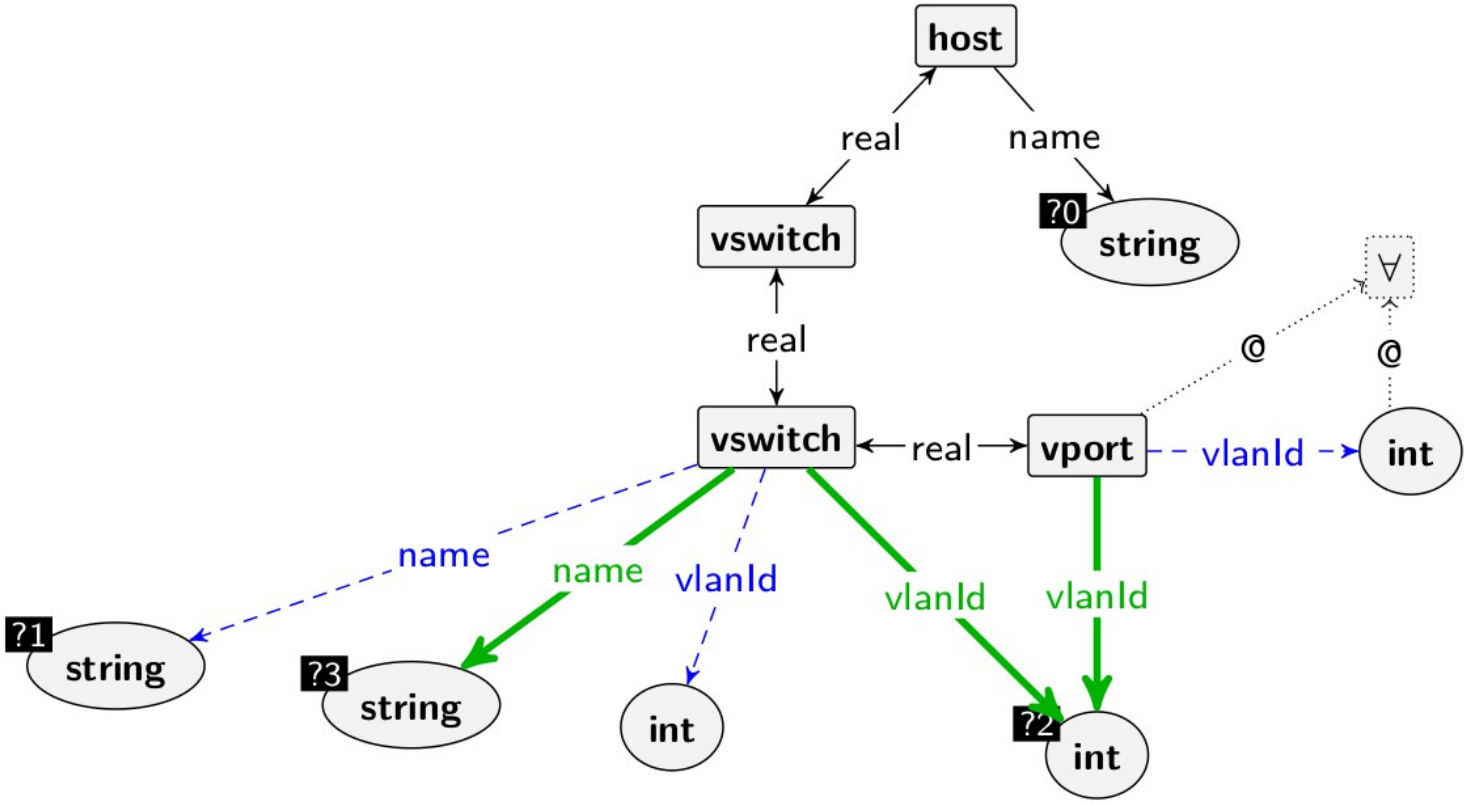


Introduction of Operations Transition Model

- Operations induce changes to the infrastructure topology or configuration
- Infrastructure modeled as a graph
- Model operations and their changes as *graph transformations*
- Well-studied formalism, many tools available

Operation Model Example: UpdatePortGroup

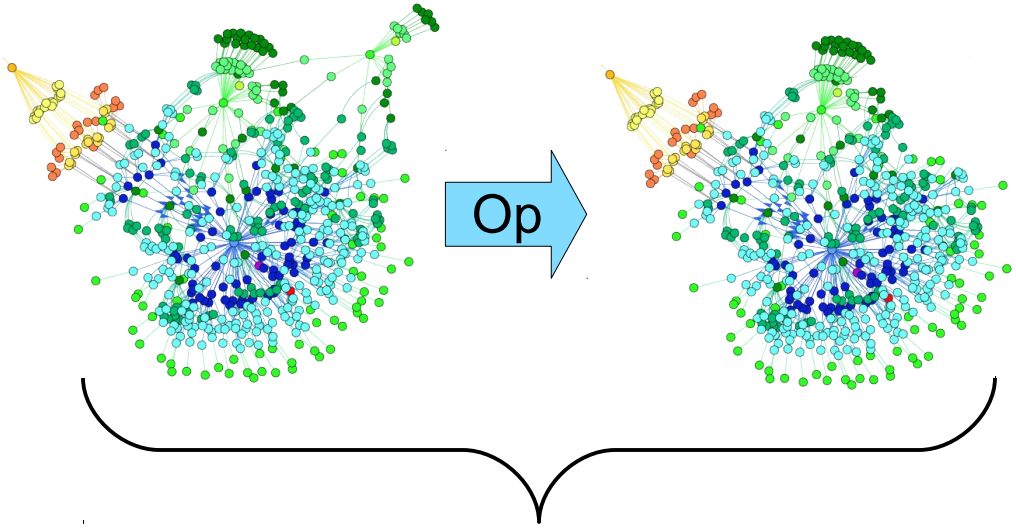
```
UpdatePortGroup(string hostname, string pgName,
  string newPGName, int newPGVlanId)
```



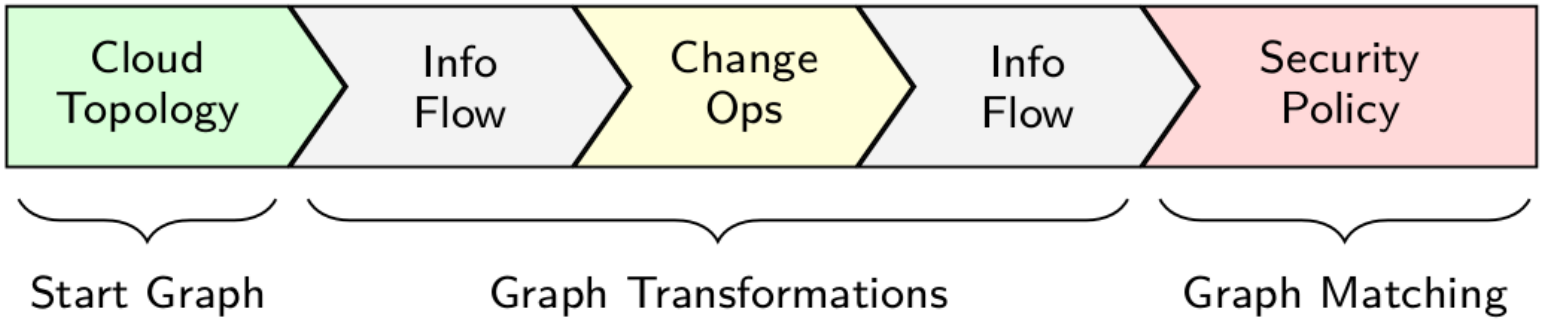
How to Create a Good Model?

1) Documentation (VMware API, ~500 operations)

2) Assessment of actual changes in the infrastructure

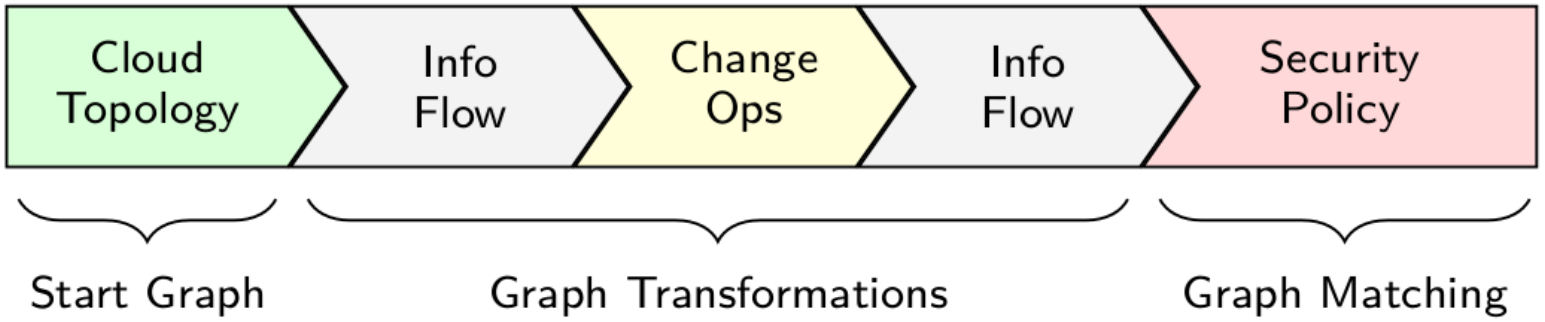


Dynamic Information Flow Analysis



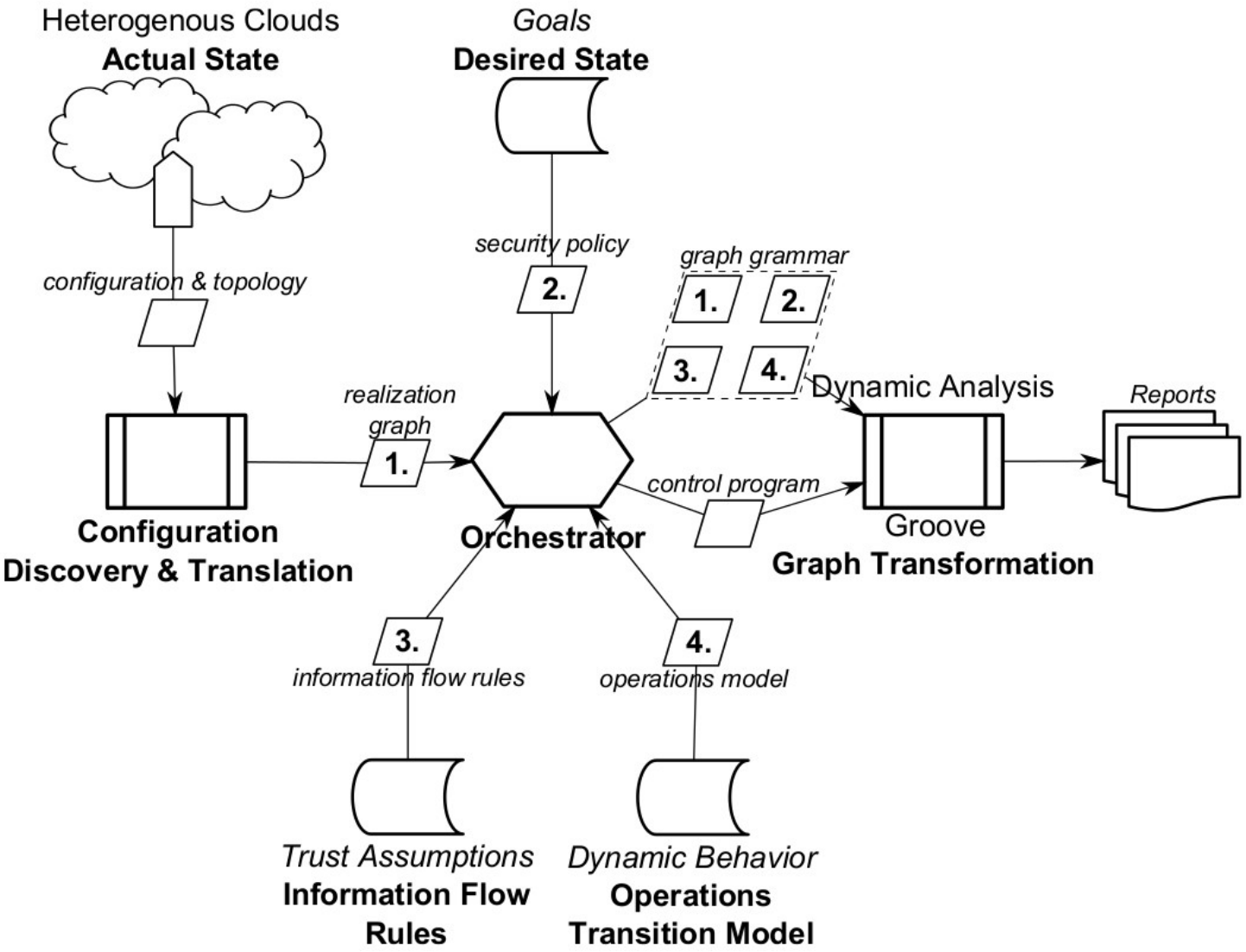
- Initial information flow analysis
- Adjustment of flows after operation
- Based on existing analysis for static infrastructures
- Extended to dynamic ones and formalized as graph transformations

Security Policy Matching



- Express policies as attack states
- Formalize attack states as graphs with conditions
- Try to match attack state graph in transformed cloud topology graph
- A match constitutes a policy violation

Weatherman Architecture



Time Measurements for Change Plan Analysis

Scenario	Complete
Lab, Safe	5.61 ± 0.25
relative	
Lab, Fault	5.74 ± 0.14
relative	
Production, Safe	154.71 ± 6.91
relative	
Production, Fault	69.53 ± 1.71
relative	

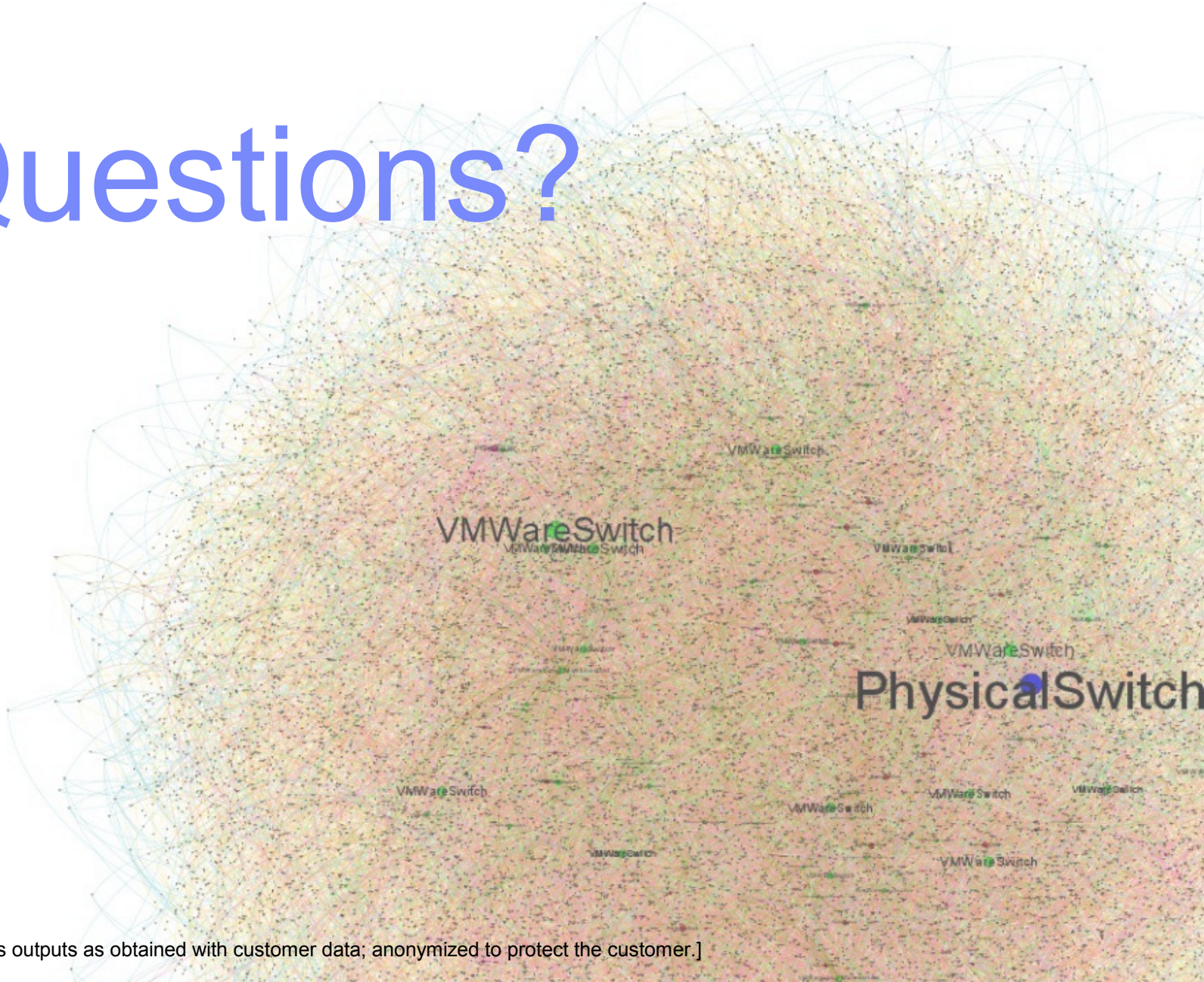
- Lab
  - 4 hosts
  - 16 VMs
  - 2 Security zones
  - Graph: 210 nodes, 548 edges
  - Simplified: 101 nodes, 310 edges
- Production
  - 60 hosts
  - Around 1400 VMs
  - Five security zones
  - Graph: 23579 nodes, 61564 edges
  - Simplified: 9576 nodes, 32902 edges

Conclusions and Future Work

- *Weatherman*: Pro-active, model-based assessment of changes to mitigate misconfigurations.

- Future Work
  - Run-time mitigation and enforcement
  - Case and user studies
  - Extend coverage of operations model

Questions?



 [*) Realistic analysis outputs as obtained with customer data; anonymized to protect the customer.]