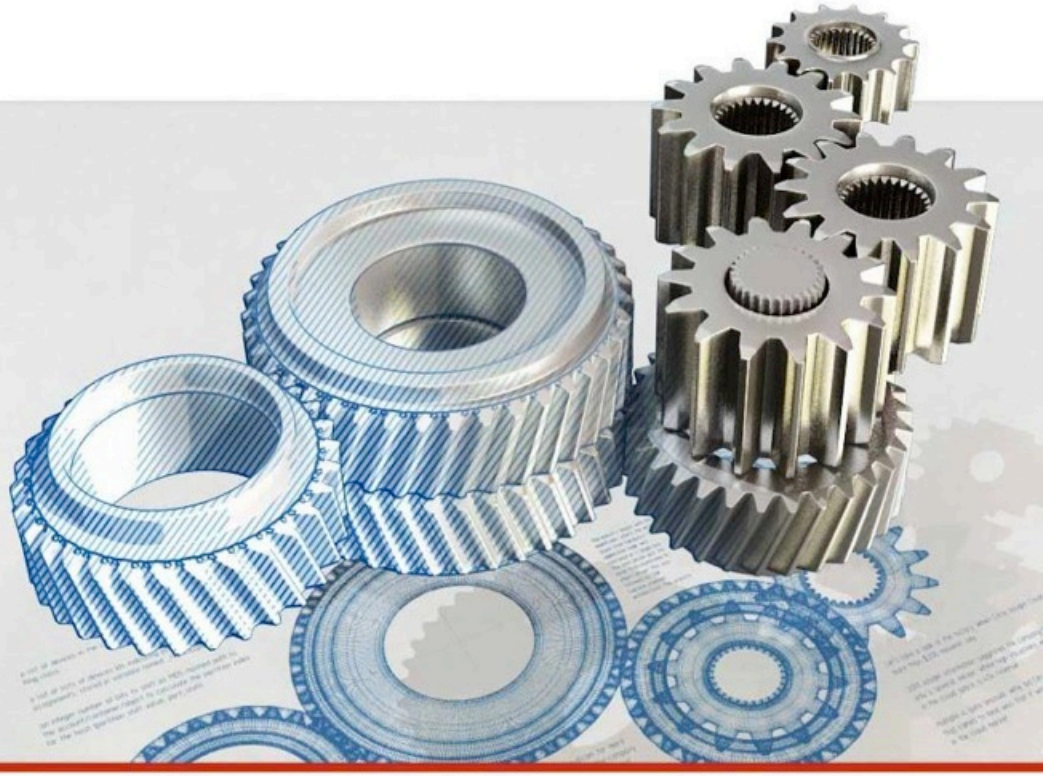
MIRANTIS

Securing openstack™ for compliance



BUILT FOR openstack™ CLOUD SOFTWARE

Tomasz ‘Zen’ Napierała

Sr. OpenStack Engineer

Tomasz Z. Napierała

Senior OpenStack Engineer @ Mirantis, Inc.

automation, web performance, compliance, security

MIRANTIS

Mirantis, Inc.

Largest independent vendor of OpenStack services and technology.

We operate from Mountain View, California, with remote offices in Russia, Ukraine and Poland.

60+ successful OpenStack implementations and 400+ infrastructure experts.

Mirantis, Inc.

MIRANTIS

Pure Play OpenStack®

BUILT FOR openstack CLOUD SOFTWARE

Agenda

MIRANTIS

What's included

- State of cloud compliance
- Modules overview
- Practical tips

What's not included

- Securing VMs
- Guarantee

MIRANTIS

PCI DSS overview

PCI DSS recap

- Set of policies and procedures
- Optimize security of financial data processing
- Protect cardholders
- 12 general requirements
- Ongoing process
- PCI DSS version 2.0

State of compliance in cloud

- Not possible (pre 2012)
- Hard, not clear (pre 2013)
- PCI DSS 2.0 Cloud Computing Guide (Feb. 2013)
- Production deployments
  - Rackspace

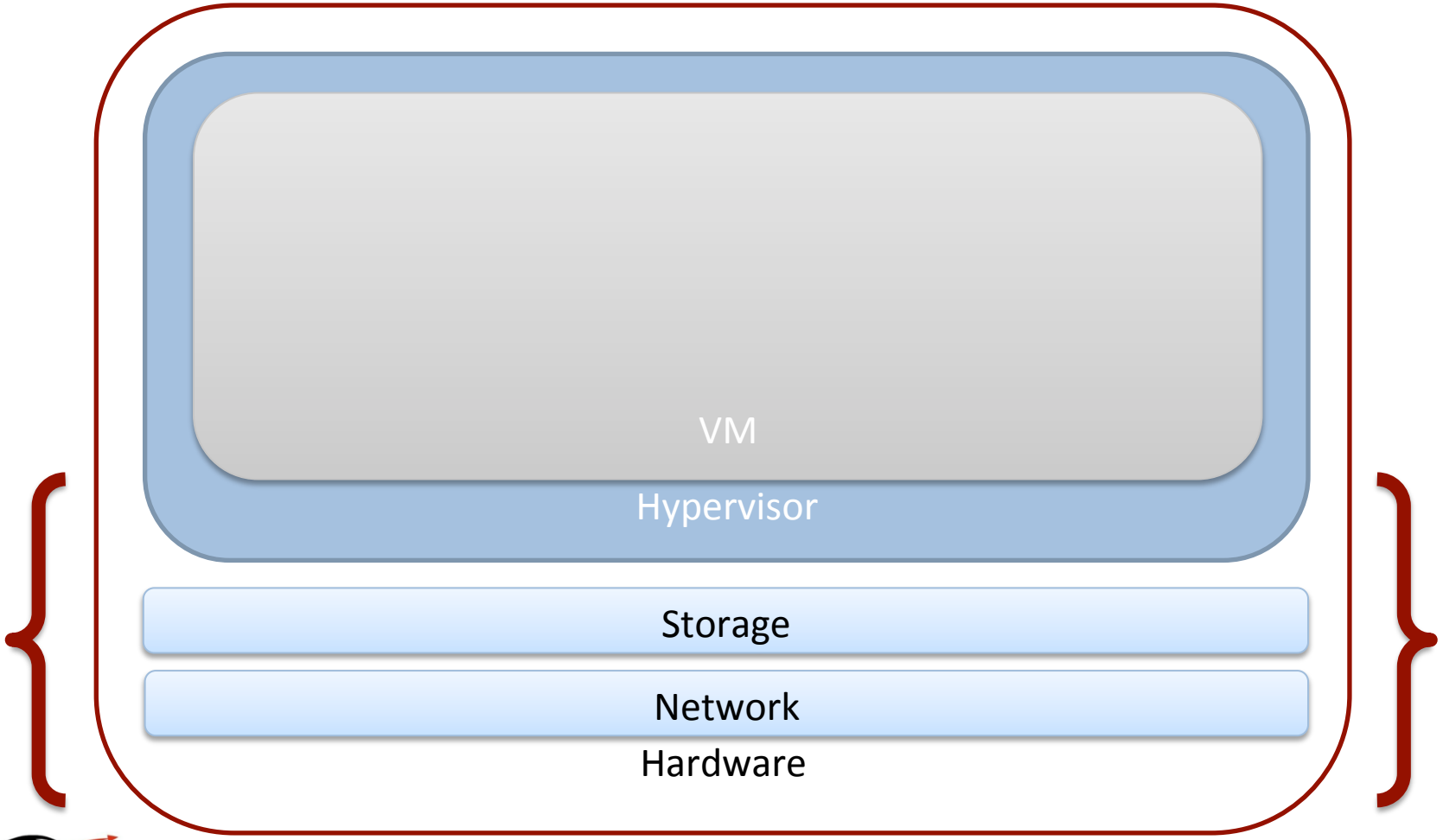
Where are we

12 x

Rely on Cloud Service Provider
for HW->Hypervisor related compliance

Phil Cox, RightScale

Whare are we



PCI DSS requirements

Source: http://www.datasecureworks.com/images/Trustwave/pci-requirements-grid.png

Projects history

- Initially launched for customer (2 engineers)
- Moved into internal project (2+ engineers)
- Some parts reused in other projects
- 2 clients using the tools

MIRANTIS

Projects limitations

- RedHat / CentOS compatible
- Only for private IaaS clouds
- Operator centric
- Technology focused
- Everything in scope
- No “redo”
- No OpenStack patches
- No firwall management

BUILT FOR openstack CLOUD SOFTWARE

Ingredients

Elements

- Baseline hardening
- HSM PoC
- Auditing system
- Log collection system
- Intra cluster secure communication
- Audit tools
- Documentation

Tools

- Fuel extension
- Puppet modules
- OpenStack patches (not included)
- OpenSCAP profiles (SRR)
- Documentation
- Checklist

Notes

- PCI DSS 2.0
- NIST

External dependencies

- LDAP / AD
- HSM (PoC available)
- Secure database + SSL

Puppet modules

aide

- File integrity checking with AIDE

auditd

- Auditing and logging during boot
- Auditing ang logging in runtime
  - Crucial file access monitoring
  - Over 80 rules
  - Based on Aqueduct project https://fedorahosted.org/aqueduct/

baseline

- Disabling services
- Sysctl tuning
- Disabling interactive startup
- Password for single mode
- Profile tuning
- PCI DSS required info in issue/issue.net

clamav

- Scanning policies
- Update policies
- Logging

controller_ipsec

- Mesh tunnels between controllers

limits

- Tuning system limits

Logstash (+ kibana + zeromq)

- Entire log collection infrastructure
- Predefinded OpenStack inputs + filters

pam

- Cracklib
- Blocking accounts

pwpolicy

- Password policies

rabbitmq

- Added SSL support

securetty

- Disabling root login on console

secureusers

- Securing internl OpenStack and systems users

ssh

- Secure SSH client and server configuration

sudo

- Protecting from shell escapes
- Disabling sudo su for root
- Secure defaults for sessions

What's not included

- System images
- Glance protection
- Swift encryption

Tips

- HSM (PoC available)
- Compliance is not technology
- Virtualized != cloud
- Automation is a king
- Get an expert
- Get experienced QSA
- Use Quantum

Notes

- Buggy egress filtering in Grizzly
- No default TLS support in VNC
- No image scanning, shredding, etc.
- User cleanup scripts
- No logging framework for tracking cloud activities?
- No granular access rights
- No default „zero access” policy

Notes on 8.5

8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:					
	8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	keystone	Not implemented	Custom extension can be built to allow tracking of all user activities	
	8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use	keystone	Not implemented	Custom extension can be built to support using OTP	
	8.5.5 Remove/disable inactive user accounts at least every 90 days.	keystone	Not implemented	Custom extension should be built for checking system accounts and blocking them after 90 days. If LDAP or other external catalogue is used it's up to the customer to enforce such policies	
	8.5.8 Do not use group, shared, or	all components	Implemented	Mirantis provides configuration that removes all shared user	
	8.5.9 Change user passwords at least every 90 days.	keystone	Not implemented	Custom extension should be built to support enforcing strong password policies when using internal Keystone accout system. If LDAP or other external catalogue is used it's up to the customer to enforce such policies	
	8.5.10 Require a minimum password length of at least seven characters.	keystone	Not implemented	Custom extension should be built to support enforcing strong password policies when using internal Keystone accout system. If LDAP or other external catalogue is used it's up to the customer to enforce such policies	
	8.5.11 Use passwords containing both numeric and alphabetic characters.	keystone	Not implemented	Custom extension should be built to support enforcing strong password policies when using internal Keystone accout system. If LDAP or other external catalogue is used it's up to the customer to enforce such policies	
	8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	keystone	Not implemented	Custom extension should be built to support enforcing strong password policies when using internal Keystone accout system. If LDAP or other external catalogue is used it's up to the customer to enforce such policies	
	8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	keystone	Not implemented	Custom extension should be built to implement account locking and unlocking. If LDAP or other external catalogue is used it's up to the customer to enforce such policies	
	8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	keystone	Not implemented	Custom extension should be built to implement account locking and unlocking. If LDAP or other external catalogue is used it's up to the customer to enforce such policies	
	8.5.15 If a session has been idle for	keystone	Implemented	OpenStack allows configuring keystone tokens to be valid for	

Notes on 10.1

Requirement 10: Track and monitor all access to network resources and cardholder data					
Requirement	**Sub requirement**	**Affected**	**Impl. status**	**Way to implement with OpenStack**	**Additional notes**
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.					
		operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
10.2 Implement automated audit trails for all system components to reconstruct the following events:					
	10.2.2 All actions taken by any	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.2.4 Invalid logical access	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.2 5 Use of identification and	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.2.6 Initialization of the audit logs	operating system	Implemented	We provide system audit daemon configuration allowing	
	10.2.7 Creation and deletion of	operating system	Implemented	We provide system audit daemon configuration allowing	
10.3 Record at least the following audit trail entries for all system components for each event:					
	10.3.1 User identification	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.3.2 Type of event	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.3.3 Date and time	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.3.4 Success or failure indication	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.3.5 Origination of event	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
	10.3.6 Identity or name of affected	operating system	Implemented	We provide system audit daemon configuration allowing	
		all OpenStack	Not implemented	Custom extension would need to be developed to allow	
10.4 Synchronize all critical system clocks and times.					
		operating system	Implemented	Customer has to provide internal time sources that are then	
10.5 Secure audit trails so they cannot be altered.					
	10.5.1 Limit viewing of audit trails to	external	Implemented	Audit trails can be sent to external system and it's up to the	
	10.5.2 Protect audit trail files from	external	Implemented	Audit trails can be sent to external system and it's up to the	
	10.5.3 Promptly back up audit trail	external	Implemented	Local copies of audit trails are not backed up. It's up to the	
	10.5.4 Write logs for external-facing	external	Implemented	Audit trails can be sent to external system	
	10.5.5 Use file-integrity monitoring	operating system	Implemented	We provide configuration for file integrity monitoring software	

Roadmap

- Publication will be annouced on Mirantis blog
- Planned date: end of 2013

Questions?

MIRANTIS