Barbican:
Protect your Secrets at Scale

OWASP
The Open Web Application Security Project

Matt Tesauro
AppSec EU 2014

OWASP
The Open Web Application Security Project

about us

Jarret Raim

ACADEMIC — LEHIGH UNIVERSITY

DEVELOPER — SRI

SECURITY CONSULTANT — DENIM GROUP

SECURITY ARCHITECT

SECURITY PRODUCTS

Matt Tesauro

OWASP BOARD MEMBER (former)

OWASP LIVE CD

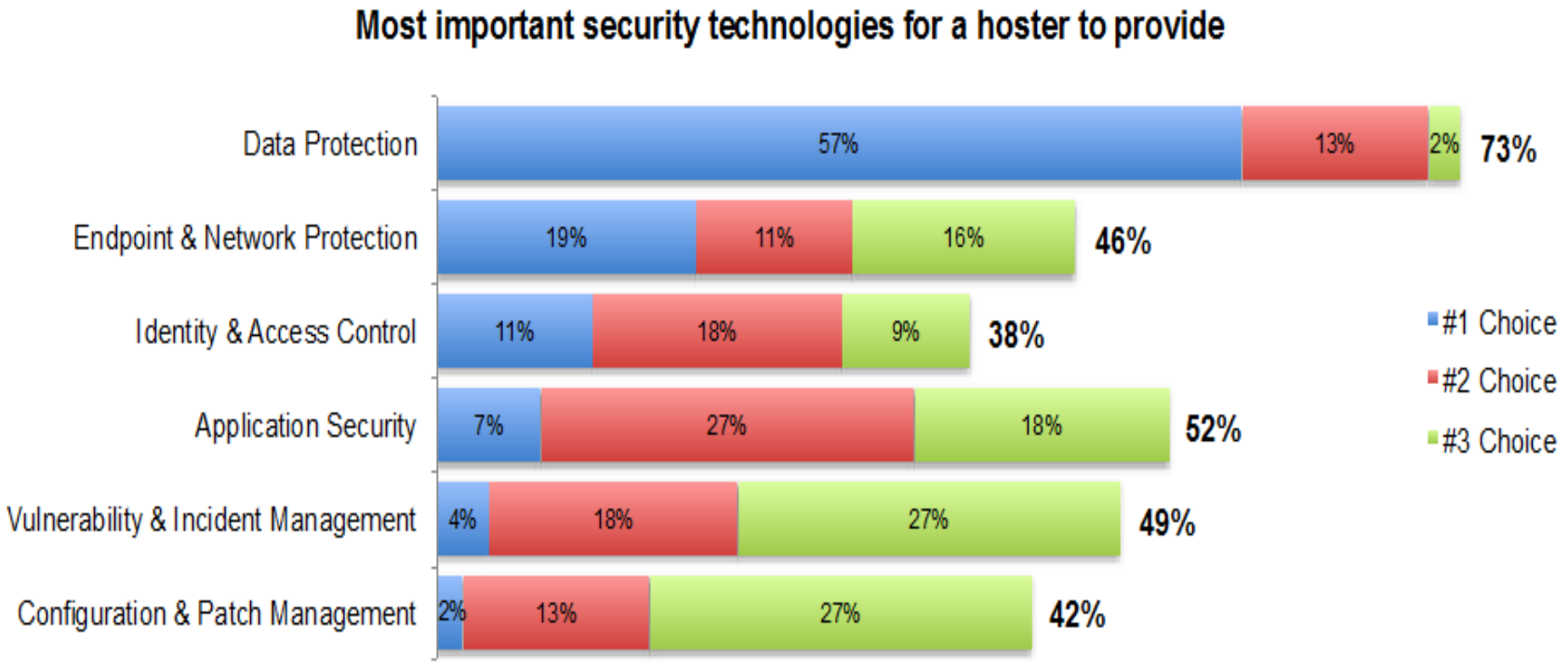
OWASP WTE

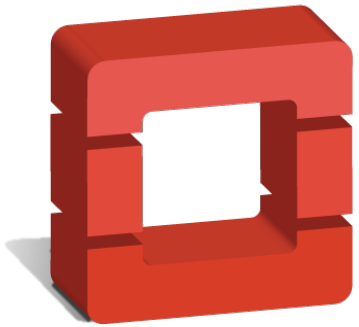
RACKER SINCE ‘11

PRODUCT SECURITY

HACKING THE RACK

Lets ask some customers...





openstack™
CLOUD SOFTWARE

Swift & Glance

Encrypted files at rest.

Trove

Encrypted databases and tables.

Neutron

SSL Certificates and VPN keys.

Nova & Ironic

SSH keys, encrypted file systems.

Keystone

Encrypted metadata, user level keys.

Cinder

Transparent volume encryption.

Heat

AES, SSH & SSL key management.

Marconi

Encrypted queue messages.

Savanna

Analytics on encrypted data.

OSLO

Support all the things.

Custom Dev

Settings

Commonly exposed settings including credentials can be protected either through encryption or by storing the entire settings file.

Encryption Keys

Keys used to provide encryption for data at rest.

SSL Keys

SSL / TLS private keys.

SSH Keys

Keys used for access control.

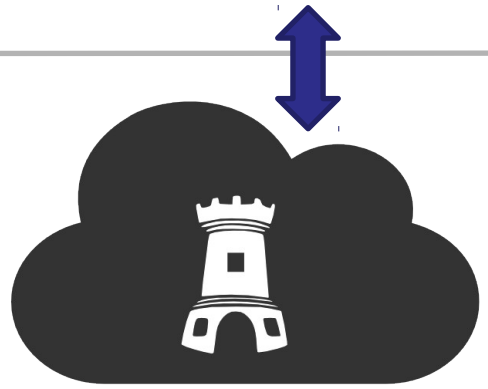
Interaction Models

Least secure

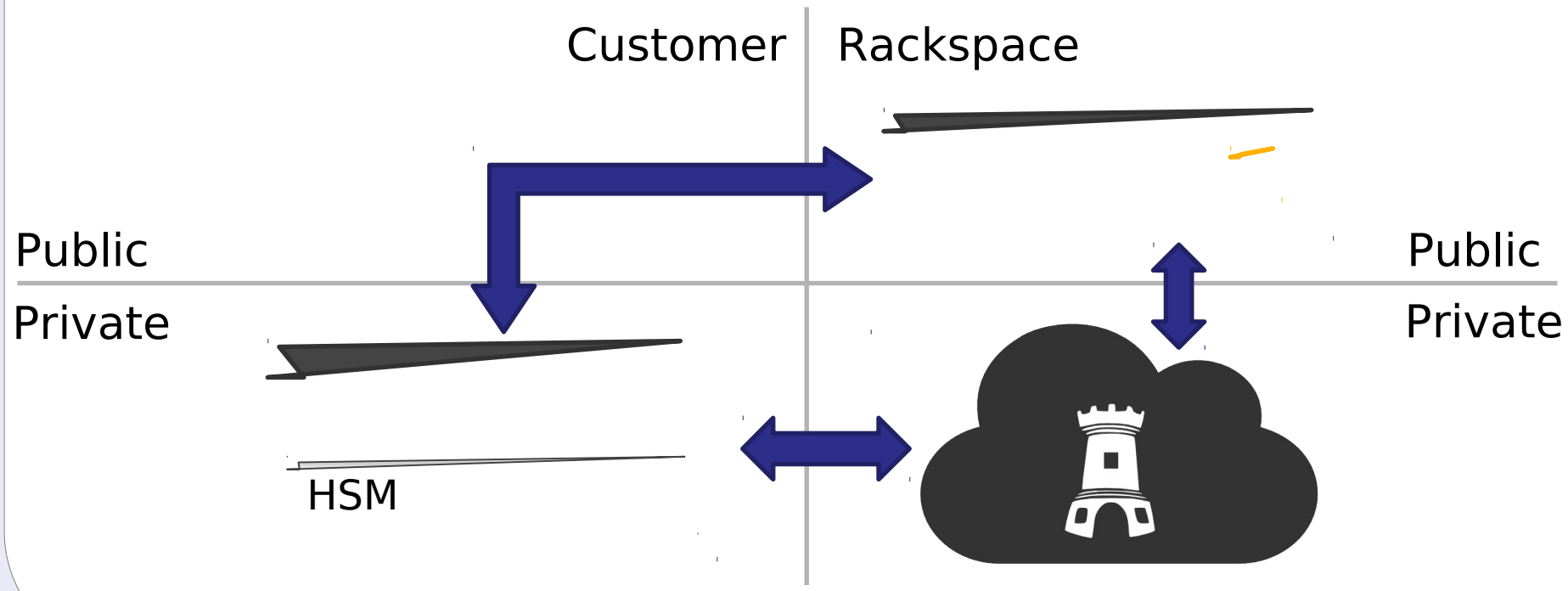
Most secure

Transparent Encryption

Customer	Rackspace
Public	Public
Private	Private



Federated Keys

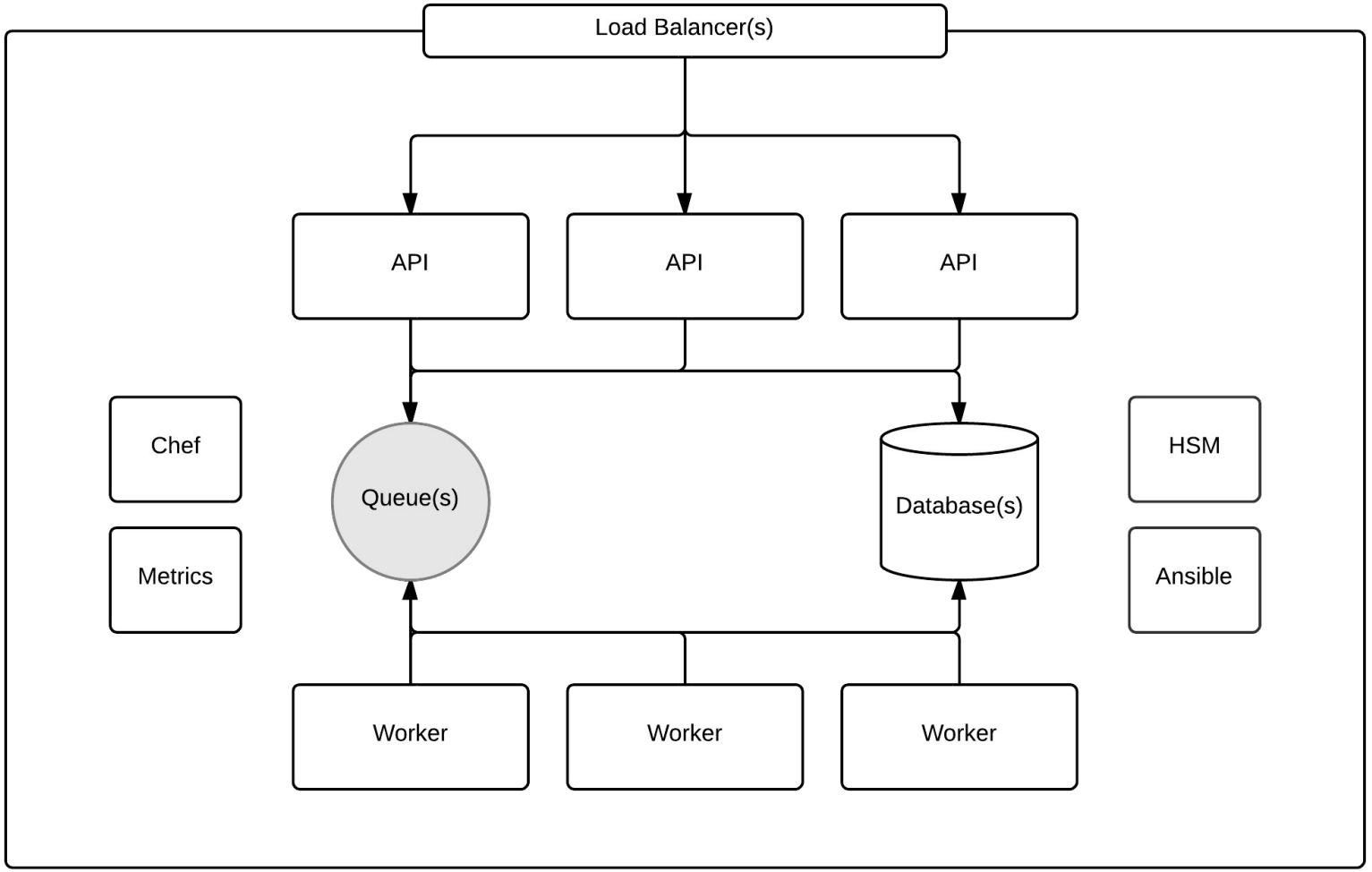


On PRemise

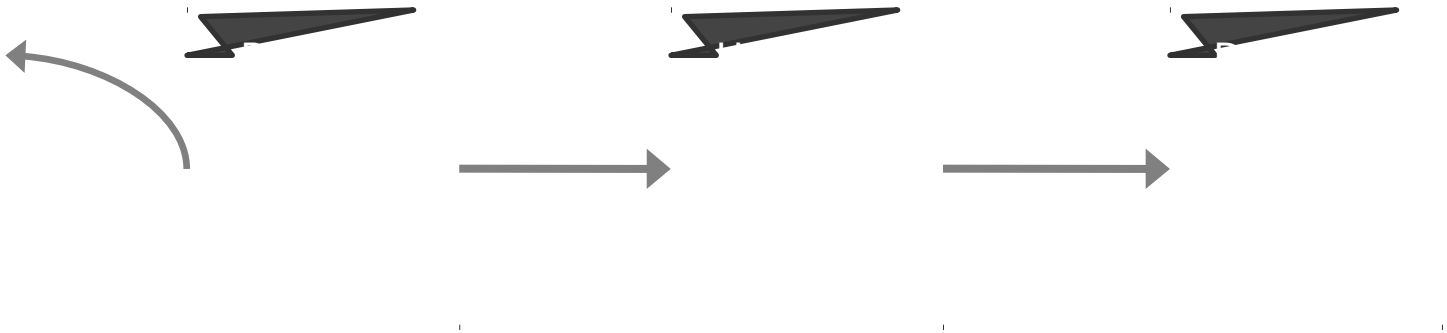
	Customer	Rackspace
Public		Public
Private		Private
	 HSM	

OWASP
The Open Web Application Security Project

Vagrant Up


Load Balancer(s)
API
API
API
Chef
Metrics
Queue(s)
Database(s)
HSM
Ansible
Worker
Worker
Worker

Key Storage

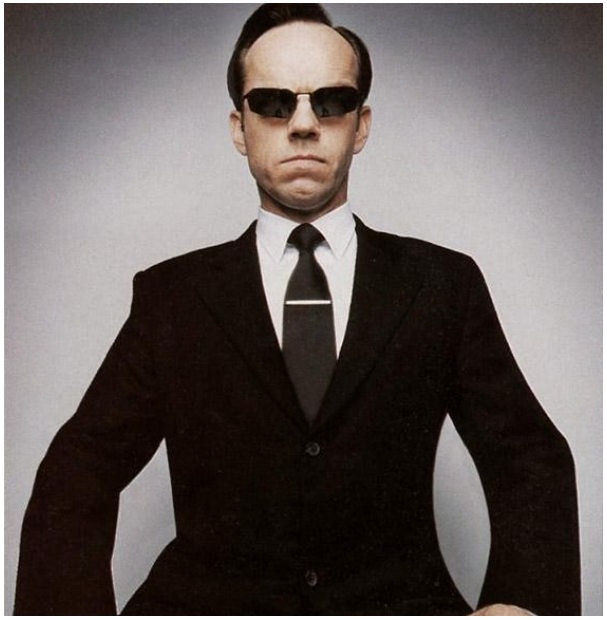


All keys are encrypted with a tenant-level key encryption key (KEK).

This key never leaves the HSM (if using one).

The encrypted data encryption key (DEK) is stored in the Barbican data store.

The Agent



Legacy Application Integration

The agent presents a FUSE file system to allow applications easy integration options.

Enforces Policies

Each secret has a set of policies that dictate its use. These policies are mostly enforced by the agent.

Keystone Integrated

The agent uses keystone for identity, pairing and policy management.

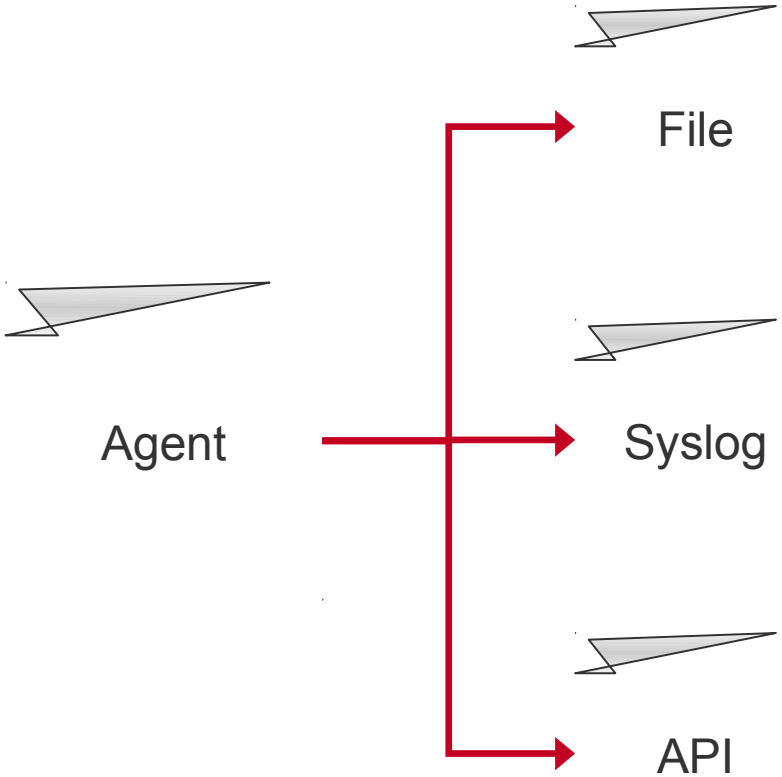
Out of Band Communication

The agent communicates with the API to represent real-time data about secret usage.

Example Policy

```
{
  "policies": [
    {
      "time_available_after_reboot": 10,
      "uuid": "26fb0877-9f6f-46ef-9c62-1338629cecb1",
      "keys": [
        {
          "secret": "ooGeewoz1choh9aiphaih4Ruu8AixiHohcoocoot6l",
          "group": "myapp",
          "uuid": "26fb0877-9f6f-46ef-9c62-1338629cecb1",
          "expiration": "2015-06-30T00:00:00",
          "owner": "myapp",
          "cachecable": false,
          "mime_type": "application/aes-256-cbc",
          "filename": "configuration_key"
        }
      ],
      "tenant_id": 123,
      "max_key_accesses": 1,
      "directory_name": "/etc/keys",
      "name": "Example, Inc"
    }
  ]
}
```

Events Auditing



- Multiple log options, specified by central policy & local configuration
- API logging provides a compliant streaming log solution
- More likely for a log to escape a compromised server
- PANICs and other events surfaced via API
- API can respond to events on the agent

Demo Time

Future Work

KMIP Support

There is a possibility that a Python KMIP client will be open-sourced by Safenet soon. If so, we'll integrate it, if not, we'll build our own.

SSL / TLS

Barbican will support the provisioning of SSL certificates from internal and external CAs.

Federation

Support for federated keys in both Barbican to Barbican and Barbican to HSM configurations.

Integrations

Barbican will help OpenStack teams integrate to provide encryption services.

OWASP
The Open Web Application Security Project

Integrate Now

Python-Barbicanclient

Provides both a programmatic and command line interface to a Barbican instance.

Source Code & Documentation

The documentation and source code both reside on GitHub in the CloudKeep organization. Blueprints and project documentation is on Launchpad.

Integration Environment

Barbican maintains an integration environment on Public Cloud for testing. Not for use in production deploys, but usable for testing / dev.

```
from barbicanclient import client

barbican_client = client.Client(endpoint='http://path-to-barbican',
    tenant_id='tenant_id_for_context')

barbican_client.secrets.store(name, payload, payload_content_type,
    payload_content_encoding, algorithm, bit_length, mode, expiration)

barbican_client.orders.create(name, payload_content_type, algorithm,
    bit_length, mode, expiration)
```

```
usage: keep [-h] [--no-auth | --os-auth-url <auth-url>]
    [--os-username <auth-user-name>] [--os-password <auth-
    password>] [--os-tenant-name <auth-tenant-name>] [--os-tenant-id
    <tenant-id>] [--endpoint <barbican-url>]
    <entity> <action> ...
```

OWASP
The Open Web Application Security Project

~ fin ~

#openstack-coudkeep
github.com/cloudkeep

barbican@lists.google.com