STEPPING OFF A CLIFF: COMMON SENSE APPROACHES TO CLOUD SECURITY

Mike Bursell
Chief Security Architect, Red Hat

Ted Brunell
Principal Solution Architect, Red Hat
DoD Programs
@DoDCloudGuy

Jared Sanders
Principal Operations Engineer
Tapestry Technologies
AGENDA

● Overview of Current Security Risks
● Security In the Hybrid Cloud
● Identity, Lifecycle and Configuration Management
● Using Placement and APIs
● Governance in Hybrid Clouds

● How Industry Incorporates These Ideas Today

“Hybrid cloud computing refers to policy-based and coordinated service provisioning, use and management across a mixture of internal and external cloud services.” - Gartner IT Glossary
TOP IT SECURITY RISKS

What is the greatest security risk to your organization?

- Internal attack by an employee: 11%
- Employees not taking the proper security measures: 36%
- Bring your own device/mobile security: 3%
- Unpatched or unpatchable devices: 14%
- Outside breach: 32%
- Shadow IT: 4%

Source: TechValidate survey of 385 users of IT Security
BUSINESS CONCERNS ON SECURITY

What is the top business concern for your organization related to security?

- Revenue loss: 12%
- Not able to access your data and resources: 19%
- Negativity toward your company/brand: 22%
- Customer trust: 47%

Source: TechValidate survey of 373 users of IT Security
OTHER INTERESTING STATS

Security updates
How often do you install security updates?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>14%</td>
</tr>
<tr>
<td>Weekly</td>
<td>28%</td>
</tr>
<tr>
<td>Monthly</td>
<td>25%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>19%</td>
</tr>
</tbody>
</table>

Source: TechValidate survey of 351 users of IT Security

Plans for hybrid cloud environments
Are you currently running both traditional and cloud-based IT environments?

- Yes: 61%
- No, but have plans to do so in the near future: 12%
- No, but evaluating: 15%
- No plans to do so: 12%

Source: TechValidate survey of 606 users of Red Hat Enterprise Linux
THE THREAT

DoS - Termination of Guest
Activity within an individual guest or host that impacts the ability for the host to effectively run virtual machines.

Escaping Confinement
Bypassing the protection provided by the hypervisor or container host to execute code.
- workload-to-host
- workload-to-workload
- host-to-workload

Memory Corruption/Leakage
Ability to corrupt or access guest memory from outside the constraints of the virtual machine.
SECURITY IN THE HYBRID CLOUD

Look at the whole picture and integrate existing management systems
SECURITY IN THE HYBRID CLOUD
Look at the whole picture and integrate existing management systems

- Security cannot exist solely at the platform level - but it should still exist
- Deploy diverse tools that can interoperate
- Design for diverse and distributed environments
- Work with existing physical and virtual resources
- Tools implemented based on requirements and capabilities
- Able to handle emerging technologies, threats and vulnerabilities
## Challenges to Configuration Management

<table>
<thead>
<tr>
<th></th>
<th>Traditional Environment</th>
<th>Cloud Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mapping to configuration items (CIs)</td>
<td>1 system &lt;=&gt; 1 CI</td>
<td></td>
</tr>
<tr>
<td>Relationships between CIs</td>
<td>Easy to maintain</td>
<td></td>
</tr>
<tr>
<td>Configuration changes / update</td>
<td>Tracked by CM (Configuration Management) processes</td>
<td></td>
</tr>
<tr>
<td>Incident reporting system</td>
<td>Integrated with CM database</td>
<td></td>
</tr>
<tr>
<td>Identity management</td>
<td>Single identity source</td>
<td></td>
</tr>
</tbody>
</table>
## Challenges to Configuration Management

<table>
<thead>
<tr>
<th></th>
<th>Traditional Environment</th>
<th>Cloud Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mapping to configuration items (CIs)</td>
<td>1 system &lt;=&gt; 1 CI</td>
<td>Challenged by dynamic changes</td>
</tr>
<tr>
<td>Relationships between CIs</td>
<td>Easy to maintain</td>
<td>Relationships change as apps deployed, scaled, terminated</td>
</tr>
<tr>
<td>Configuration changes / update</td>
<td>Tracked by CM (Configuration Management) processes</td>
<td>Difficult to track</td>
</tr>
<tr>
<td>Incident reporting system</td>
<td>Integrated with CM database</td>
<td>Requires additional integration with cloud infrastructure</td>
</tr>
<tr>
<td>Identity management</td>
<td>Single identity source</td>
<td>Multi-tenant identity source(s)</td>
</tr>
</tbody>
</table>
IDENTITY, LIFECYCLE AND CONFIGURATION MANAGEMENT

Automation helps solve the problem
- Create repeatable processes
- Reduce human errors (36% not taking proper security measures)
- Removes guesswork and can be validated with reports
- Ensure systems stay in compliance with local policies

“59% of surveyed IT organizations agree mitigating risk is very important in terms of issues they face regarding cloud computing and security.” - Source: TechValidate. https://www.techvalidate.com/tvid/20A-788-046
IDENTITY, LIFECYCLE AND CONFIGURATION MANAGEMENT

Automation helps solve the problem

- Create repeatable processes
- Reduce human errors (36% not taking proper security measures)
- Removes guesswork and can be validated with reports
- Ensure systems stay in compliance with local policies

Integrate Identity, Lifecycle and Configuration Management

- Register and patch new workloads during provisioning - security from the beginning
- Ensure access control and configuration knowledge is managed throughout the lifecycle
- On workload termination, remove from lifecycle and identity management services
- Data cleanup (Physical and SD Network Layer, Virtualization/Container Layer, Storage Layer)
- Legacy systems are still included

“59% of surveyed IT organizations agree mitigating risk is very important in terms of issues they face regarding cloud computing and security.” - Source: TechValidate. https://www.techvalidate.com/tvid/20A-788-046
Using Placement and APIs
Using Placement and APIs
Internal != Public and other suggestions

Secure endpoints with TLS
  ● Proxies & load balancing
Placement
  ● Protect sensitive components
Internal API endpoints
  ● Included in the Identity service catalog
  ● Avoid internal comms on public endpoints
  ● Services use Internal API
Isolate the endpoints
  ● Network Namespaces and Policy
  ● Mandatory Access Controls (aka SELinux)
Rate Limiting - especially on the public network
  ● Defeat denial of service attacks

[root@overcloud-controller-0 ~]# openstack endpoint show neutron

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>adminurl</td>
<td><a href="http://192.168.162.38:9696/">http://192.168.162.38:9696/</a></td>
</tr>
<tr>
<td>enabled</td>
<td>True</td>
</tr>
<tr>
<td>id</td>
<td>5ab9045319884e9e97ef38f69388393d</td>
</tr>
<tr>
<td>internalurl</td>
<td><a href="http://192.168.162.38:9696/">http://192.168.162.38:9696/</a></td>
</tr>
<tr>
<td>region</td>
<td>regionOne</td>
</tr>
<tr>
<td>service_id</td>
<td>f866b2a9edc741f396cc87a1cf83db62</td>
</tr>
<tr>
<td>service_name</td>
<td>neutron</td>
</tr>
<tr>
<td>service_type</td>
<td>network</td>
</tr>
</tbody>
</table>

# URL for connecting to neutron (string value)
#url=http://127.0.0.1:9696
url=http://192.168.162.38:9696
GOVERNANCE IN HYBRID CLOUDS

Governance is a set of policies applied to cloud computing services with the goal of securing applications and data.

- Policy enforcement and remediation via APIs
- Real-time monitoring
- Segmentation of users and resources
  - Tenants and groups within tenants
  - Hardware classification
- Configuration tracking, auditing and drift-analysis
- Enforced quotas
- Device discovery
- View relationships between resources and workloads
HOW INDUSTRY INCORPORATES THESE IDEAS TODAY

Jared Sanders
Principal Operations Engineer,
Tapestry Technologies
STATE OF THE ARCHITECTURE

Current State
- Traditional Virtualization
- Physical Compute & Network
- Mainframes

Evolution of the Data Center
- Private Cloud: Enhance & Augment Traditional Hosting
- Migration to Commercial & Private Cloud
- New Commercial Cloud Security Architecture
ORCHESTRATOR BLUEPRINT VISUALIZATION

Ordering Portal

Service Catalog

Storefront

Multi Cloud Orchestrator

Configuration Management

Orchestration & Automation Suite

Commercial Cloud

Traditional Hosting

On-Premise Cloud

Deployment Environments
ORDERING PROCESS: END-TO-END EXAMPLE

Mission Owner

Commercial Cloud
- Traditional Hosting
- On-Premise Cloud
  Infrastructure Selection

Engineering
- Service Desk
- Accreditation
  Optional Services
  Storefront

LAMP
- RHEL
- Windows
- Solaris
  OS Image Selection
- Exchange
- SharePoint
  VDC Selection
  Orchestration

RHEL
- Apache
- MySQL
- PHP
  VDC Components

Security Settings
- Monitoring Agent
  Security & Tools Selection
  Configuration Management
CLOSED LOOP OPERATIONS

- **Application Auto-Scaling**
  - Real-time Monitoring
  - Orchestrator Integration

- **Cyber Tool Integration**
  - Improve Reactions
  - Alert and Act
  - Enable Automated Action

- **Automated Action**
  - Quarantine
  - Honey Pot
  - Decommission and Re-provision
ULTIMATE CHALLENGES

**Business Process**
- Isolation to Automation
- Retire Legacy Processes
- Merge Technology and Process

**Storefront**
- Enable Cloud Adoption
- Diverse Offerings
- Common Security Services
OPS HAS CHANGED.

The next I.T. is never static.
Collaboration is now a requirement.
Security is non-negotiable.
The platform is hybrid.
Digital innovation is the goal.

HOW YOU MANAGE OPS HAS TO CHANGE, TOO.
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHatNews
LEARN. NETWORK. EXPERIENCE OPEN SOURCE.