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

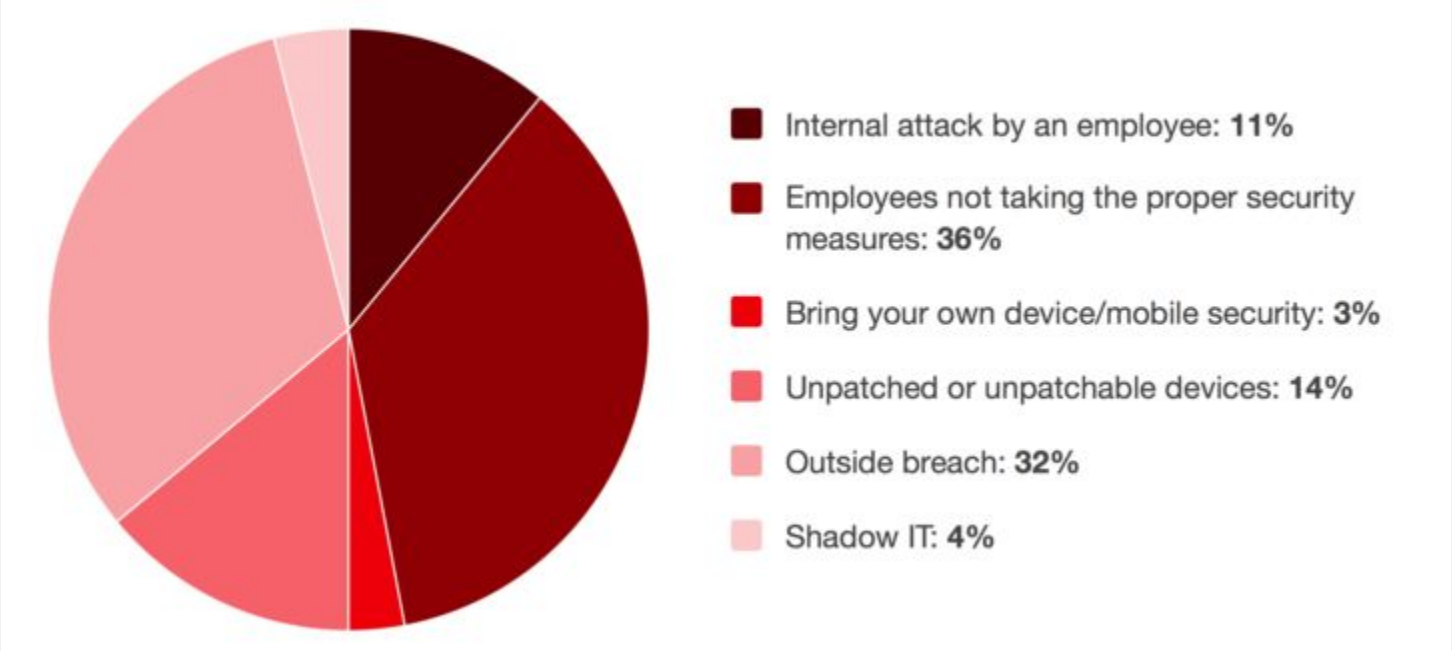
- Overview of Current Security Risks
- Security In the Hybrid Cloud
- Identity, Lifecycle and Configuration Management
- Using Placement and APIs
- Governance in Hybrid Clouds

- 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

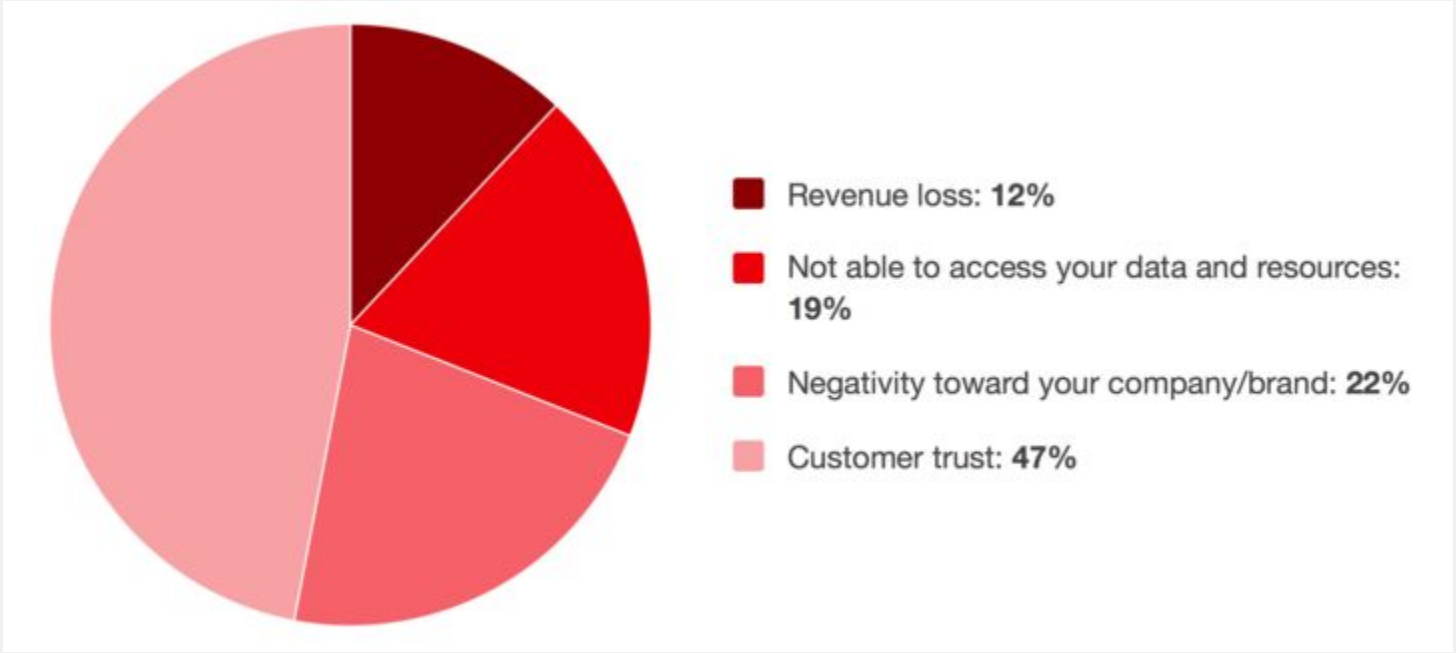
What is the greatest security risk to your organization?



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?

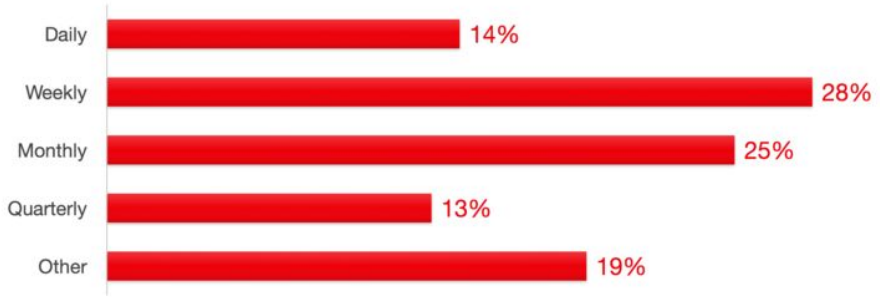


Source: TechValidate survey of 373 users of IT Security

OTHER INTERESTING STATS

Security updates

How often do you install security updates?



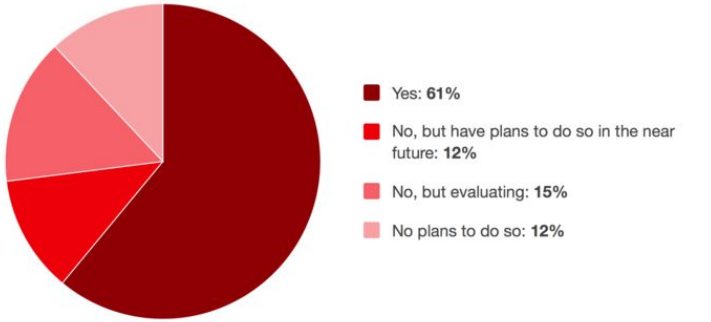
Source: TechValidate survey of 351 users of IT Security

Validated Published: Feb. 16, 2016 TVID: BED-F58-E27

redhat. TechValidate

Plans for hybrid cloud environments

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

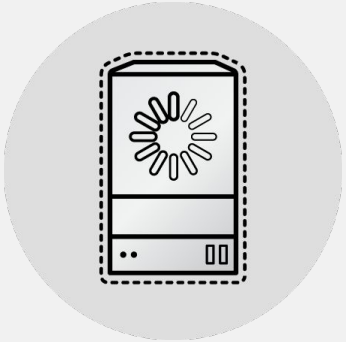


Source: TechValidate survey of 606 users of Red Hat Enterprise Linux

Validated Published: Jan. 22, 2016 TVID: E43-E2F-8B6

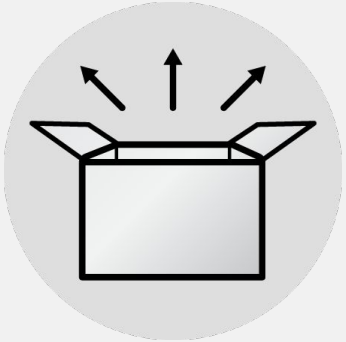
redhat. TechValidate

THE THREAT



DoS - Termination of Guest

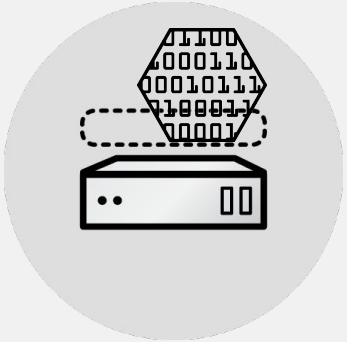
Activity within an individual guest or host that impacts the ability for the host to effectively run virtual machines



Escaping Confinement

Bypassing the protection provided by the hypervisor or container host to execute code.

- workload-to-host
- workload-to-workload
- host-to-workload

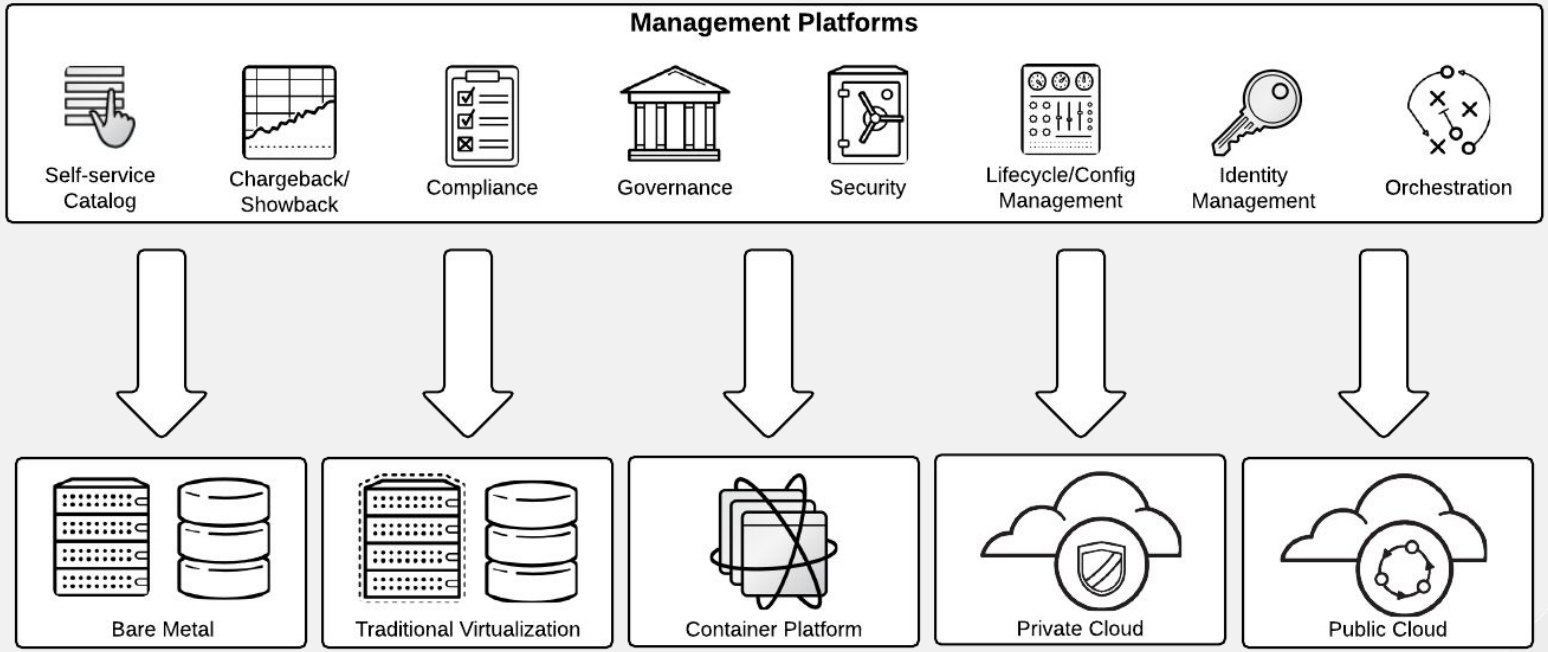


Memory Corruption/Leakage

Ability to corrupt or access guest memory from outside the constraints of the virtual machine

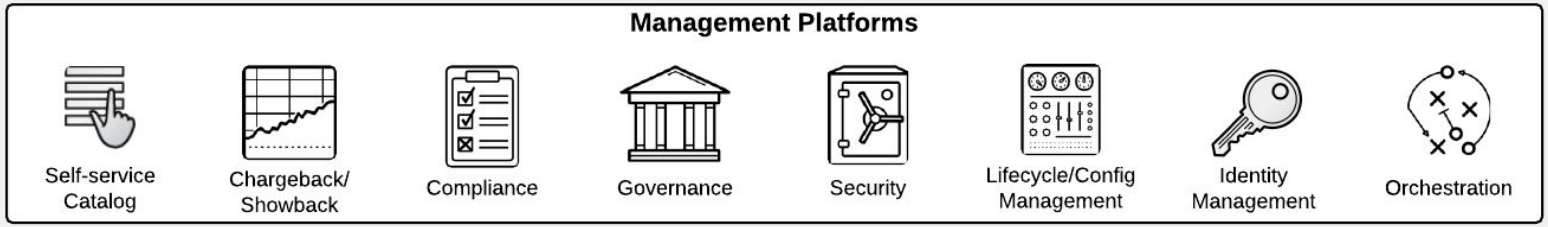
SECURITY IN THE HYBRID CLOUD

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

IDENTITY, LIFECYCLE AND CONFIGURATION MANAGEMENT

Challenges to Configuration Management

	Traditional Environment	Cloud Environment
Mapping to configuration items (CIs)	1 system <=> 1 CI	
Relationships between CIs	Easy to maintain	
Configuration changes / update	Tracked by CM (Configuration Management) processes	
Incident reporting system	Integrated with CM database	
Identity management	Single identity source	

IDENTITY, LIFECYCLE AND CONFIGURATION MANAGEMENT

Challenges to Configuration Management

	Traditional Environment	Cloud Environment
Mapping to configuration items (CIs)	1 system <=> 1 CI	Challenged by dynamic changes
Relationships between CIs	Easy to maintain	Relationships change as apps deployed, scaled, terminated
Configuration changes / update	Tracked by CM (Configuration Management) processes	Difficult to track
Incident reporting system	Integrated with CM database	Requires additional integration with cloud infrastructure
Identity management	Single identity source	Multi-tenant identity source(s)

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

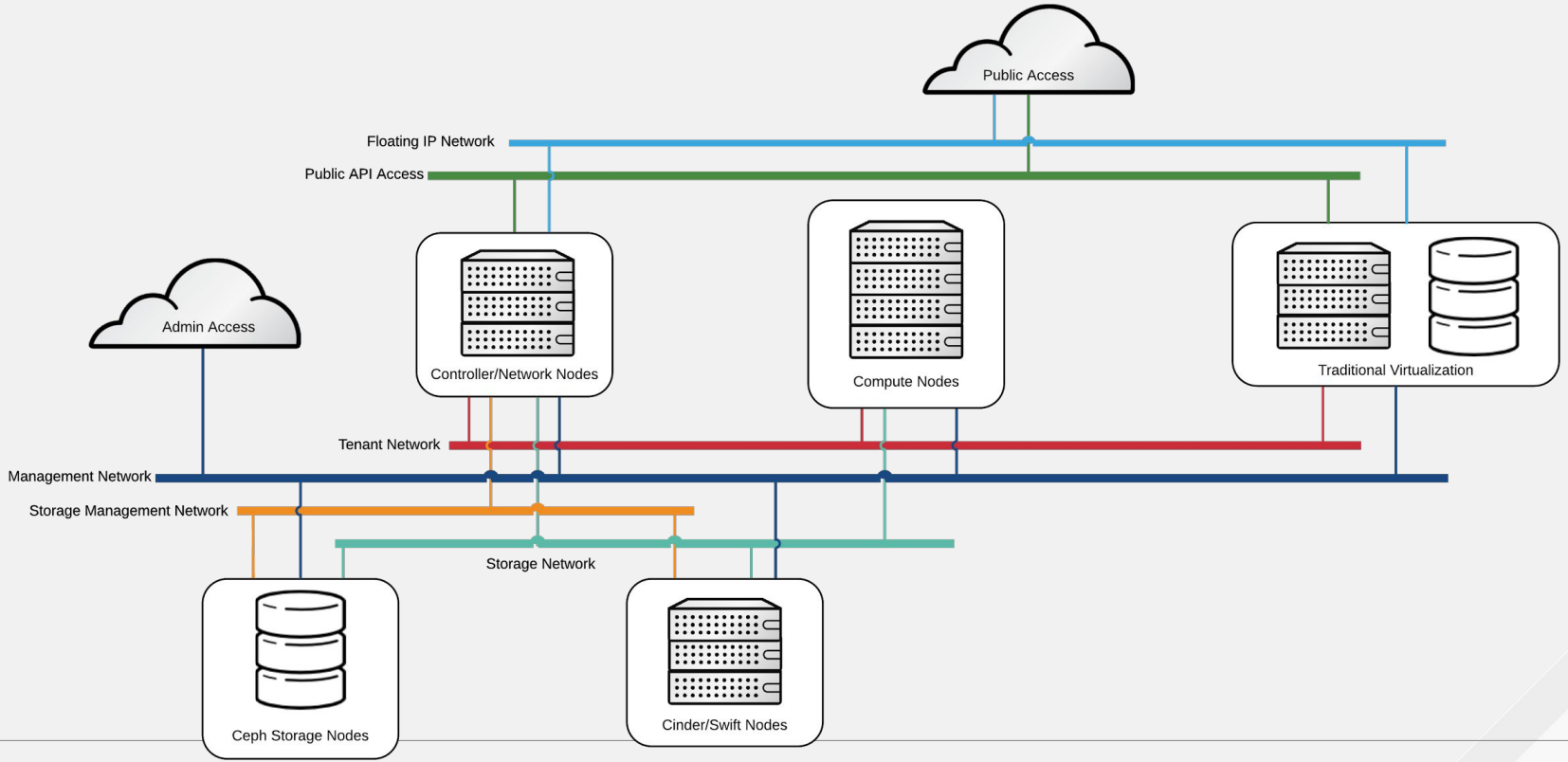
- Create **repeatable processes**
- **Reduce human errors** (36% not taking proper security measures)
- **Removes guesswork** and can be validated with reports
- Ensure systems stay in **compliance with local policies**

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
+--------------+----------------------------------+
| Field        | Value                            |
+--------------+----------------------------------+
| adminurl     | http://192.168.102.30:9696/      |
| enabled      | True                             |
| id           | 5ab9045319884e8e87ef38f68308093d |
| internalurl  | http://192.168.102.30:9696/      |
| publicurl    | http://192.168.100.30:9696/      |
| region       | regionOne                        |
| service_id   | f86682a9edc741f396cc07a1cf83db62 |
| service_name | neutron                          |
| service_type | network                          |
+--------------+----------------------------------+
```

```
# URL for connecting to neutron (string value)
#url=http://127.0.0.1:9696
url=http://192.168.102.30:9696
```

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

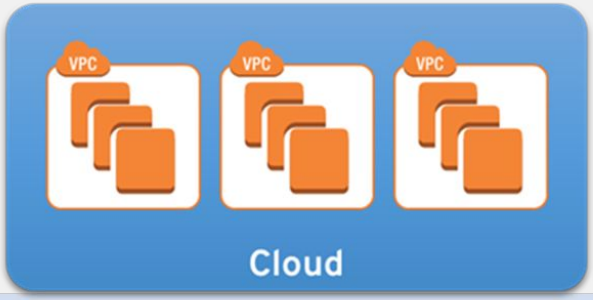
HOW INDUSTRY INCORPORATES THESE IDEAS TODAY

Jared Sanders
Principal Operations Engineer,
Tapestry Technologies

STATE OF THE ARCHITECTURE

Current State

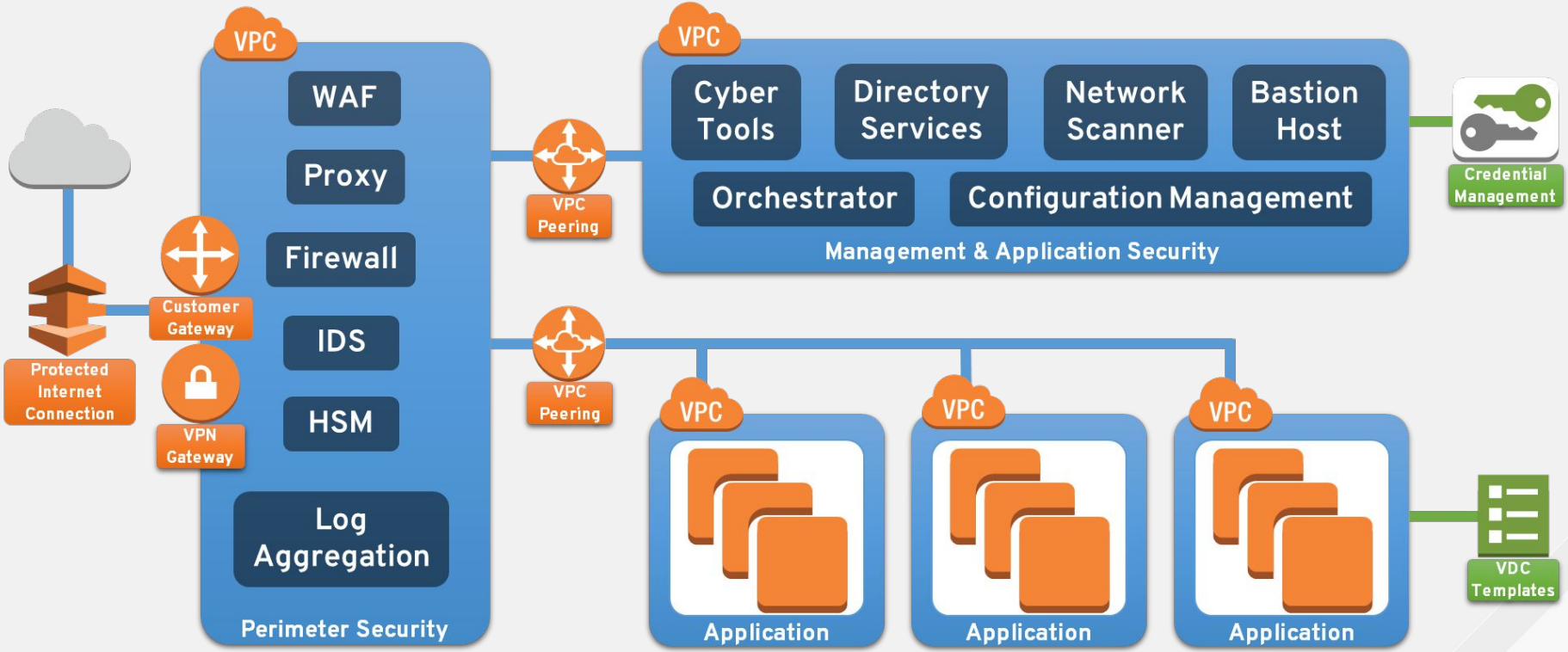
- Traditional Virtualization
- Physical Compute & Network
- Mainframes



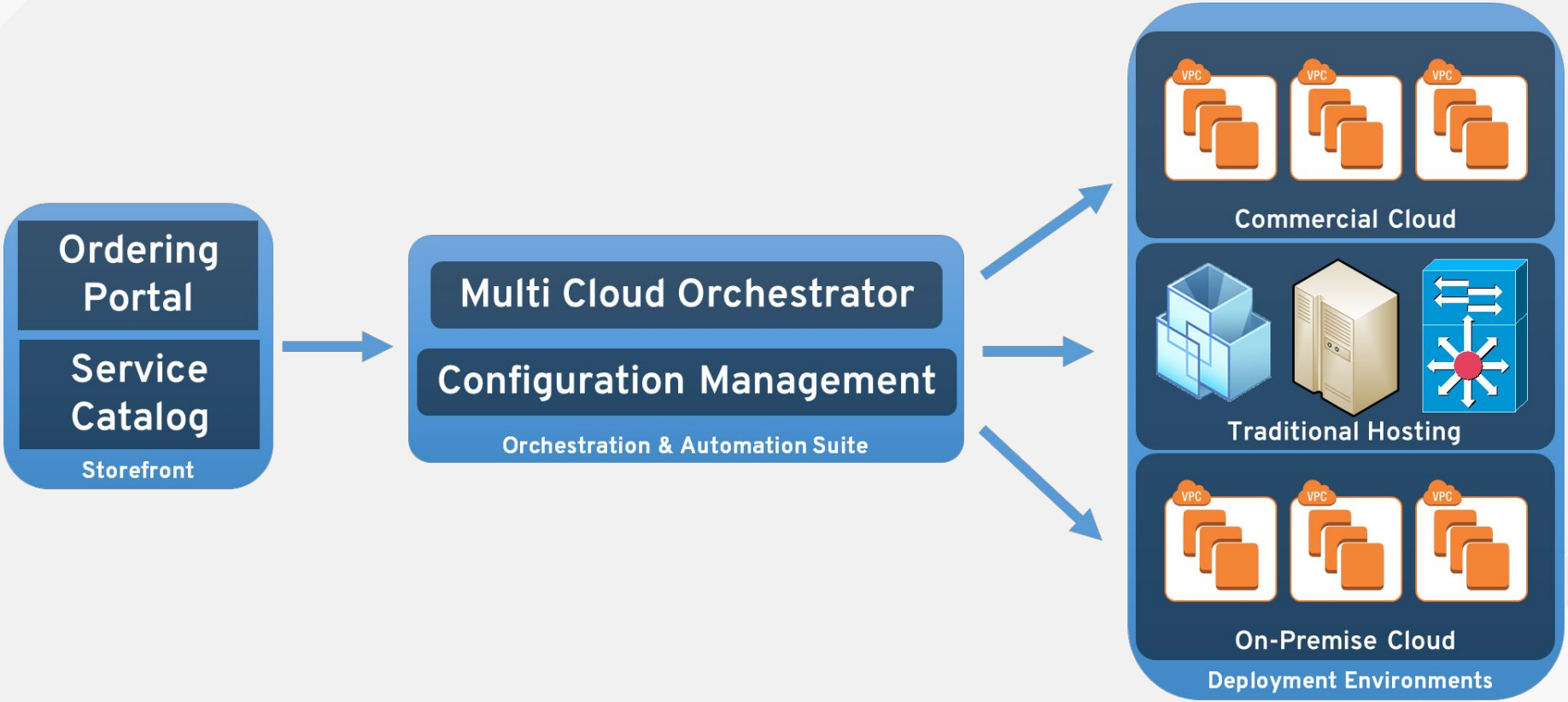
Evolution of the Data Center

- Private Cloud: Enhance & Augment Traditional Hosting
- Migration to Commercial & Private Cloud
- New Commercial Cloud Security Architecture

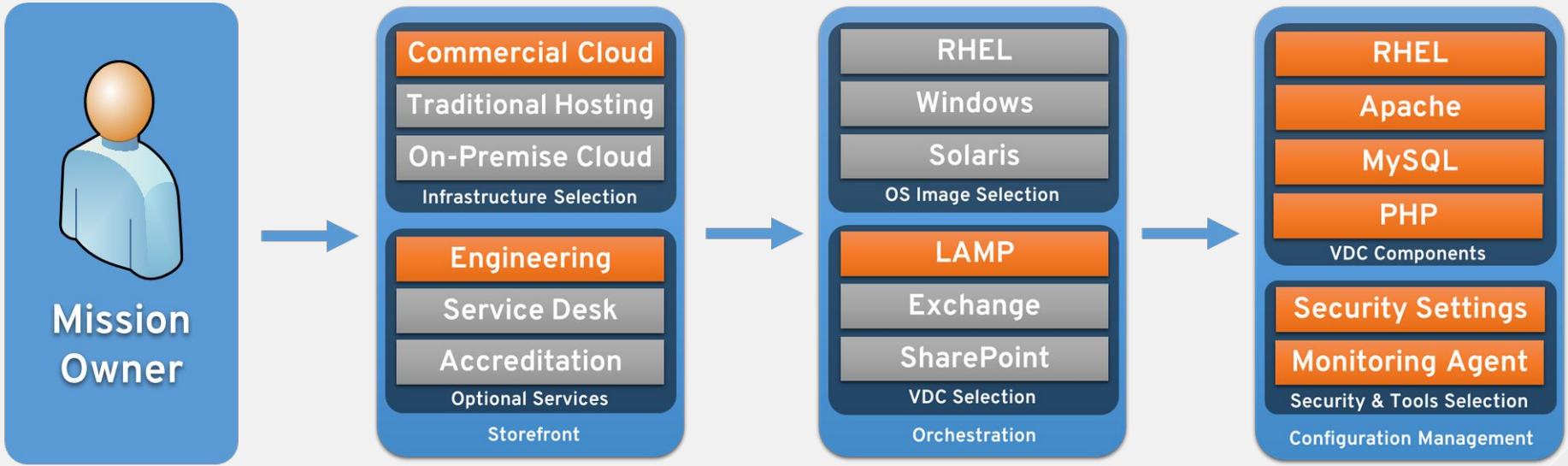
ARCHITECTURAL VISUALIZATION: CLOUD



ORCHESTRATOR BLUEPRINT VISUALIZATION



ORDERING PROCESS: END-TO-END EXAMPLE



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.

RED HAT SUMMIT

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos

LEARN. NETWORK.
EXPERIENCE
OPEN SOURCE.