SECURITY AT THE EDGE

Ansible to Automate Security for Edge Computing

Kevin Jones
Cloud Domain Architect

Red Hat

What we'll be discussing today

Define Edge

Use Cases

Automation Considerations

Edge at Red Hat

Project Hat Trick Demo

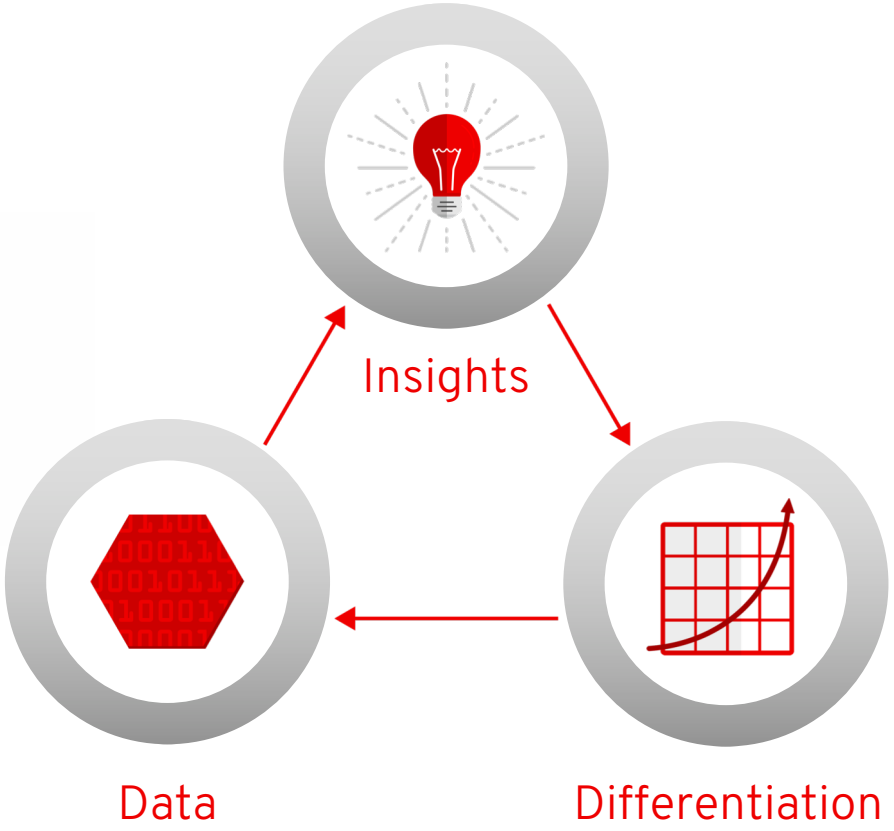
DEFINE EDGE

Edge is focused on
"where the workload is located."

Pivot from network centric services to workload centric services.

WHY DO EDGE COMPUTING?

Create a new, distributed architecture



React faster

Red Hat

BENEFITS OF EDGE COMPUTING ARCHITECTURE

Reduce Latency

Place processing power closer to the data source

Save Bandwidth

Reduce the amount of traffic that needs to travel back to the data center core

Increased Resilience

Continuous business operations in the event of unexpected site blackout

Data Sovereignty

Meet standards and compliance requirements

YOU ARE ON EDGE!

EDGE IS NOT SPECIFIC TO ANY INDUSTRY

- Telecommunications
- Manufacturing
- Retail
- Health–life science
- Transportation
- Public sector
- Many others

Red Hat

USE CASES

NETWORK FUNCTION VIRTUALIZATION
NEXT GENERATION MOBILE NETWORKS

Responsible for:

- Mobile connectivity
- Global Infrastructure
- Addiction to Facebook

Limiting Factors:

- Bandwidth
- Rural locations
- VNF Vendors

Requirements:

- Increase to 1G speeds
- Minimize truck roll
- Maximize privacy and data protection

MILITARY OPERATIONS

DATA CENTERS IN VEHICLES AND REMOTE STATIONS

Responsible for:

- Human lives

Limiting Factors:

- Hostile environments
- Limited connectivity
- Small, harsh spaces - Sand

Requirements:

- Ruggedized infrastructure
- Application availability for logistics, comms, etc.
- Tight access control (both physical and logical)

ON LOCATION TRAINING
BRING THE CLASSROOM TO THE STUDENTS

Responsible for:
- Student experience
- Sufficient lab resources

Limiting Factors:
- Limited connectivity
- Availability of materials
- Instructor transport

Requirements:
- Low power
- Portable infrastructure
- Multi-tenancy

DISASTER RESPONSE AND RECOVERY

WE THINK OF DR IN THE DATA CENTER. IMAGINE RESPONDING IN REAL LIFE

Responsible for:

- Response during
- Recovery after

Limiting Factors:

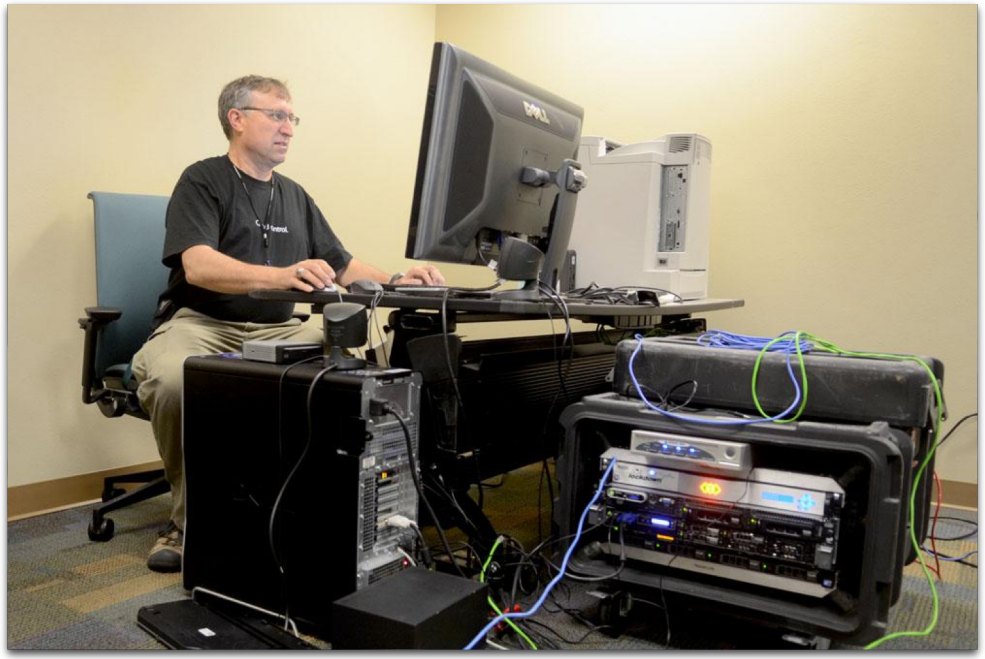
- Cell towers damaged
- Power out or unstable
- Multiple organizations

Requirements:

- Portable infrastructure
- Application availability for logistics, comms, etc.

CYBER SECURITY

THE BEST DEFENSE IS A GREAT OFFENSE



Responsible for:

- Network integrity
- Detection and defense
- Data security

Limiting Factors:

- Compromised situation
- Unknown enemy
- External connectivity

Requirements:

- Portable infrastructure
- Run tested tools

AUTOMATION CONSIDERATIONS

DEVICE AND NETWORK SECURITY CONSIDERATIONS FOR EDGE COMPUTING

Me hacking your IoT doorbell !!!

Physical

- Immutable device provisioning
- TPM enabled
- Encrypt local storage

Logical

- Encrypt all network traffic
- Service account access only
- Automatic key rotation

EXAMPLE: CERTIFICATE CREATION AND VALIDATION

```
- name: Create a challenge for sample.com using a account key from a variable.
  acme_certificate:
    account_key_content: "{{ account_private_key }}"
    csr: /etc/pki/cert/csr/sample.com.csr
    dest: /etc/httpd/ssl/sample.com.crt
   register: sample_com_challenge

- copy:
    dest: /var/www/html/{{ sample_com_challenge['challenge_data']['sample.com']['http-01']['resource'] }}
    content: "{{ sample_com_challenge['challenge_data']['sample.com']['http-01']['resource_value'] }}"
     when: sample_com_challenge is changed

- name: Let the challenge be validated and retrieve the cert and intermediate certificate
  acme_certificate:
    account_key_src: /etc/pki/cert/private/account.key
    csr: /etc/pki/cert/csr/sample.com.csr
    dest: /etc/httpd/ssl/sample.com.crt
    fullchain_dest: /etc/httpd/ssl/sample.com-fullchain.crt
    chain_dest: /etc/httpd/ssl/sample.com-intermediate.crt
     data: "{{ sample_com_challenge }}"
```


Source: https://docs.ansible.com/ansible/latest/modules/acme_certificate_module.html#acme-certificate-module

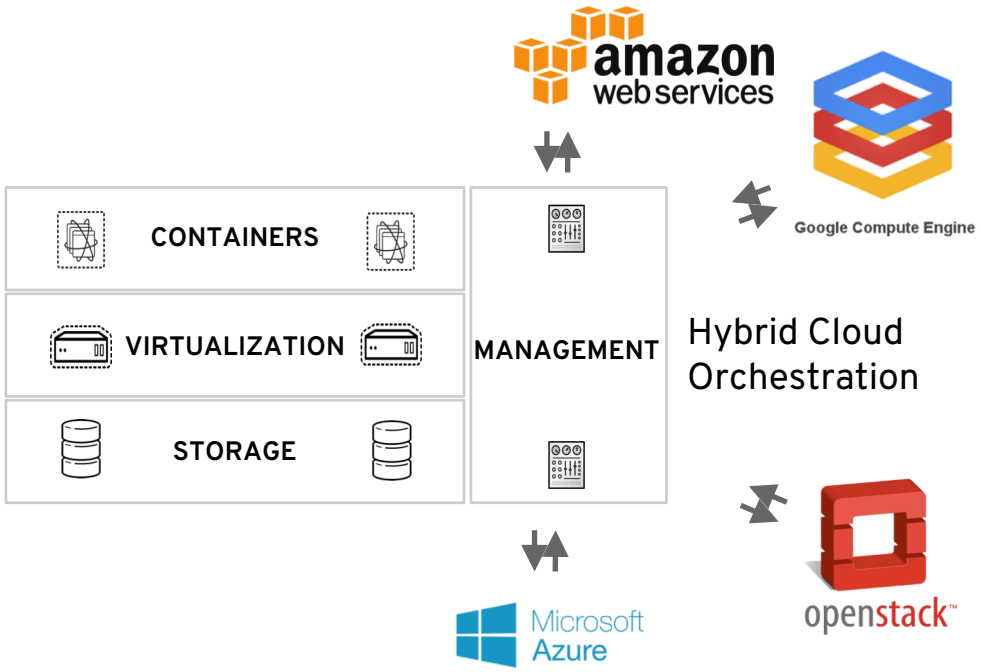
EXAMPLE: ENABLE TPM2 RESOURCE MANAGER

```
- name: Install necessary TPM packages
  become: yes
  yum:
    name: "tpm2-tools,tpm2-abrmd,tpm2-tss"
    state: present

- name: Enabled resource manager service and start now
  become: yes
  serice:
    name: tpm2-abrmd
    state: started
    enabled: true

- name: Take ownership of the TPM
  become: yes
  shell: "tpm2_takeownership -o {{ tpm_owner_pwd }} -e {{ tpm_endorse_pwd }} -l {{ tpm_lockout_pwd }}"
```

#NOTE: Luke Hinds has an ansible role which creates a TPM2 simulator https://github.com/lukehinds/ansible-tpm-simulator

Source: http://lukehinds.com/2018/08/28/TPM2-On-RHEL75.html

COMPONENTS AND SERVICES
CONSIDERATIONS FOR EDGE COMPUTING



Cloud Providers

- Ansible Cloud Modules
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

Private Infrastructure

- Containerization
- OpenStack
- Traditional Virt

EXAMPLE: UTILIZING IAM IN AWS

```
tasks:
- name: Create a new IAM user with API keys
  iam:
    iam_type: user
    name: kevinjones
    state: present
    password: "{{ temp_pass }}"
    access_key_state: create

- name: Create IAM role with custom trust relationship
  iam:
    iam_type: role
    name: AAALambdaTestRole
    state: present
    trust_policy:
      Version: '2012-10-17'
      Statement:
      - Action: sts:AssumeRole
        Effect: Allow
        Principal:
           Service: lambda.amazonaws.com
```


Source: https://docs.ansible.com/ansible/latest/modules/iam_module.html

EXAMPLE: MANAGE USER ROLES IN OPENSTACK

```
# Grant an admin role on the user admin in the project project1
- os_user_role:
    cloud: hattrick
    user: kevinjones
    role: admin
    project: project1

# Revoke the admin role from the Chris Reynolds in the raleigh domain
- os_user_role:
    cloud: hattrick
    state: absent
    user: creynolds
    role: admin
    domain: raleigh
```


Source: https://docs.ansible.com/ansible/latest/modules/os_user_role_module.html#os-user-role-module

CONNECTIVITY
CONSIDERATIONS FOR EDGE COMPUTING

ANSIBLE RESOURCES FOR NETWORK AUTOMATION

Network Automation with Ansible

https://www.ansible.com/integrations/networks

Modules Maintained by the Ansible Network Team

https://docs.ansible.com/ansible/latest/modules/network_maintained.html

EXAMPLE: SIMPLE NETWORK INTERFACE CHANGES

```
- name: configure interface
  net_interface:
    name: ge-0/0/1
    description: test-interface

- name: remove interface
  net_interface:
    name: ge-0/0/1
    state: absent

- name: make interface up
  net_interface:
    name: ge-0/0/1
    description: test-interface
    enabled: True

- name: make interface down
  net_interface:
    name: ge-0/0/1
    description: test-interface
    enabled: False
```


Source: https://docs.ansible.com/ansible/latest/modules/net_interface_module.html#net-interface-module

LOCAL OR CENTRALIZED ANALYTICS CONSIDERATIONS FOR EDGE COMPUTING

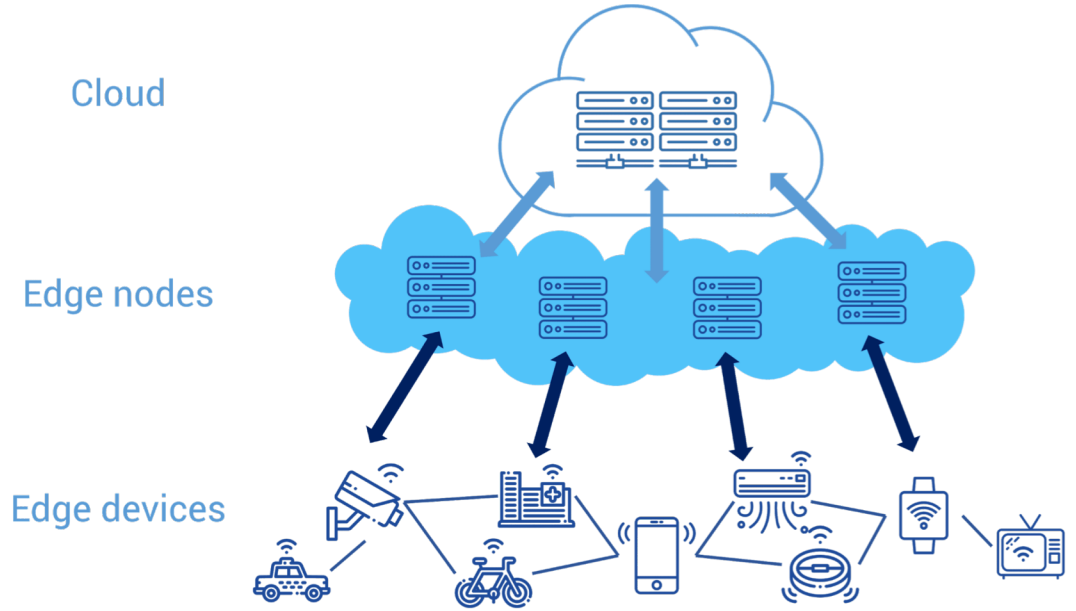
Depends on Use Case and Workload

Local

- Source data is larger
- Decision localized
- Time to decision critical

Centralized

- Derived data is larger
- Aggregate decisions



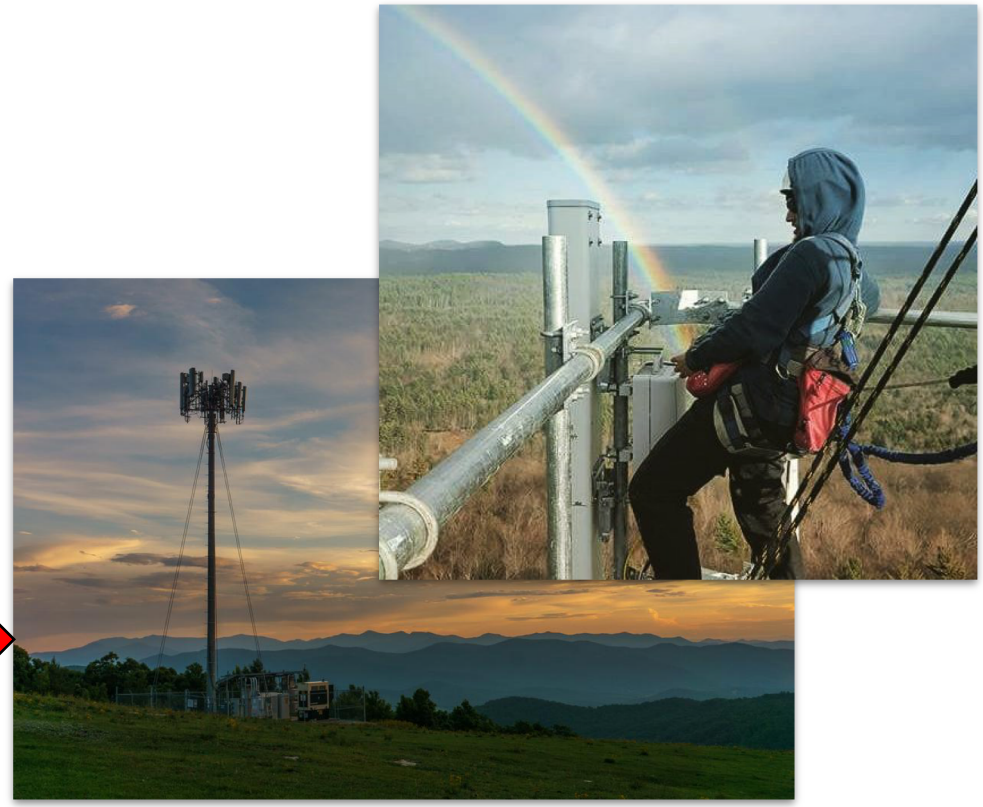
MINIMIZE MAINTENANCE
CONSIDERATIONS FOR EDGE COMPUTING

Operators

- People are expensive
- Not repeatable
- They also die

Hardware

- Compact spaces
- Rugged
- Reduce need to visit



EDGE AT RED HAT

MOBILE PORTFOLIO CENTER

A TRUCK THAT BRINGS RED HAT SUMMIT TO YOU

248 Days

108 Events

44 States

2 Countries

Red Hat's edge weighs 85,000 pounds :)

Red Hat

PROJECT HAT TRICK
DEVELOPMENT PLATFORM

ADMIN Node: 1

- RAM: 2 x 16GB
- M.2 SATA: Intel 540S 1TB
- 2.5" SSD 1: Intel S3520 960GB

COMPUTE Nodes: 4

- Motherboard / CPU: Xeon D1541 - (10GbE)
- RAM: 128GB (4x 32GB)
- M.2 NVMe SSD: Intel P600 480GB
- 4 x 2.5" SSD 1: Intel S3520 480GB
- TPM Module: Yes

NETWORK

- Netgear XS716T: 16 x 10GBaseT

DEMO:
PIMP WORK.
RUN COMMAND.
BE A ROCKSTAR!

HAT TRICK DEPLOY PLAYBOOK

```
---
- name: Configure KVM host
 import_playbook: kvm.yml

- name: Provision, install and configure IDM
 import_playbook: idm.yml

- name: Provision, install and configure Director
 import_playbook: director.yml

- name: Configure and deploy OpenStack overcloud
 import_playbook: overcloud.yml

- name: Provision, install and configure Tower
 import_playbook: tower.yml

- name: Provision, install and configure CloudForms
 import_playbook: cloudforms.yml
```


Source: https://github.com/RedHatGov/hattrick/blob/master/playbooks/hattrick/deploy-full.yml

RESOURCES

Roles - https://galaxy.ansible.com/RedHatGov

Repo - https://github.com/RedHatGov/hattrick

Other

https://www.redhat.com/en/technologies/industries/government
https://www.redhat.com/en/blog/channel/vertical-industries-blog
https://www.redhat.com/en/technologies/industries/telecommunications
https://www.redhat.com/en/mobile-portfolio-center
https://www.openstack.org/edge-computing/

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat