



# Simplifying Security

## Through Red Hat Satellite and Insights

Bill Hirsch  
Principal Solutions Architect



# Who Am I?



 [bhirsch@redhat.com](mailto:bhirsch@redhat.com)

 <https://www.linkedin.com/in/billhirsch/>

 <https://github.com/bhirsch70>

Principal Solutions Architect - RHCA, RHCE

Work in Public Sector helping government & EDU create better strategies for infrastructure management

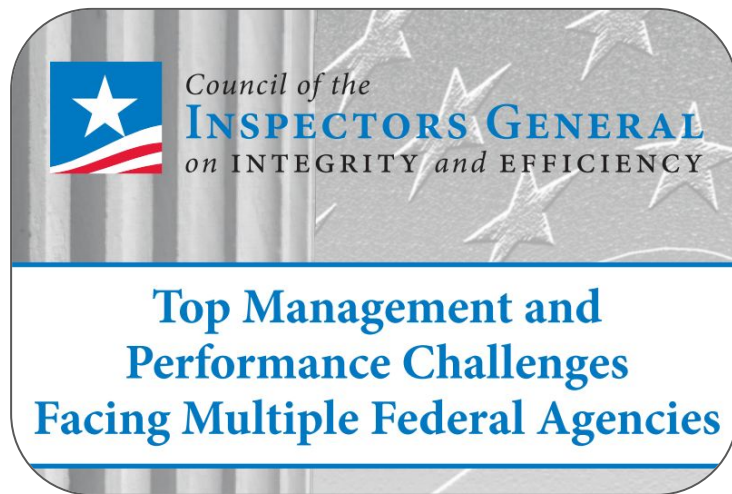
Former Director of Infrastructure at a large healthcare company

Fun Fact: I “accidentally” became an I.T. guy while trying to be a film guy



## Why Simplify Security?

### Top Management and Performance Challenges Oversight.Gov April 2018 Report



**Information Technology Security and Management**  
Safeguarding sensitive assets against cyber-attacks

**Human Capital Management**  
Recruiting, training, and retaining qualified staff

## The Challenge of Complexity

“91% of security professionals express concern over their organizations’ security complexity.”

- Forrester, 2019

# Cost of Data Breaches



2017

## Large Consumer Credit Reporting Agency

**Loss:** Exposed 150 Million people's personal information

**Cause:** Outdated and vulnerable software

**Cost:** **\$1.4 Billion**



2018

## Telecom Mobile Network Provider

**Loss:** Mobile network outage for less than 1 Day

**Cause:** Expired certificates

**Cost:** **\$127 Million**



2019

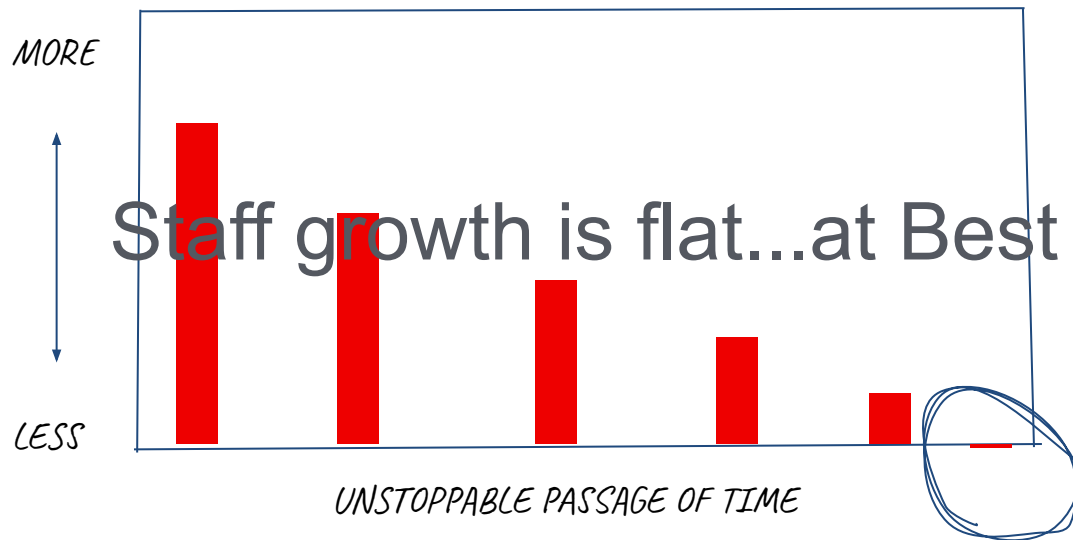
## Large Financial Firm

**Loss:** 106 Million credit card holders personal information

**Cause:** Public cloud misconfiguration

**Cost:** **Between \$200 Million and \$1 Billion**

## Resource Constraints

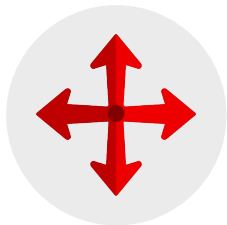




# HOW TO SIMPLIFY



# How do you currently manage your IT environment?



Do your processes scale?

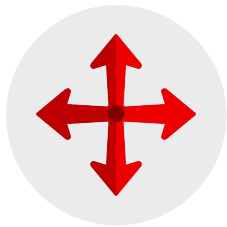


Are you confident you can  
quickly respond?



Are your systems compliant?

## Red Hat Satellite can help



Do your processes scale?



Increase efficiency



Are you confident you can quickly respond?



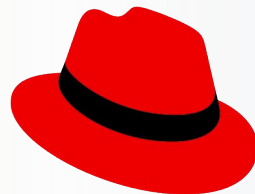
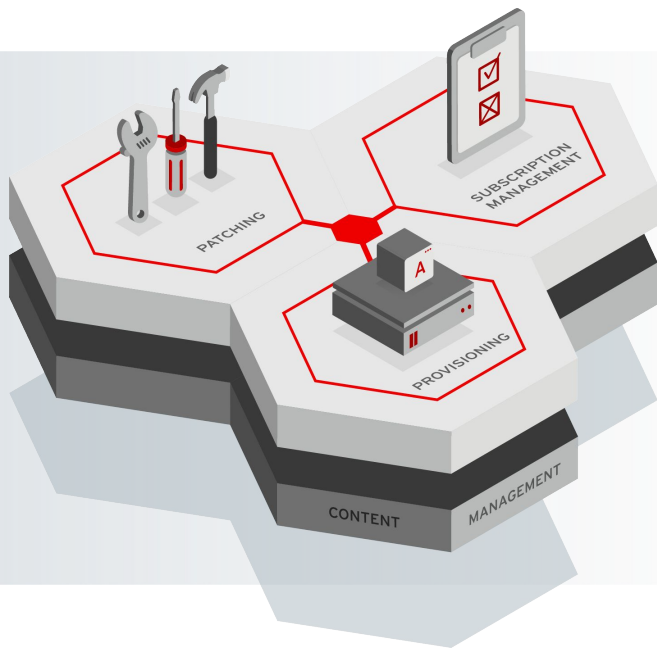
Address security easily



Are your systems compliant?

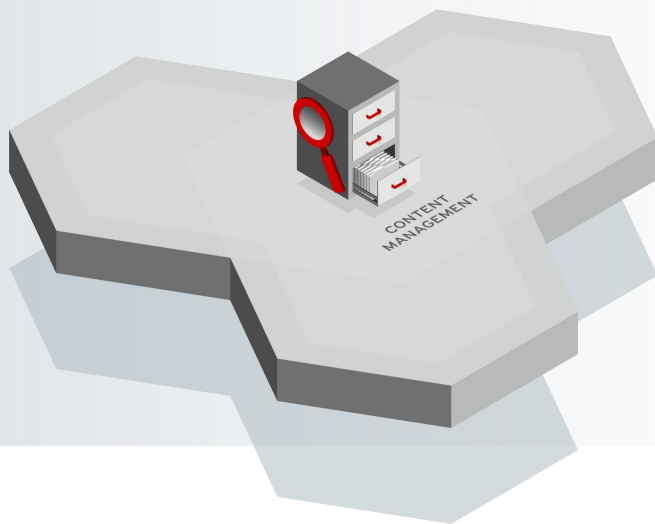


Audit and remediate systems



# Red Hat Satellite

# Content Management



**Content Repository** any type of content made available to any host

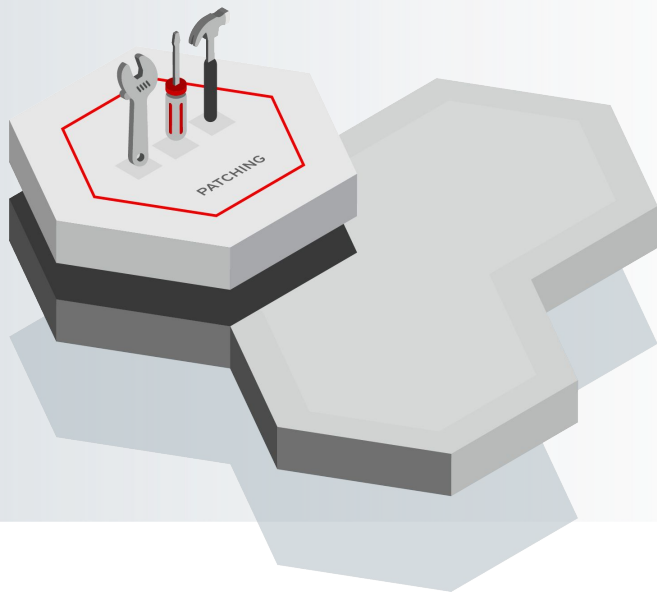


**Curation** of content prior to distribution



**Distribution** of content as close as possible to the end point.

# Patch Management



**Report** on hosts that need updates, fixes, or enhancements

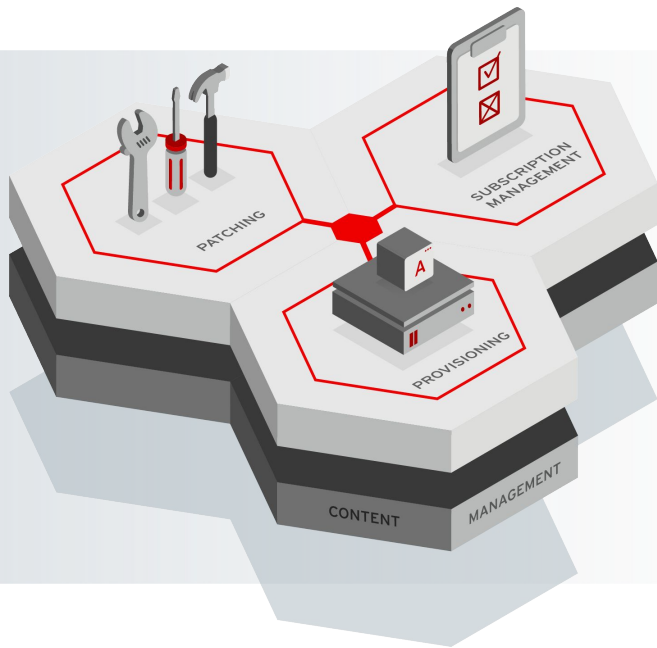


**Group** homogeneous systems so that you can easily work with them



**Respond** quickly to patching requirements using scalable automation

# Additional Satellite Capabilities



**Configuration Management** using Ansible or Puppet

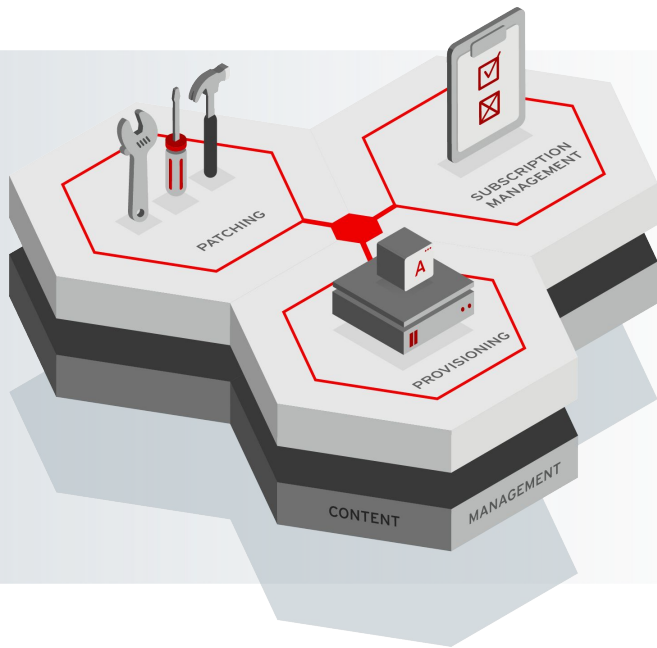


**Automation** through integration with Ansible Tower



**Compliance** using OpenSCAP policies

# Compliance Management with Satellite



## **Compliance** using OpenSCAP policies

- Security Content Automation Protocol
- Managed by National Institute of Standards and Technology (NIST)
- Vulnerability and configuration security baselines
- Helps comply with security standards
  - DISA STIG
  - PCI-DSS
  - Your own custom security standards
- Red Hat natively ships NIST validated National Checklist content



**PREDICT RISK. GET GUIDANCE. STAY SECURE.**

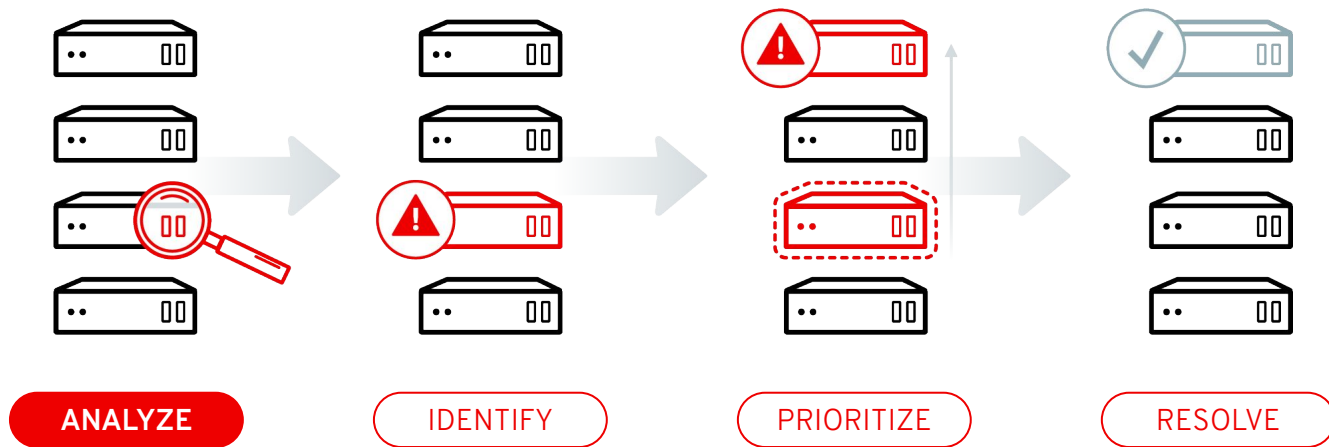
**PREDICTIVE I.T. ANALYTICS**

**AUTOMATED EXPERT ASSESSMENT**

**SIMPLE REMEDIATION**



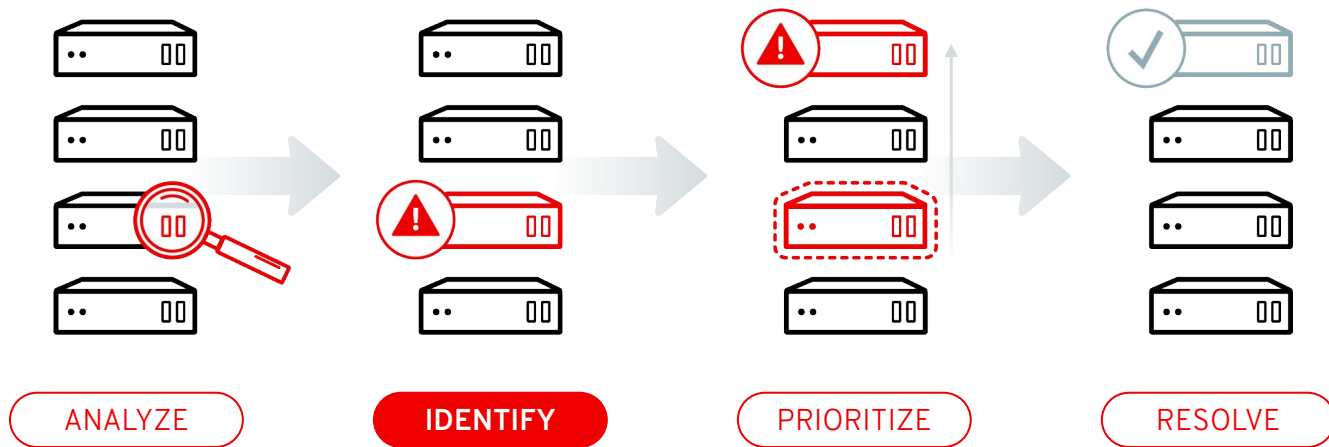
# Managing infrastructure risk



“99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident.”

- Gartner, 2017

# Managing infrastructure risk

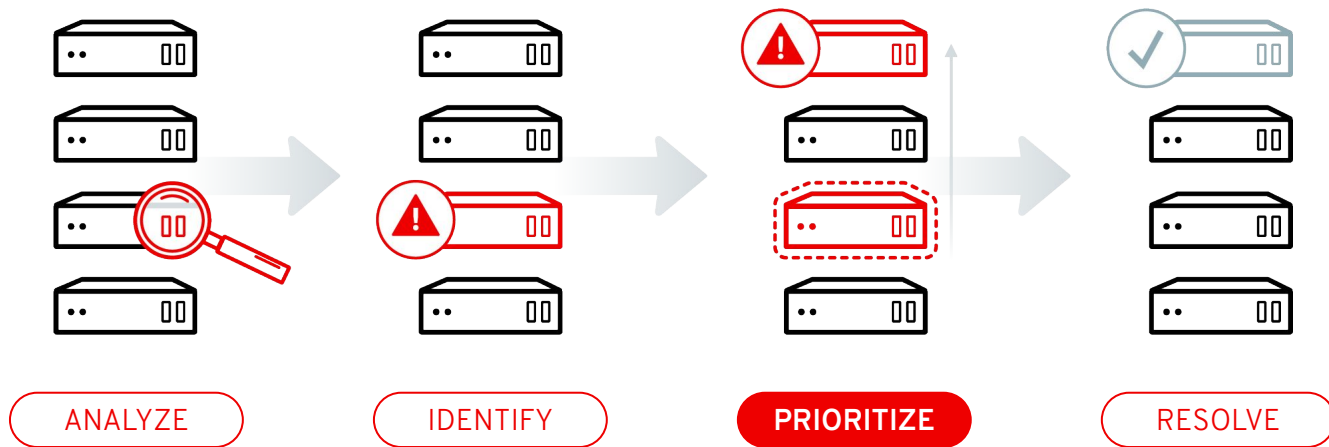


## Remediate the Right Vulnerabilities

“While CVSS scores are an important aspect of understanding the risk a vulnerability poses to your organization, understanding the likelihood of its exploitability should also be given due consideration.”

- Skybox Security

# Managing infrastructure risk



# Get ahead of key security risks

Don't wait for your security team to tap you on the shoulder

➤ Security > NetworkManager DHCP vulnerable to remote code execution (CVE-2018-1111)

Impact Likelihood Total Risk Risk of change: Very Low

➤ Stability > New Ansible Engine packages are inaccessible when dedicated Ansible repo is not enabled

Impact Likelihood Total Risk Risk of change: Very Low

➤ ⚠Stability > Kdump crashkernel reservation failed due to improper configuration of crashkernel parameter

Impact Likelihood Total Risk Risk of change: Moderate

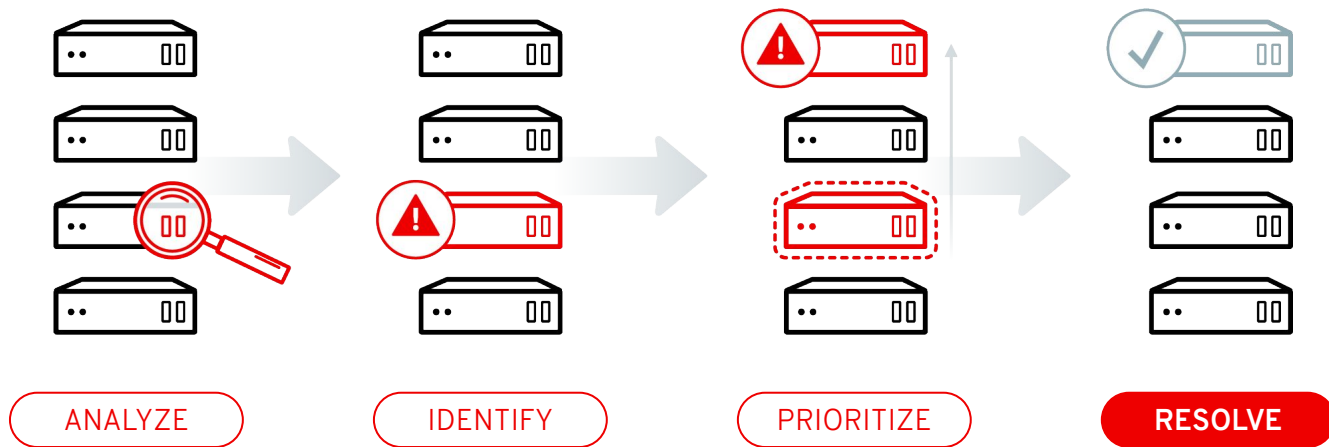
- Prioritizes security response by analyzing runtime configuration and usage

- Automates security analysis, beyond just CVEs

*“...when a vulnerability is released, it's likely to be exploited within 40-60 days. However, it takes security teams between 100-120 days on average to remediate...”*

— KENNA SECURITY GROUP

# Managing infrastructure risk



# Automatic remediation with Satellite 6.6

Resolve issues with a click of a button

The screenshot displays the 'Insights maintenance plan for host' page in the Satellite 6.6 web interface. The page is divided into several sections: 'Overview' (selected) and 'Hosts'. Under 'Overview', it shows 'Target hosts' with a manual selection using a static query 'plan\_id=35963'. It indicates the plan was evaluated at 2018-05-18 20:57:54 -0400 and that there are 2 total hosts. A large green circular progress indicator on the right shows '100% Success' and 'succeeded'. Below this, the 'Providers and templates' section shows the 'Ansible - Run insights maintenance plan through Ansible' template. The bottom part of the screen displays the Ansible playbook code, which includes tasks for determining the insights version, obtaining the insights report, and registering the insights result.

Job invocations > Insights maintenance plan for host

Refresh | Rerun | Rerun failed | Job Task | Cancel job | Abort job

Overview | Hosts

Target hosts

Manual selection using Static Query

plan\_id=35963

Evaluated at: 2018-05-18 20:57:54 -0400

Total hosts

2

Providers and templates

Ansible - Run insights maintenance plan through Ansible

Preview for target tomcatclient.example.com

```
---
- name: run insights to obtain latest report info
  hosts: all
  become: true
  tasks:
    - name: determine insights version
      shell: redhat-access-insights --version
      changed_when: false
      register: insights_version
    - when: insights_version.stdout[0:2] != "1."
      block:
        - name: obtaining insights report
          shell: redhat-access-insights --to-json --quiet
          register: insights_result
          changed_when: false
          check_mode: false
        - name: register insights report as fact for use by other plays
          set_fact: insights_report={{ insights_result.stdout }}
    - when: insights_version.stdout[0:2] != "1."
      block:
        - name: obtaining insights report (legacy client)
```

**Apply remediation plans**  
with a click of a button—and  
track activity and progress  
on your machines.



# Customer Stories

- Insights was able to immediately identify 10 issues on an Oracle RAC system that has been **plaguing a customer for 6 months**.
  - Oracle RAC systems are EXPENSIVE. Why not keep them running at **optimal** capacity?
- One customer swore their 2,000 servers were up-to-date.
  - A demonstration of Red Hat Insights showed them that **400 of their servers were not up-to-date**, and therefore at **risk**.

# 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](https://linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://facebook.com/redhatinc)

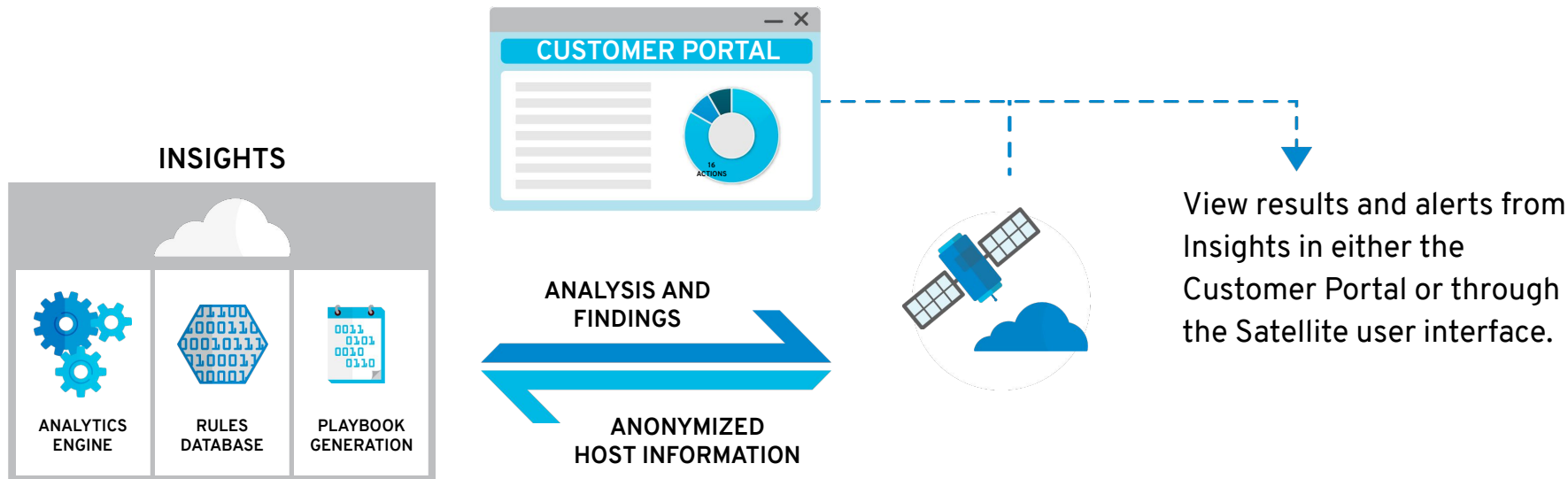


[twitter.com/RedHat](https://twitter.com/RedHat)



**Red Hat**

# How Insights Works



# Red Hat Insights

Now included with all Red Hat Enterprise Linux subscriptions

Buy



**Red Hat**  
Enterprise Linux

Get



**Red Hat**  
Insights