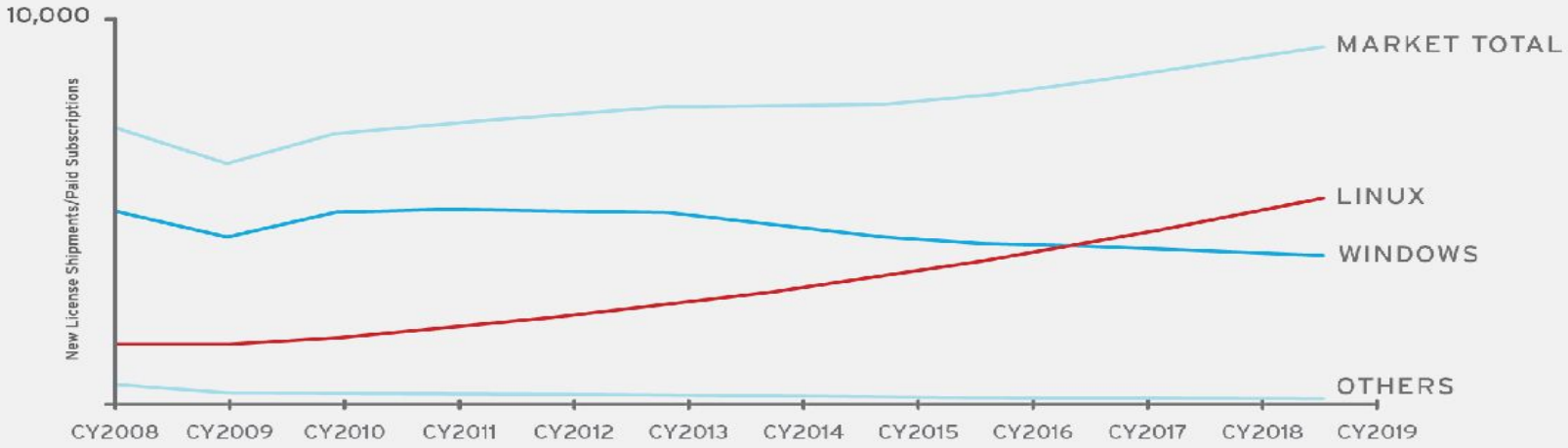
Secure Foundations: Why RHEL isn't just another Linux distribution

Lucy Kerner
Principal Technical Product Marketing Manager - Security, Red Hat
May 3, 2017

ONLY TWO OPERATING SYSTEMS MATTER

WORLDWIDE SERVER OPERATING ENVIRONMENT NEW LICENSE SHIPMENTS AND PAID SUBSCRIPTIONS 2008-2019 (000)



IDC Analyze the Future

Source: Worldwide Client and Server Operating Environments Forecast, 2015-2019, IDC #US40371515, December 2015

Why does the OS matter?

“Vulnerabilities, patch management, and their exploitation are still the root cause of most breaches.”

- Gartner, September 2016
[http://www.gartner.com/doc/3438517/time-align-vulnerability-management-priorities]

There are lots of OS's out there....

TRADITIONAL | LIGHTWEIGHT | ABSTRACTION

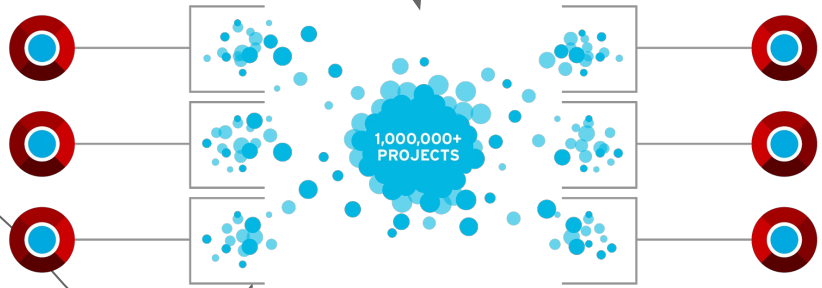
15 Years of Making Open Source Enterprise-Ready

PARTICIPATE

We participate in and create community-powered upstream projects.

INTEGRATE

We integrate upstream projects, fostering open community platforms.



STABILIZE

We commercialize these platforms together with a rich ecosystem of services and certifications.

‘02 — Red Hat Enterprise Linux is Born

‘03 — Cluster File Systems

‘05 — IBM Power, IBM Z Series

‘07 — Virtualization

‘10 — Secure Virtualization, Control Groups, Automated Security Audits

‘11 — Software Defined Storage

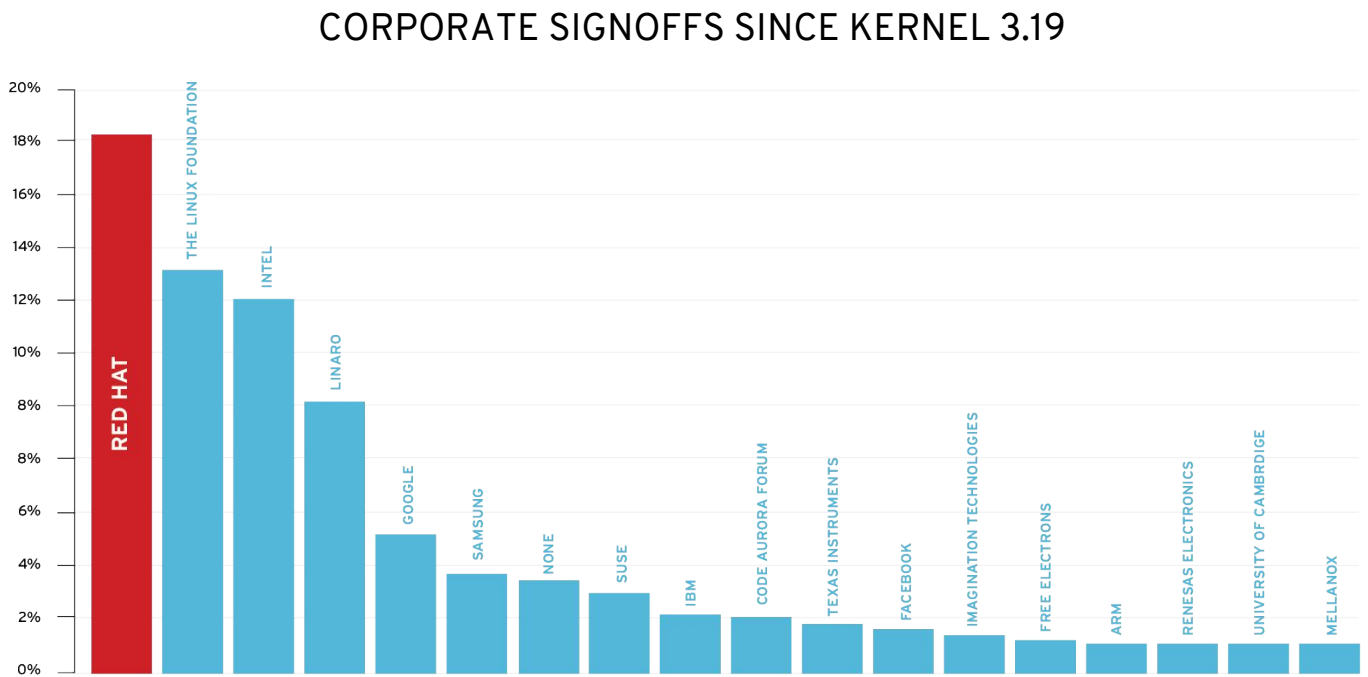
‘12 — Real-Time Kernel

‘13 — Containers, Software Defined Networking

‘15

‘17

Top Corporate Maintainer of the Linux Kernel



Source: Linux Kernel Development (The Linux Foundation, August 2016)

What security do I get with Red Hat Enterprise Linux?

Security Technologies in Red Hat Enterprise Linux

VALUE OF A RED HAT SUBSCRIPTION

CUSTOMER PORTAL

GLOBAL TECHNICAL SUPPORT

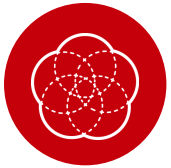
AUTOMATED SERVICES

PRODUCT SECURITY

EXPERTISE

CERTIFICATIONS

COMMUNITIES



CONTINUOUS FEEDBACK

ASSURANCES

LIFE-CYCLE PROMISE

Red Hat Customer Portal Labs

Developed by Red Hat engineers to help you improve performance, troubleshoot issues, identify security problems, and optimize configuration.

FEATURED APPS

KICKSTART GENERATOR

Create optimal Kickstart configurations for Red Hat Enterprise Linux 5, 6, or 7 that are tailored to meet specific deployment goals.

Go to App ▸ More info ▸

PRODUCT LIFE CYCLE CHECKER

Query the life cycle of Red Hat products, and better plan your deployment or maintenance.

Go to App ▸ More info ▸

AD INTEGRATION HELPER (SAMBA FS - WINBIND)

This tool helps you connect a Red Hat Enterprise Linux system to an Active Directory server by generating Samba Winbind configuration. Basic information of Active Directory server is needed and a script will be generated. The script will config Samba, NSS and PAM for you.

Go to App ▸ More info ▸

ALL LABS

Showing 16 of 57 Labs

All Labs | Configuration | Deployment | Security | Troubleshoot

All products (57)

Filter apps by name or descripti

SSLV3 (POODLE) DETECTOR

The SSLv3 Detector allows customers to scan vulnerable systems for CVE-2014-3566 (POODLE).

SHELLSHOCK - BASH VULNERABILITY DETECTOR

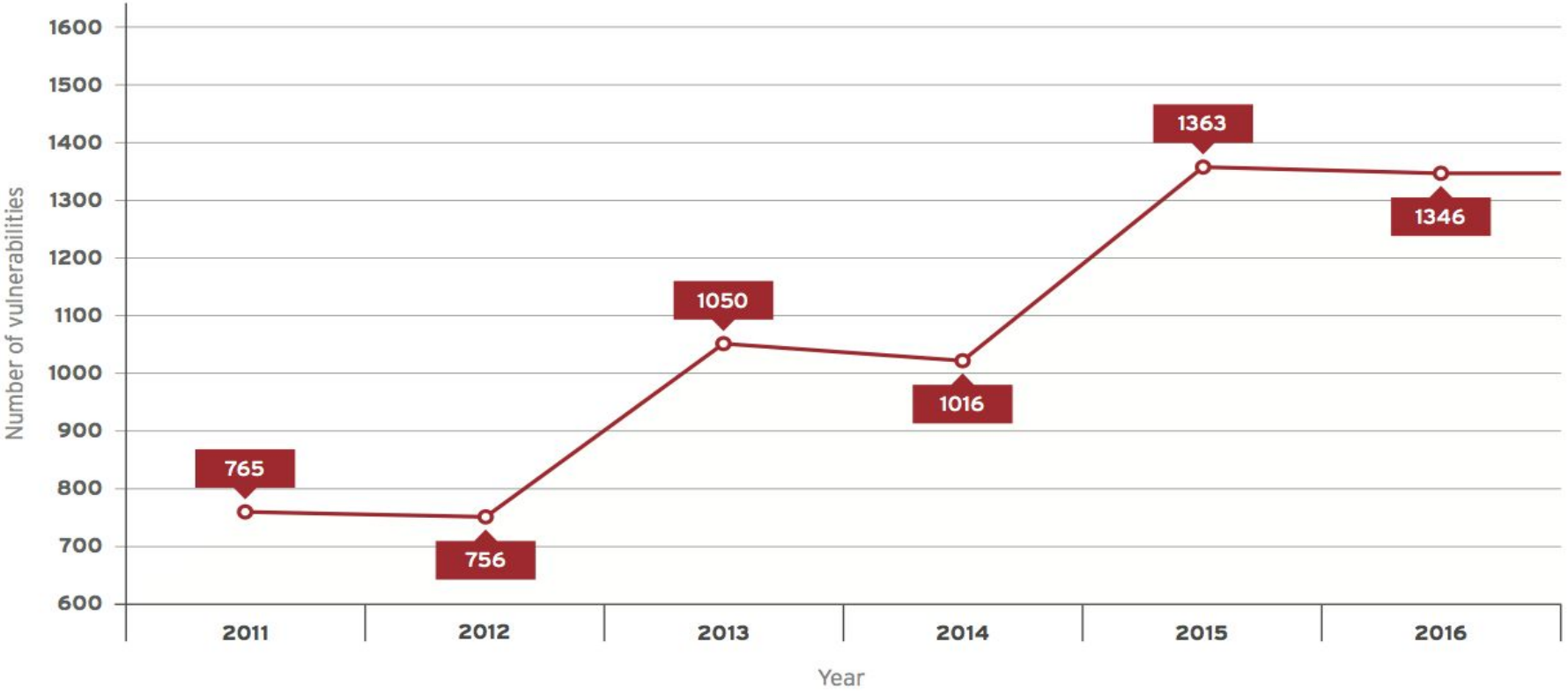
This application helps you test whether your system is vulnerable to Bash code injection.

IAVM MAPPER

Look at the IAVM reports that are related to Red Hat products.

Red Hat security timeline

Vulnerabilities increase as we deliver more products and versions.



WE DON'T BELIEVE THE HYPE.

A vulnerability may get a name, a logo, or press attention, but that doesn't mean it poses greater risk. Red Hat tells you **which branded vulnerabilities matter and which do not.**

BRANDED
HIGH RISK

httpoxy

Dirty Cow

ImageTragick
CVE-2016-3714

BRANDED
LOW RISK

DROWN

SWEET32

Badlock

mAlert
OpenSSL DoS

Red Hat security advisories and vulnerabilities for 2016

PRODUCT	CRITICAL ADVISORIES	IMPORTANT ADVISORIES	CRITICAL VULNERABILITIES	IMPORTANT VULNERABILITIES
All products	110	270	318	255
Red Hat Enterprise Linux 5,6,7	38	90	50	89
› Red Hat Enterprise Linux 6 (all)	30	43	50	66
› Red Hat Enterprise Linux 6 Server (Default)	7	17	9	22
› Red Hat Enterprise Linux Supplementary (5,6,7)	41	29	270	122
Red Hat JBoss® Middleware (all JBoss products)	21	34	2	15
Red Hat Storage (all storage products)	1	0	1	1
Red Hat OpenStack® Platform	0	31	0	9

37% of all Critical advisories were for Red Hat Enterprise Linux supplementary channels (Java, Flash, and others)

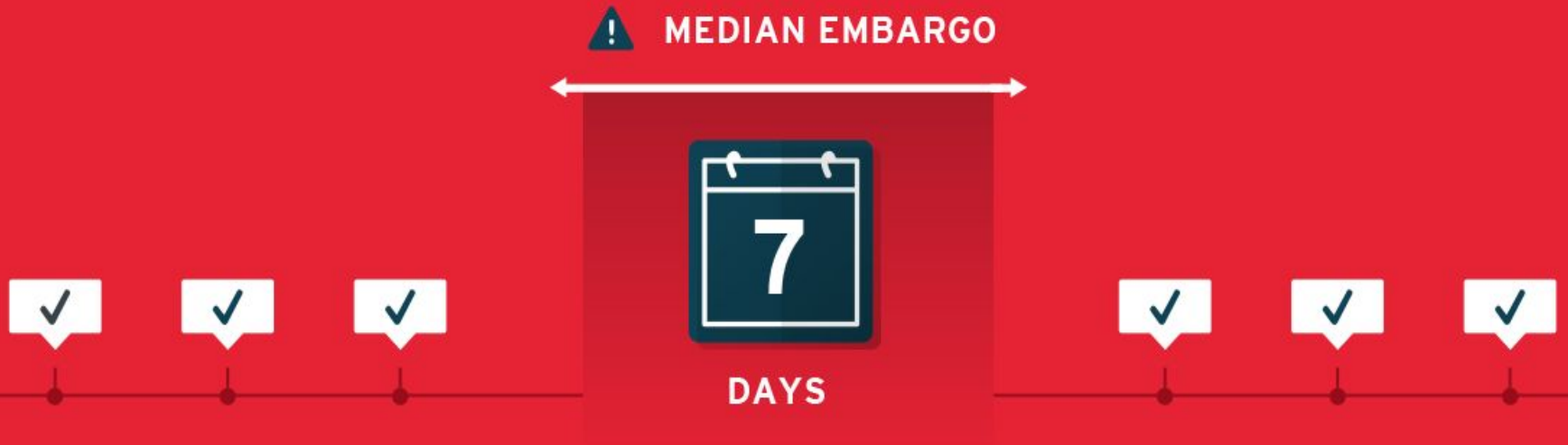
100% of Red Hat Enterprise Linux Critical issues had updates the same or next day after public knowledge

WE FIX THE ISSUES THAT MATTER–FAST

100% of Red Hat Enterprise Linux critical issues had updates **the same or next day after public knowledge.**

WE REDUCE RISK WITH TRANSPARENCY

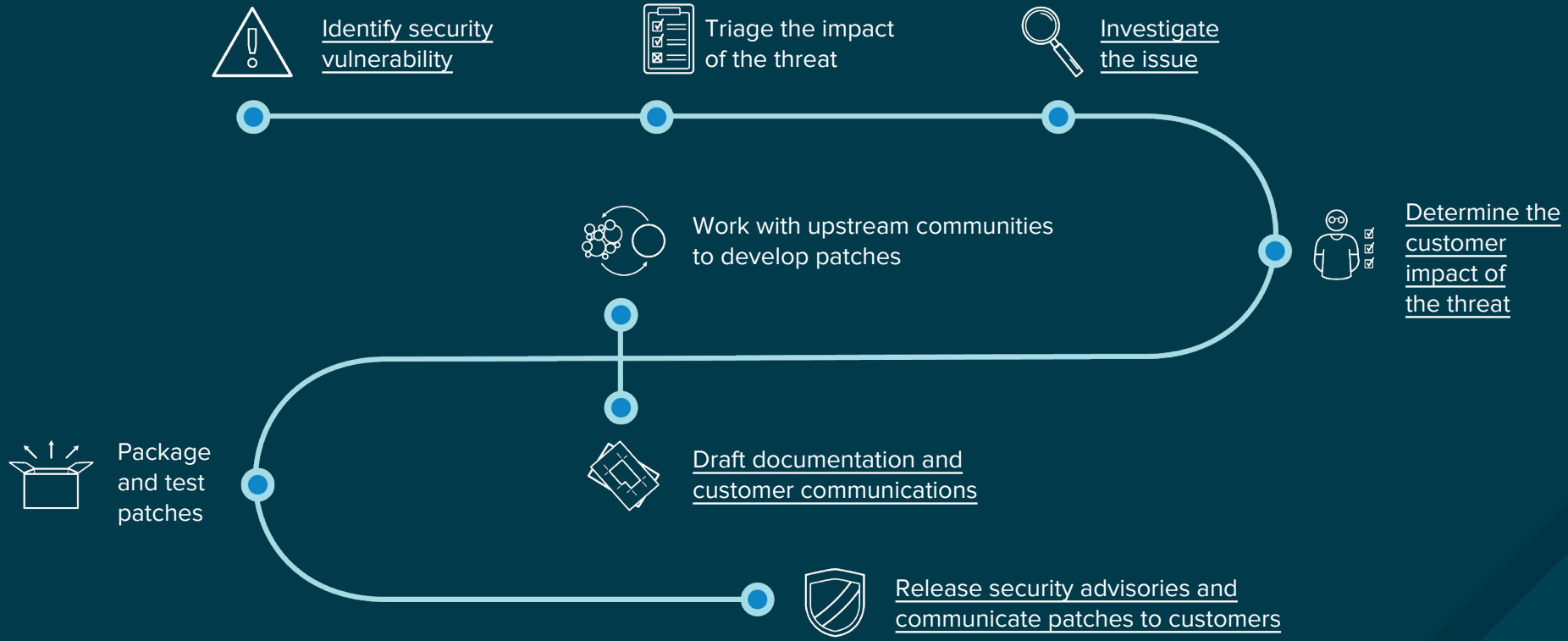
Keeping issues private increases their value to attackers. In 2016, the median time issues were private before being made public was just **seven days, a six-day decrease from 2015**.



WE SEEK OUT VULNERABILITIES

Red Hat employees find 11% of the issues we fix.

CUSTOMER SECURITY AWARENESS WORKFLOW



From Community to Red Hat Enterprise Linux

RED HAT SUPPLY CHAIN SECURITY

- Community leadership
- Package selection
- Manual inspection
- Automated inspection
- Packaging guidelines
- Trusted builds

- Quality assurance
- Certifications
- Signing
- Distribution
- Support
- Security updates/patches

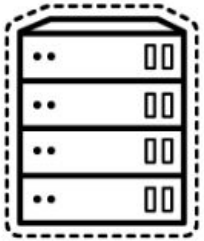
Build Roots: Repeatability for binaries

- We don't just build on some developer's workstation
- Everything that's built is translated into a "buildroot"
- We can say exactly what was on the system when the rpm was built
  - Versions of RPMSs
  - Versions of libraries
  - Versions of compilers
  - Compiler flags (optimization, function fortification, etc)
  -
- If needed, we could rebuild an RPM down to the same checksum

Where does the OS matter?

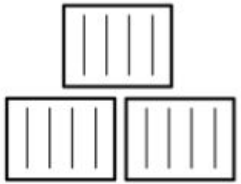
THE OS MATTERS

Where does the OS matter?



TRADITIONAL INFRASTRUCTURE

Datacenters - physical and virtual



CONTAINERS

Host OS, base Image, runtime

NEXT GEN INFRASTRUCTURE

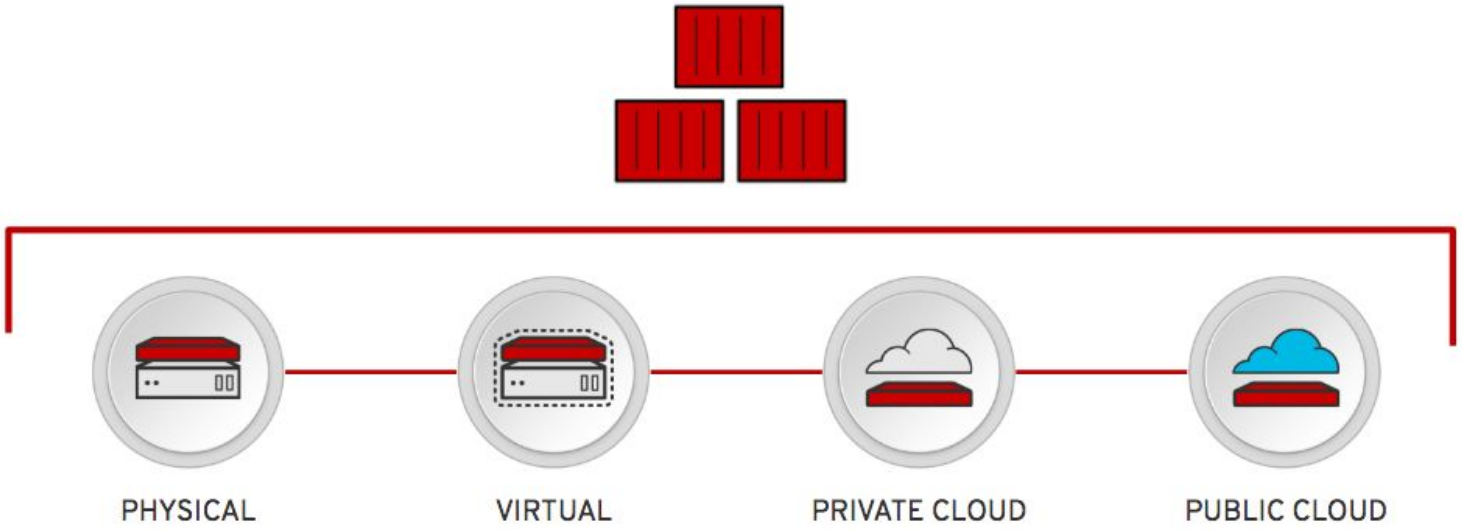
IaaS, PaaS, IoT and more

PUBLIC CLOUD

Portability across public clouds

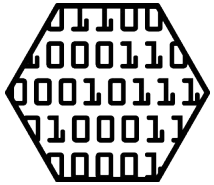
CONSISTENCY VIA THE HOST OS

DRIVES PORTABILITY ACROSS PHYSICAL, VIRTUAL, AND CLOUD ENVIRONMENTS

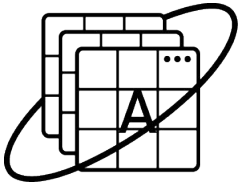


RED HAT ENTERPRISE LINUX -- AT THE HOST AND CONTAINER LAYERS

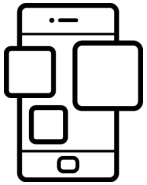
A Standard Foundation for Next Gen Infrastructure



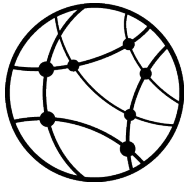
Big Data



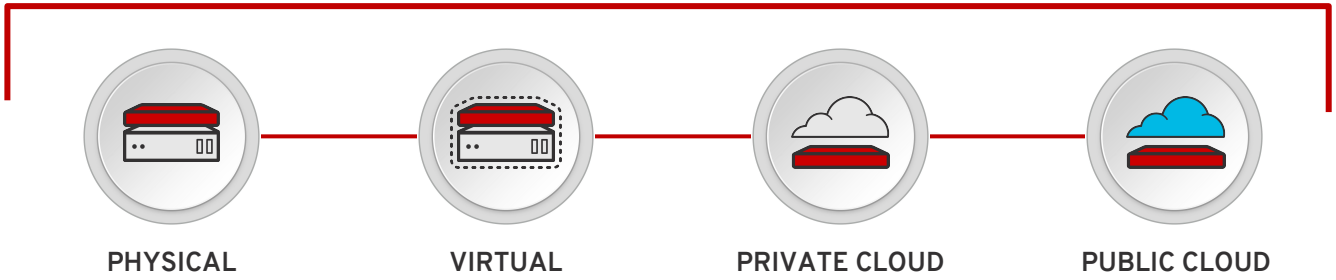
Modern apps



Mobile



IoT



PHYSICAL

VIRTUAL

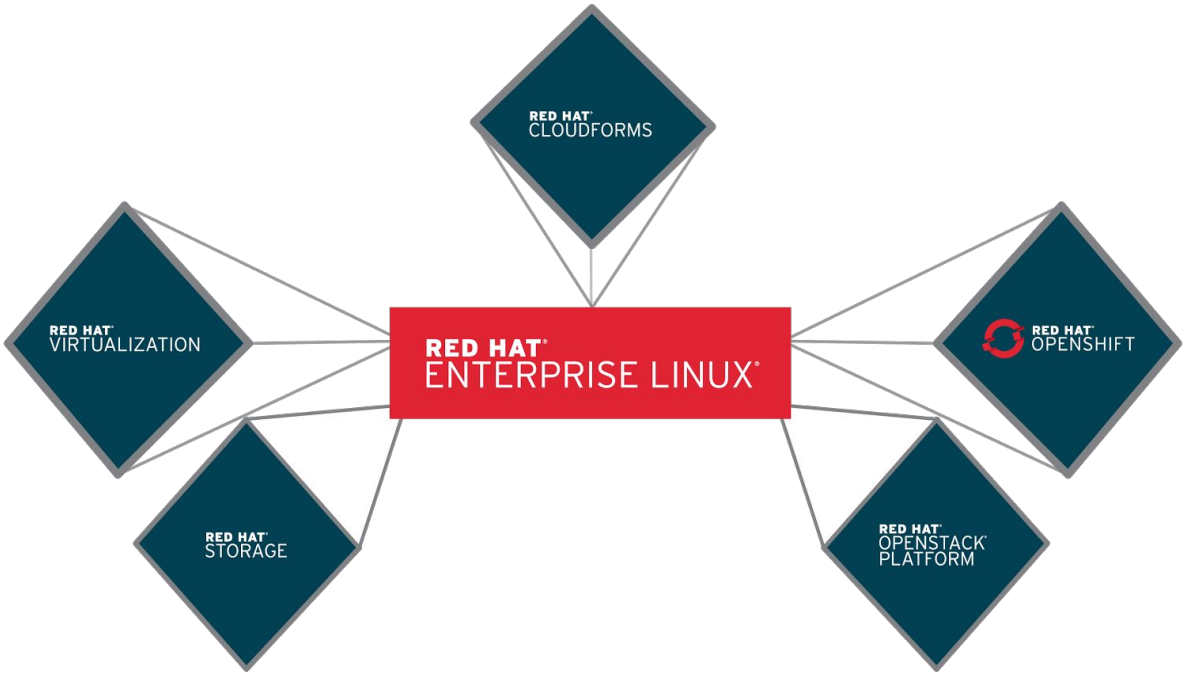
PRIVATE CLOUD

PUBLIC CLOUD

RED HAT ENTERPRISE LINUX

RED HAT ENTERPRISE LINUX

THE FOUNDATION FOR ALL RED HAT PLATFORMS



Want to have a deeper discussion?

- Come visit us at the Red Hat Enterprise Linux Ask the Experts area at the Partner Pavilion !
- The Security Pod at the Partner Pavilion will also feature demos on Secure Foundation as well
- And come talk to our Product Security experts at the Partner Pavilion as well
- And of course , come check out the Red Hat Enterprise Linux breakout sessions and labs we have here for you at Summit!

Secure Foundations: Infrastructure Risk Management

Will Nix
Principal Technical Product Marketing Manager
Red Hat Management

COMPLEXITY IS RISK

80%

Percentage of commercial application outages caused by software failure and operational complexity

Carnegie Mellon

$336k/hr

The median cost per hour of downtime for a production application for a large enterprise

Gartner®

$15m/yr

Mean annualized cost of cybercrime deference and remediation for large US-based corporations

Ponemon INSTITUTE

65% CompTIA®

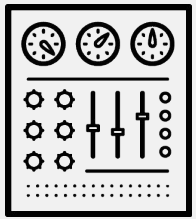
Customers thought they were significantly behind in training and capabilities needed to manage their next generation infrastructure.

RED HAT® INSIGHTS

ANALYZING INFRASTRUCTURE RISK

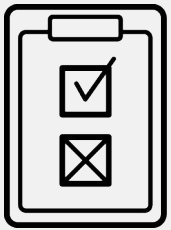
RESPONSE

Are you confident that you can quickly respond when vulnerabilities strike?



TOOLS

Are you comfortable that your tooling and processes will scale as your environment scales?



COMPLIANCE

Are you certain that systems are compliant with various internal infosec and package security requirements?

ANALYZING INFRASTRUCTURE RISK

WE CANNOT

JUST THROW PEOPLE AT THE PROBLEM,

WE NEED

TECHNOLOGY

RED HAT® INSIGHTS

INFRASTRUCTURE RISK MANAGEMENT

DO MORE

WITH LESS

ANSIBLE by Red Hat®

AUTOMATE YOUR IT PROCESSES & DEPLOYMENTS

- Simple & powerful language
- No agents to install
- Scale with ANSIBLE TOWER by Red Hat®

RED HAT® INSIGHTS

PREVENT CRITICAL ISSUES BEFORE THEY OCCUR

- Continuous Insights
- Verified Knowledge
- Proactive Resolution

RED HAT® SATELLITE

BUILD A TRUSTED & SECURE RED HAT ENVIRONMENT

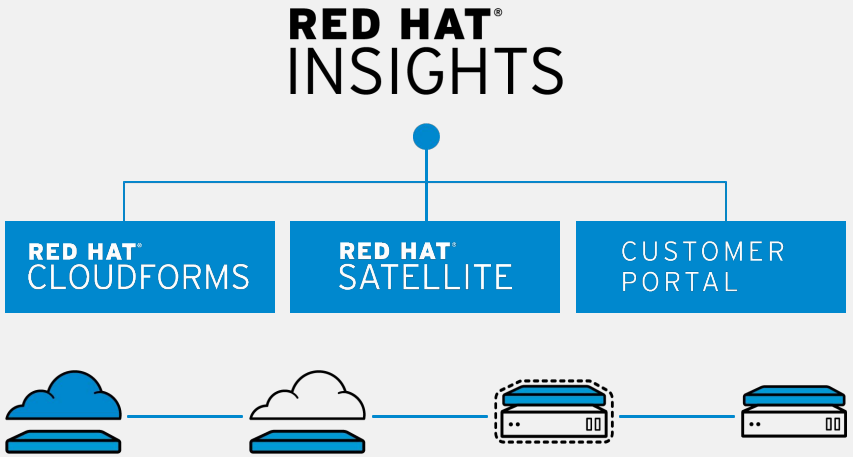
- Manage the Red Hat Lifecycle
- Provision & Configure at Scale
- Standardize Your Environment

RED HAT® CLOUDFORMS

DELIVER SERVICES ACROSS YOUR HYBRID CLOUD

- Hybrid Cloud Management
- Self-Service Provisioning
- Policy-driven Compliance

INTEGRATED INTO TOOLS YOU USE



- Works on physical, virtual, cloud, and container-based workloads
- No new infrastructure to manage
- Integrated into Satellite 5.7, 6.1+, CloudForms 4.0+, and Red Hat Customer Portal
- API available for custom integration
- Ansible Tower integration enables playbooks generated in Red Hat Insights to be automatically imported into Ansible Tower

RED HAT® INSIGHTS

RISK MANAGEMENT WITH INSIGHTS

ACTIONABLE INTELLIGENCE POWERED BY RED HAT

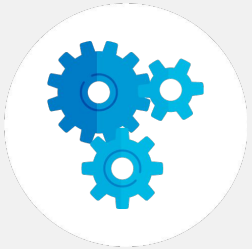
Confidently scale complex environments with no added infrastructure cost.

CONTINUOUS VULNERABILITY ALERTS

Maximize uptime and avoid fire-fighting so businesses can focus on strategic initiatives.

INCREASED VISIBILITY TO SECURITY RISKS

Get ahead of security risks and fix them before businesses are impacted.

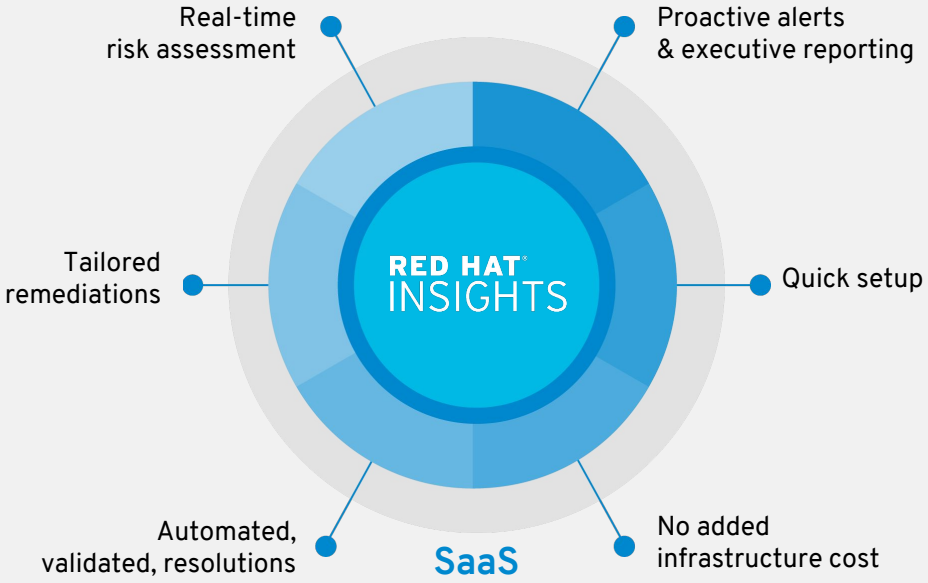


AUTOMATED REMEDIATION

Minimize human error, do more with less, and fix things faster.

RISK MANAGEMENT WITH INSIGHTS

RED HAT® INSIGHTS



" As a global leader in healthcare information technology, security, and infrastructure intelligence are main priorities for us. Red Hat Insights enables us to be alerted to potential vulnerabilities across thousands of active systems and provide swift remediation."

The technology helps us prioritize risk resolution in our infrastructure.

– TIM ERDEL
Senior director,
Cerner Works Technology Improvement Center

RED HAT INSIGHTS CAPABILITIES

RED HAT® INSIGHTS

REMEDIATION MADE SIMPLE

- Automatically tailored recommendations and remediation down to the per-host level
- Create and share maintenance plans to better coordinate responses within your team

“ 22% of disasters are caused by human error.”

– QUORUM DISASTER RECOVERY REPORT

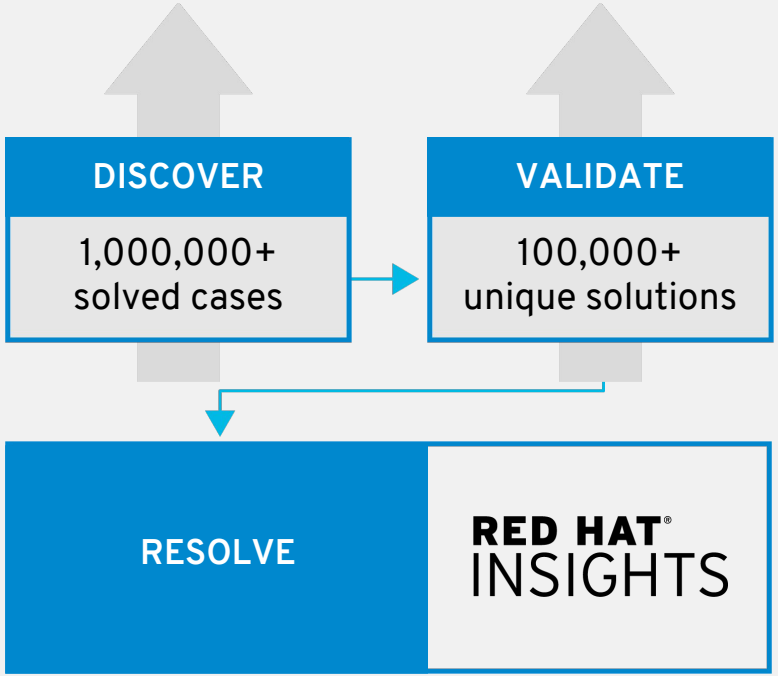
AUTOMATE RISK MANAGEMENT

- Monitor RHEL 6.4 and higher, OSP 7 and higher, RHV 4 and higher, with OCP support coming soon
- Generate Ansible playbooks for use with Ansible core or Ansible Tower

- Available in RHEL base channels via yum or deploy quickly with Satellite or playbook
- Integrates with Satellite, CloudForms, Customer Portal, and Ansible Tower

RED HAT® INSIGHTS

PROACTIVE & CONTINUOUS ASSESSMENT



- Continuous identification of new risks driven by unique industry data
- Based on real-world results from millions of enterprise deployments

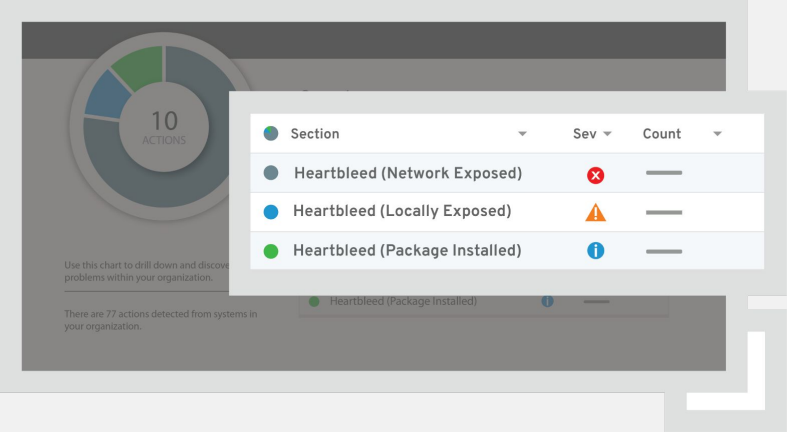
“ 85% of critical issues raised to Red Hat® support are already known to Red Hat or our partners.”

— RED HAT GLOBAL SUPPORT SERVICES

RED HAT® INSIGHTS

GET AHEAD OF KEY SECURITY RISKS

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



- Prioritizes security response by analyzing runtime configuration and usage
- Automates security analysis for customers, beyond just CVEs

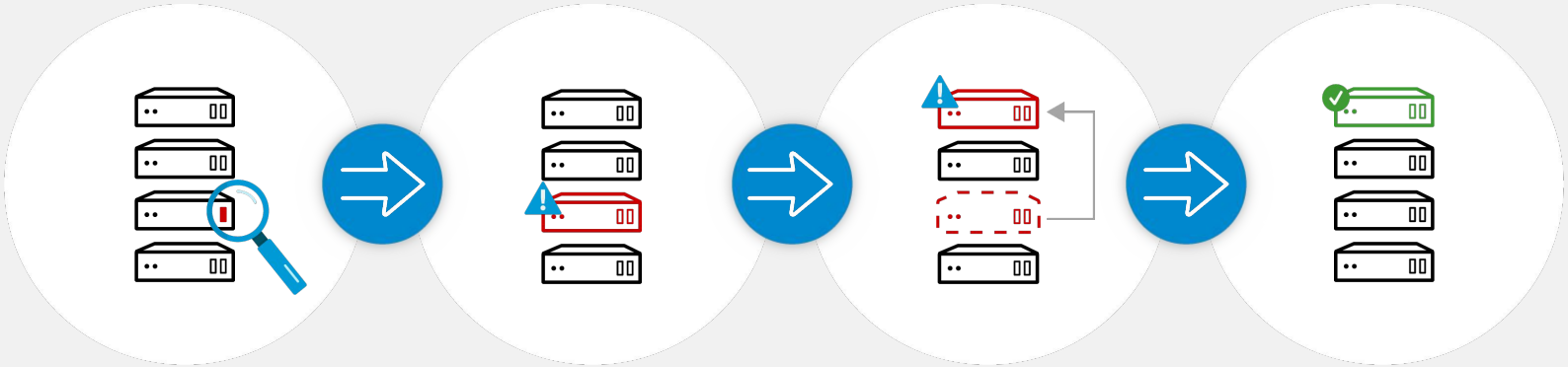
“ In the first year when a vulnerability is released, it’s likely to be exploited within 40-60 days. However, it takes security teams between 100-120 days on average to remediate existing vulnerabilities.”

— KENNA SECURITY GROUP


HOW INSIGHTS WORKS

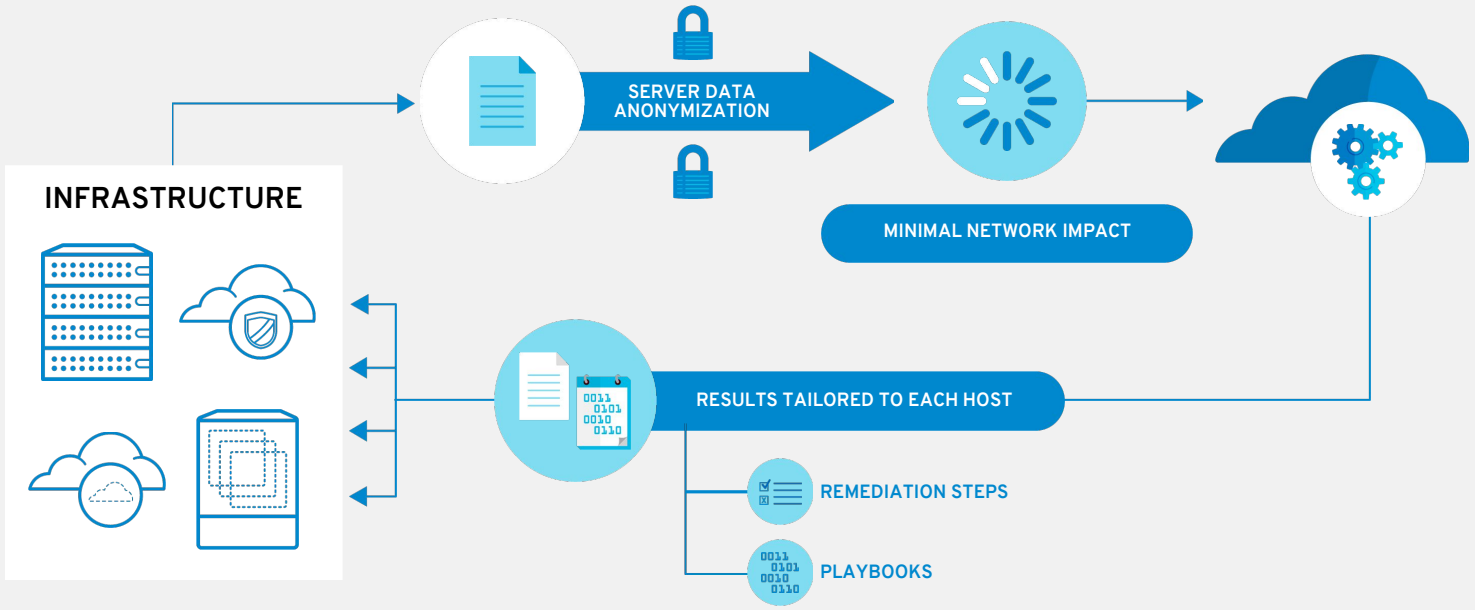
MANAGING INFRASTRUCTURE RISK

Automated remediation



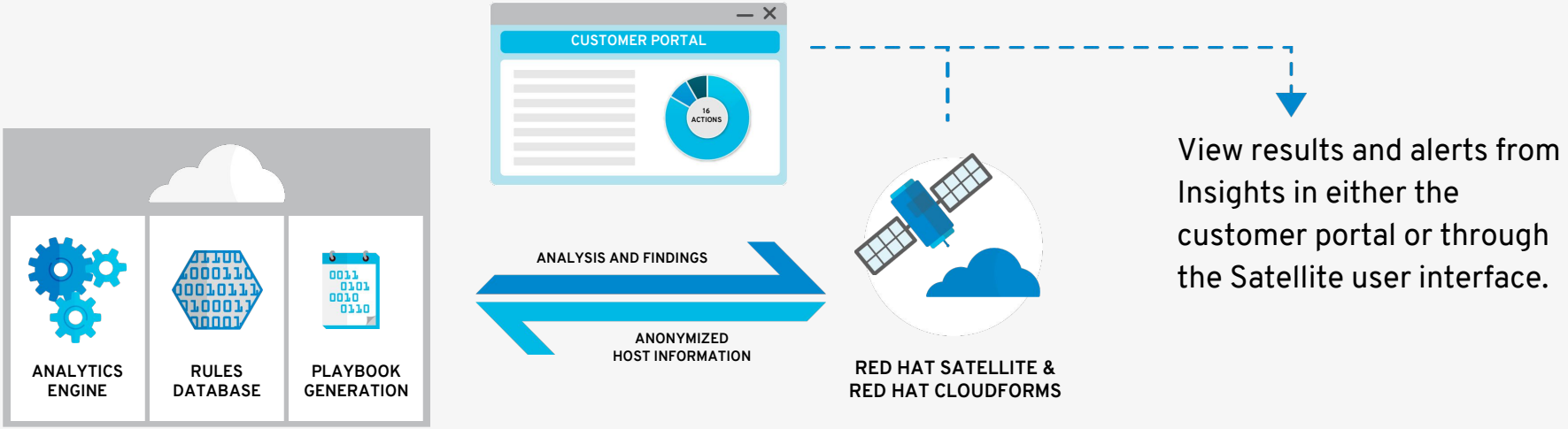
ANALYZE | IDENTIFY | PRIORITIZE | RESOLVE

ARCHITECTURE



ARCHITECTURE

RED HAT® INSIGHTS



RED HAT® INSIGHTS

AUTOMATED KEY RISK REPORTING

Tailored resolution steps included for resolution

Performance issue:
Network interface is not performing at maximum speed

→

Recommended action:
Check cable, connections, and remote switch settings.

Security risk detected:
Privilege escalation

→

Recommended action:
Apply mitigation and update the Kernel.

Availability/stability:
Unexpected behavior with syntax in bonding config

→

Recommended action:
Change uppercase to lowercase in the config file.

RED HAT® INSIGHTS

START RISK MANAGEMENT TODAY

Start using Insights with your RHEL subscription.

ALREADY A RED HAT® ENTERPRISE LINUX® CUSTOMER?

Try Insights at no cost:

https://access.redhat.com/insights/getting-started

INTERESTED IN A MANAGEMENT SUITE?

Insights is included in:

Red Hat Cloud Infrastructure + Red Hat Cloud Suite

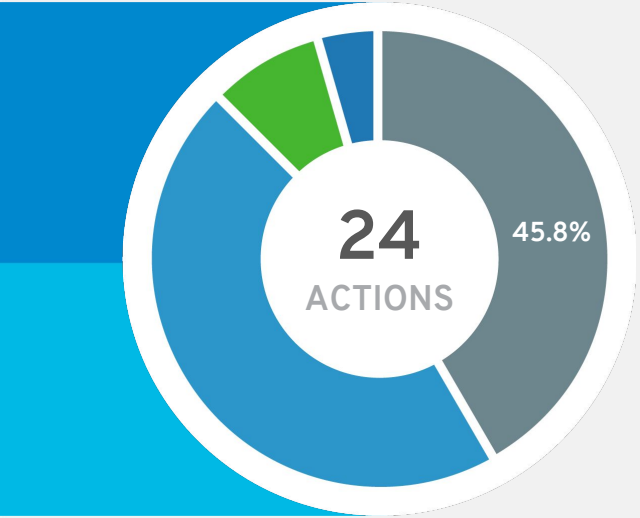
WOULD YOU LIKE TO LEARN MORE ABOUT INSIGHTS?

https://www.redhat.com/en/technologies/management/insights

For more info, visit: https://access.redhat.com/insights/info

RED HAT® INSIGHTS

START RISK MANAGEMENT TODAY



Run an Insights assessment for 30 days:

1. Work with your account team to get an Insights eval subscription.
2. Install the Red Hat Insights RPM.
3. Register 50+ systems for best view.
4. See results immediately.
5. Schedule a best practices workshop.

See valuable insights in minutes:

1. Activate eval: https://access.redhat.com/insights/evaluation.
2. Installation: https://access.redhat.com/insights/getting-started.

QUESTIONS?

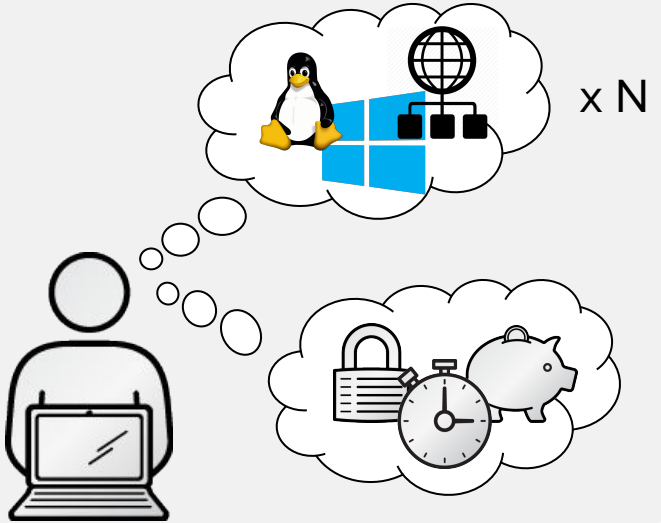
insights@redhat.com

MAKING DAY-TO-DAY OPERATIONS MORE PROACTIVE, LESS REACTIVE

Phil Griffiths
Senior Solutions Architect
May 2017

WHY?

MORE THINGS THAN EVER AFFECTING YOU



SUPPORT

OPERATIONS

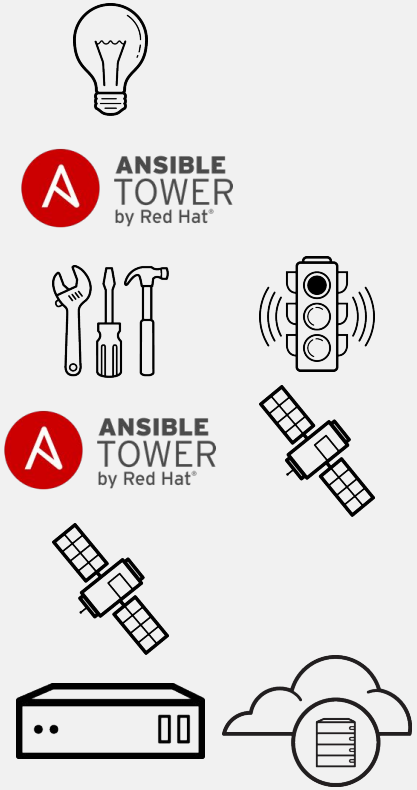
SECURITY

SUPPORT

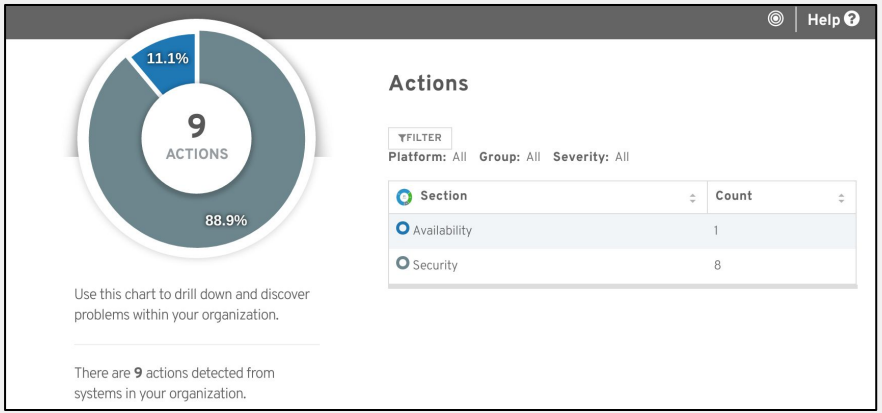
Break-fix scenarios
No centralised audit/logging?
More support tickets than people
False positives disguise problems

BUILD THE CAKE

- Predictive Analytics
- Application install and configuration
- Automated Testing (CI/CD)
- OS customisation
- Minimal OS
- Infrastructure - physical/virtual/cloud



ADD SPRINKLES...

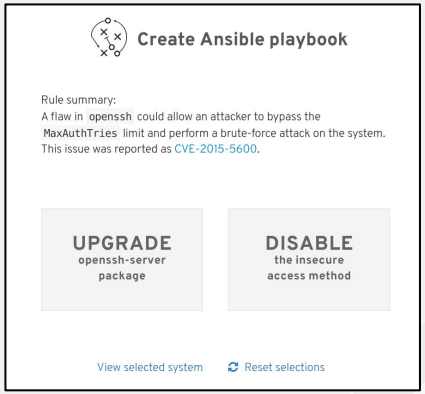


DISCOVER
1,000,000
solved cases

VALIDATE
100,000
unique solutions

RESOLVE

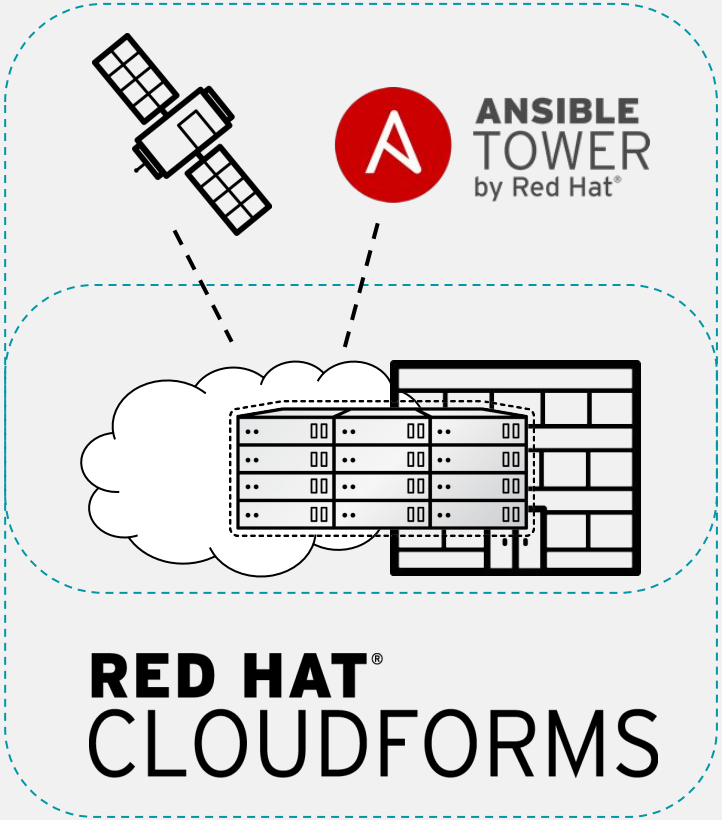
RED HAT INSIGHTS



OPERATIONS

Manual or semi-manual
Mostly homebrew scripts
Everyone has *their* favourites
Configuration management (drift)

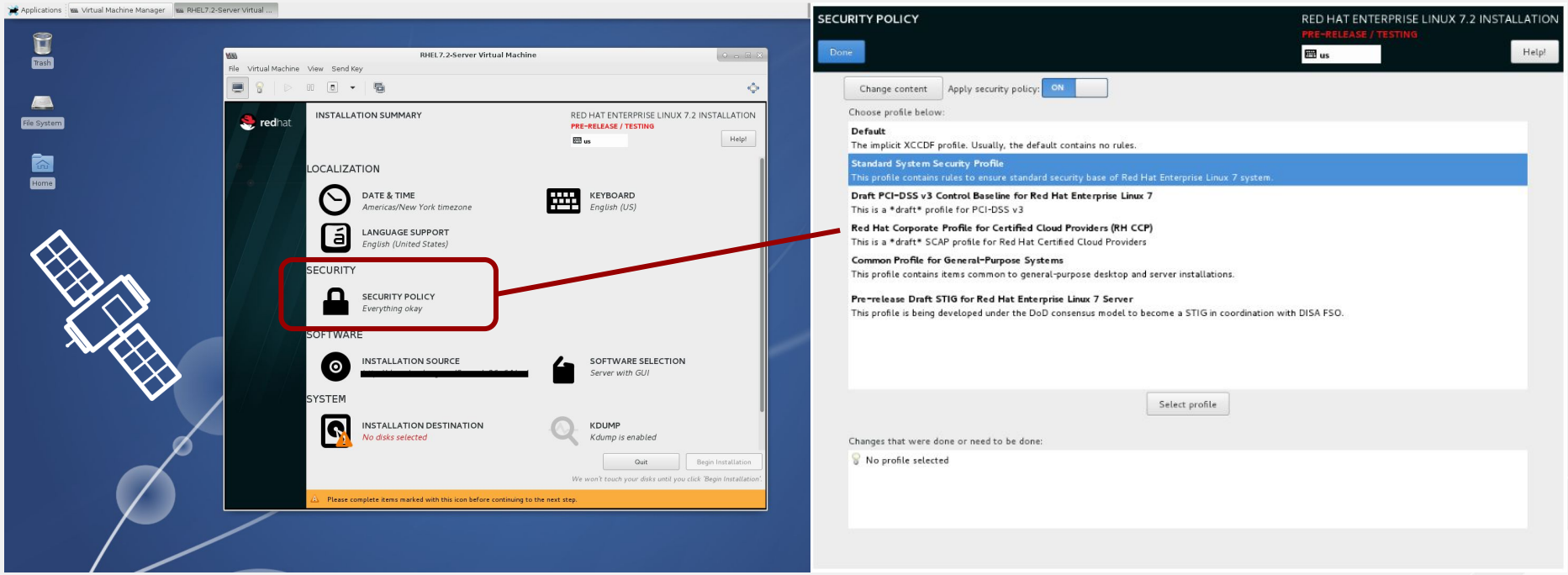
AUTOMATION IS THE KEY



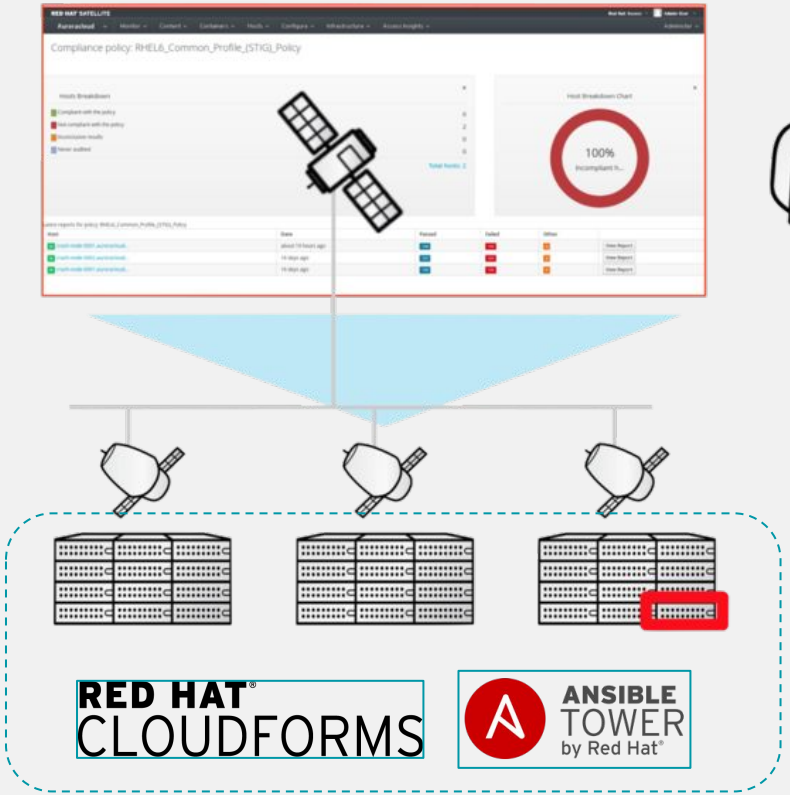
SECURITY

Port scanning
One way traffic - security team
Can’t see wood for the trees
Only fix critical **red** issues

APPLY POLICY AT DAY-1 *BUILD* TIME...



… THEN DAY-2 OPS COMPLIANCE



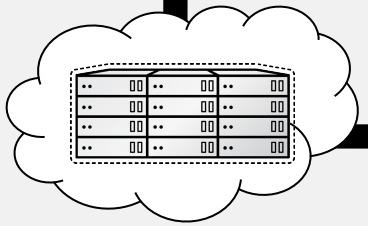
JOIN THE DOTS.

BUSINESS PROCESS AUTOMATION, MEET SYSTEMS AUTOMATION

RED HAT® JBOSS®
BPM SUITE

ANSIBLE
TOWER
by Red Hat®

Full post provision
lifecycle management:
control, audit, utilisation, planning,
chargeback and more



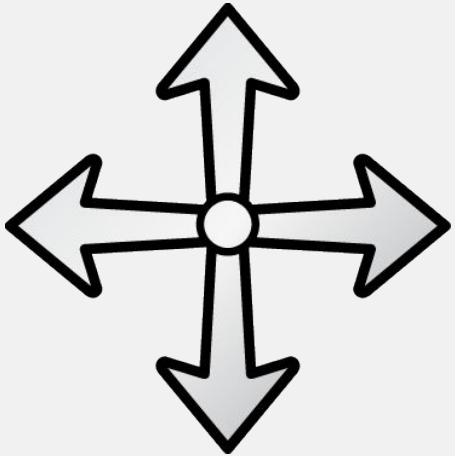
RED HAT®
CLOUDFORMS

Proactive analysis of your systems with regularly updated information

RED HAT® INSIGHTS

RED HAT® JBOSS® BPM SUITE

End-to-end policy and rules driven business automation



RED HAT® CLOUDFORMS

The most powerful, simple yet effective systems automation tool on the market

ANSIBLE TOWER by Red Hat®

Full systems lifecycle management