

Some Assembly Required: Enterprise Patching

More Than Just Yum Update

Josh Swanson
Platform Specialist Solution Architect
joshswanson@redhat.com

Scott Danielson
Senior Solution Architect
sdaniels@redhat.com

Josh Swanson

joshswanson@redhat.com





Agenda:

- What: What is patching?
- Why: Why do we patch?
- How: How do we patch?
 - Technical tools in the toolbox
 - Patching architecture
 - Patching procedure

What is Patching?

Patching is the act of applying new code to RHEL.

Security

Focused on fixing or closing security issues

Bug Fix

One or more bug fixes and might contain enhancements

Enhancement

Contain one or more enhancements or new features

What is Patching?

Mapping our categories to errata types

Security

Focused on fixing or closing security issues



**Red Hat Security
Advisory (RHSA)**

Bug Fix

One or more bug fixes
and might contain
enhancements



**Red Hat Bug Advisory
(RHBA)**

Enhancement

Contain one or more
enhancements or new
features



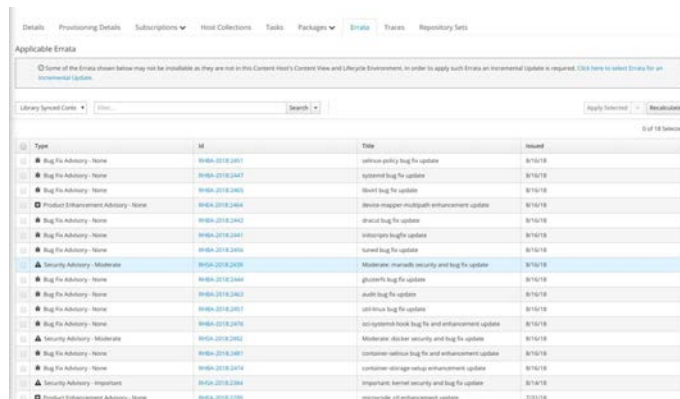
**Red Hat Enhancement
Advisory (RHEA)**

What is Patching?

We (Red Hat) refer to patches as “errata”.


The word errata comes from Latin and is the plural form of the word erratum. Historically, the word erratum referred to a correction of a published text, typically because of an error in the publishing process. Red Hat Errata refers to the correction or update of a software package based on a security issue, bug, or the availability of a new feature. The advisory (errata advisory) is the published text; the errata is the packaged release.

Note: Red Hat uses the terms errata, advisory, and even errata advisory interchangeably.



The screenshot shows the Red Hat Errata website interface. At the top, there are tabs for Details, Provisioning Details, Subscriptions, Host Collections, Tools, Packages, Errata (selected), Trainers, and Repository Sets. Below the tabs, there's a section titled 'Applicable Errata' with a note about incremental updates. A search bar and filters are present. The main content is a table of errata with columns for Type, ID, Title, and Issued. The table lists various errata, including security advisories and product enhancement advisories, with the 'Moderate: chronicle security and bug fix update' highlighted.

Type	ID	Title	Issued
Bug Fix Advisory - None	RH-BA-2018.2801	cdtman patching bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2807	systemd bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2805	libevent bug fix update	8/16/18
Product Enhancement Advisory - None	RH-BA-2018.2804	devops-mapper-multipath enhancement update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2802	chronicle bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2801	chronicle bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2800	chronicle bug fix update	8/16/18
Security Advisory - Moderate	RH-SA-2018.2806	Moderate: chronicle security and bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2803	glusterfs bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2802	glusterfs bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2801	glusterfs bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2800	glusterfs bug fix update	8/16/18
Security Advisory - Moderate	RH-SA-2018.2802	Moderate: chronicle security and bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2801	chronicle bug fix update	8/16/18
Bug Fix Advisory - None	RH-BA-2018.2800	chronicle bug fix update	8/16/18
Security Advisory - Important	RH-SA-2018.2804	Important: chronicle security and bug fix update	8/16/18
Product Enhancement Advisory - None	RH-BA-2018.2803	chronicle enhancement update	8/16/18



Why should you
patch?

Why Should We Patch?

To keep systems secure

[Vulnerability](#) > [CVEs](#) > CVE-2019-12749

CVE-2019-12749

Business risk Status

Not defined Not reviewed

A flaw was found in dbus. The implementation of DBUS_COOKIE_SHA1 is susceptible to a symbolic link attack. A malicious client with write access to its own home directory could manipulate a ~/.dbus-keyrings symlink to cause the DBusServer to read and write in unintended locations resulting in an authentication bypass. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Publish date: 10 June 2019

[View in Red Hat CVE database](#) 

Actions ▾



Important severity

[Learn more](#)

7.0

CVSS 3.0 base score

CVSS 3.0 vector 

CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Why Should We Patch?

To keep RHEL operating reliably

[Patch](#) > [Advisories](#) > RHBA-2020:5489

RHBA-2020:5489

Red Hat Insights is a service that provides analysis of registered RedHat-based systems. The insights-client package can gather the required data(such as installed packages, running services, or software configurations)to proactively identify threats to security, performance, and stabilityacross your environment.

Bug Fix(es) and Enhancement(s):

* Update insights-client to version 3.1.1 (BZ#1899590)

Issued: 15 Dec 2020

Modified: 15 Dec 2020

 [View packages and errata at access.redhat.com](#)

Why Should We Patch?

To keep RHEL operating reliably

Links				
System	ID	Priority	Status	Summary
Red Hat Product Errata	RHBA-2020:5489	None	None	None
Link Dupont 2020-11-19 15:58:40 UTC				
<p>insights-client includes a number of bug fixes and improvements.</p> <ul style="list-style-type: none">* GNU installation directories are now included in `constants.py`, so application code can dynamically look up where its installation prefix is (#123)* Fixed a bug where a systemd timer would cause a system to hang for 120 seconds at boot up. (#124)* Removed shebangs from Python files not mean to be executed by a shell. (#125)* Fixed a bug in the motd logic that prevented the motd message from being removed when a system was registered with insights (#126)* Collects collection runtime metrics and reports them back to cloud.redhat.com (#121, #127)* Various documentation updates (#128)* Fixed a bug where invoking `insights-client` through the deprecated `redhat-access-insights` command breaks JSON parsing of output. (#133)				
errata-xmllrpc 2020-12-15 17:04:22 UTC				
<p>Since the problem described in this bug report should be resolved in a recent advisory, it has been closed with a resolution of ERRATA.</p> <p>For information on the advisory (insights-client bug fix and enhancement update), and where to find the updated files, follow the link below.</p> <p>If the solution does not work for you, open a new bug report.</p> <p>https://access.redhat.com/errata/RHBA-2020:5489</p>				

Why Should We Patch?

To add new features and functionality

[Patch](#) > [Advisories](#) > RHEA-2020:0283

RHEA-2020:0283

Red Hat OpenStack Platform provides the facilities for building, deploying and monitoring a private or public infrastructure-as-a-service (IaaS) cloud running on commonly available physical hardware.

For additional information about the items in this advisory, see the Technical Notes: https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/16.0/html/release_notes/chap-technical_notes.

Issued: 06 Feb 2020

Modified: 06 Feb 2020

 [View packages and errata at access.redhat.com](https://access.redhat.com)



How do we patch?



Technical Tools in the Toolbelt

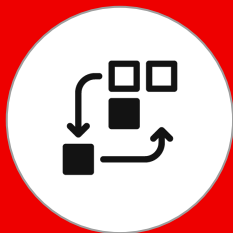
**Smart Management enables you to
improve the reliability, availability,
security and compliance of your RHEL
systems, running on any platform, while
reducing TCO and repetitive tasks**

Smart Management for Red Hat Enterprise Linux

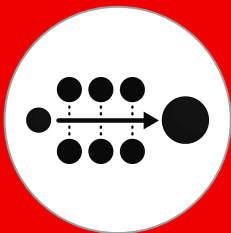
Combine the powerful infrastructure capabilities of Red Hat Satellite with the simplicity of cloud management

Improve operational efficiency

Overcome scale, skill, and security gaps



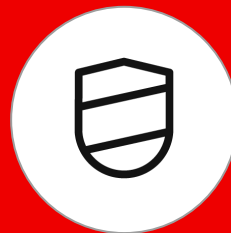
Patch



Provision



Report



Control



Identify & Remediate

What's included with Smart Management?

As of April 2020, Smart Management includes:

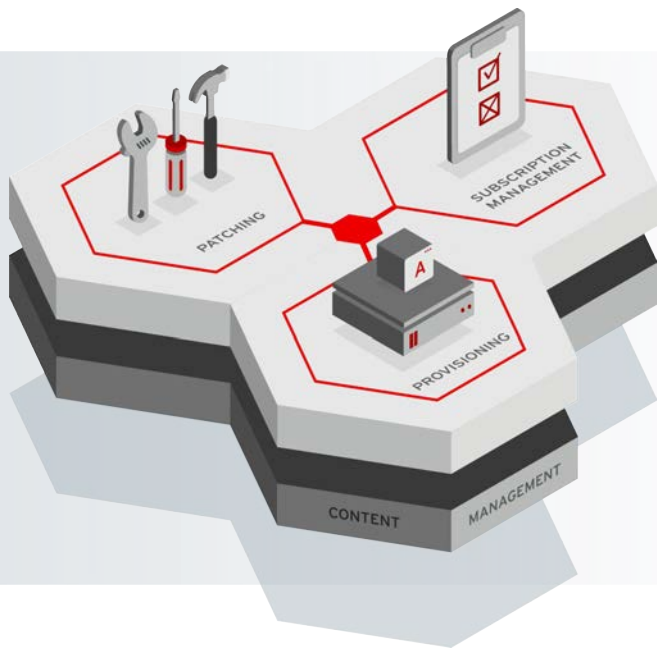


Red Hat Satellite



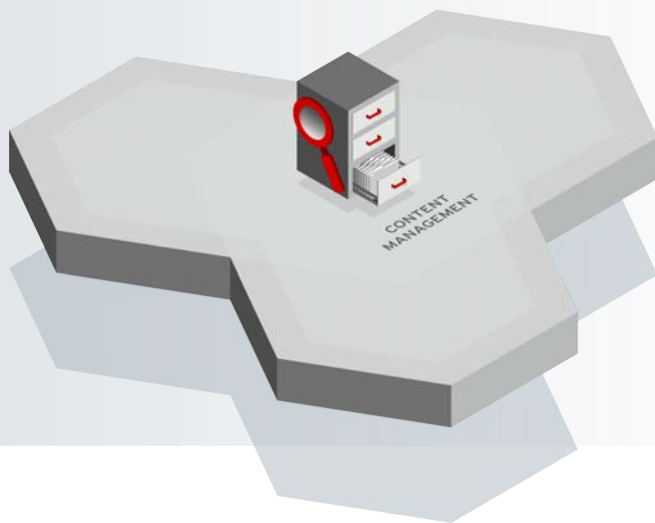
Cloud Connector

Additional functionality coming in future releases



Red Hat Satellite

Content Management



Content Repository any type of content made available to any host

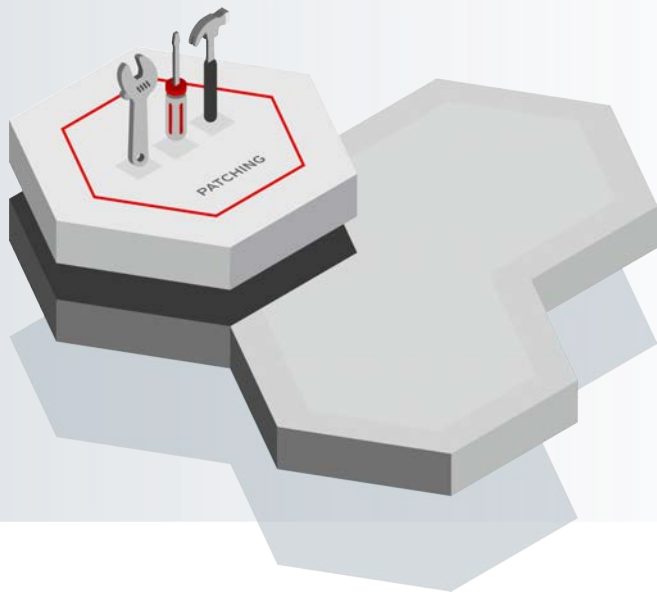


Curation of content prior to distribution



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

Patch Management



Report on hosts that need updates, fixes, or enhancements



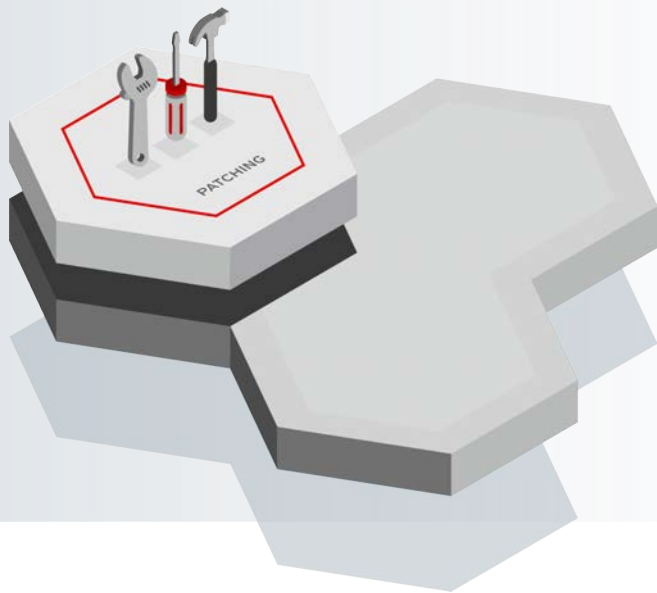
Group homogeneous systems so that you can easily work with them



Respond quickly to patching requirements using scalable automation

Tracer

Post Patch Intelligence



Report on services or processes that require restart or system that require a reboot post patching. (Tracer!)

Tracer's Use Cases

I just patched my system... Now what?

Questions for the audience

- Do you know the impact of your patch set?
- Do I need to reboot after patching?
- If I do not patch the kernel, do I need to restart anything?
- How can you tell if an application or service needs to be restarted?
- What drives the need for an application or service restart?
- Do you know where to look for indicators?

Tracer can help with the following

- Tracer helps you find outdated running applications in your system
- Tracer can identify processes and services that need restarting
- Tracer can provide the service restart command for you
- Tracer can be integrated into Satellite to provide feedback on the need for process/service restarts

Detailed View of Tracer Results from the Content Hosts Menu

tracer7500.lab.local Unregister Host

Content Hosts > tracer7500.lab.local > Traces 1

Details Provisioning Details Subscriptions Host Collections Tasks Packages Errata Module Streams Traces Repository Sets 2

ⓘ Only the Applications with a Helper can be restarted.

Traces

Filter... Search

3

<input type="checkbox"/>	Application	Type	Helper
<input type="checkbox"/>	atd	daemon	sudo systemctl restart atd
<input type="checkbox"/>	auditd	daemon	sudo systemctl restart auditd
<input type="checkbox"/>	chronyd	daemon	sudo systemctl restart chronyd
<input type="checkbox"/>	crond	daemon	sudo systemctl restart crond
<input type="checkbox"/>	dbus	static	You will have to reboot your computer
<input type="checkbox"/>	getty@tty1	session	You will have to log out & log in again
<input type="checkbox"/>	goferd	daemon	sudo systemctl restart goferd

4 Restart Selected

0 of 20 Selected

Kpatch

Security is important

Scheduling reboots is difficult

Live Kernel Patching allows customers to patch **select** critical and important kernel security CVE's, without rebooting or restarting applications

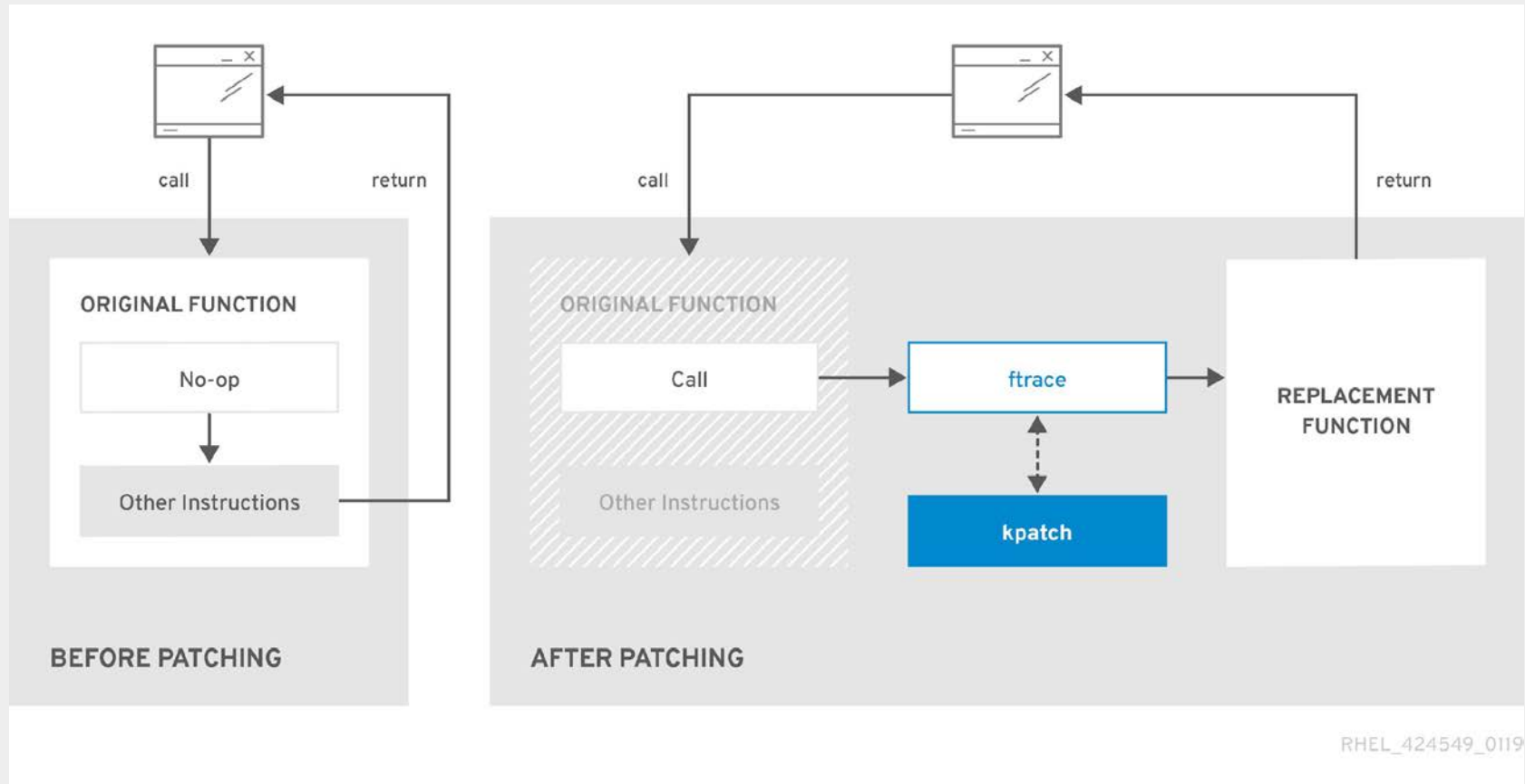
Kpatch Use Cases

- **Good Use Cases**

- to reduce the required reboots for security-related patches
- to introduce a security fix at a time that is not convenient for a reboot
- to integrate into a security driven VAP (Vulnerability Assessment Process) process

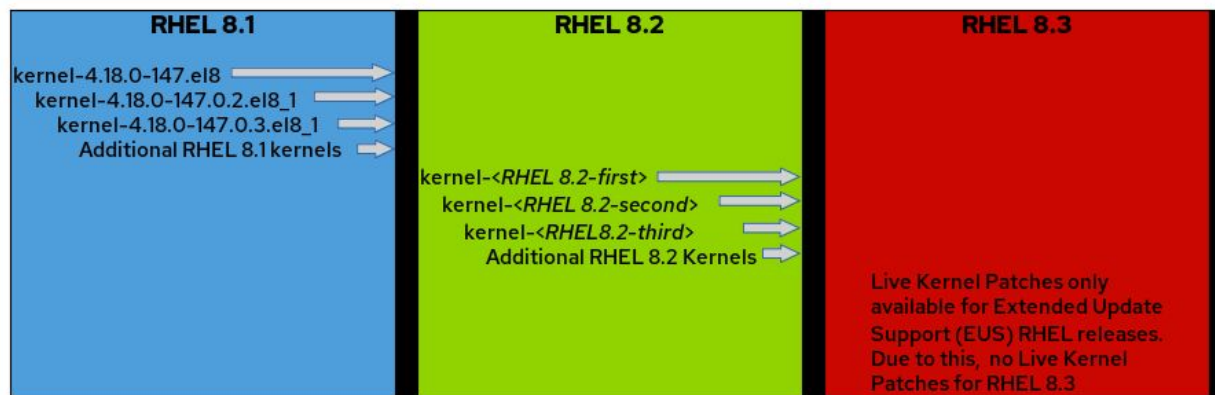
- **!Good Use Cases**

- to eliminate the need for patching in an environment
- to add new OS features to a running environment
- to patch userland software (applications, libraries, etc.)
- to patch 3rd party software



Standard RHEL Subscriptions

Live Kernel Patches Available Until Next Minor Release

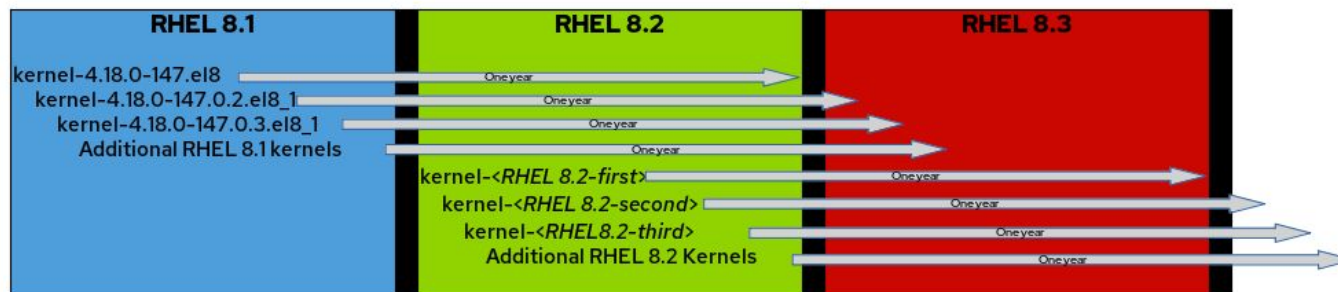


EUS Releases:

8.1
8.2
8.4
8.6
8.8

Extended Update Support RHEL Subscriptions

Live Kernel Patches Available for One Year After Kernel Release Date



<https://www.youtube.com/watch?v=RHKESTHFm0o>

YouTube

Search

RHEL 8.1 - Live Kernel Patching

Brian Smith
Senior Technical Account Manager

0:00 / 5:50

Red Hat

RHEL 8.1 - Live Kernel Patching

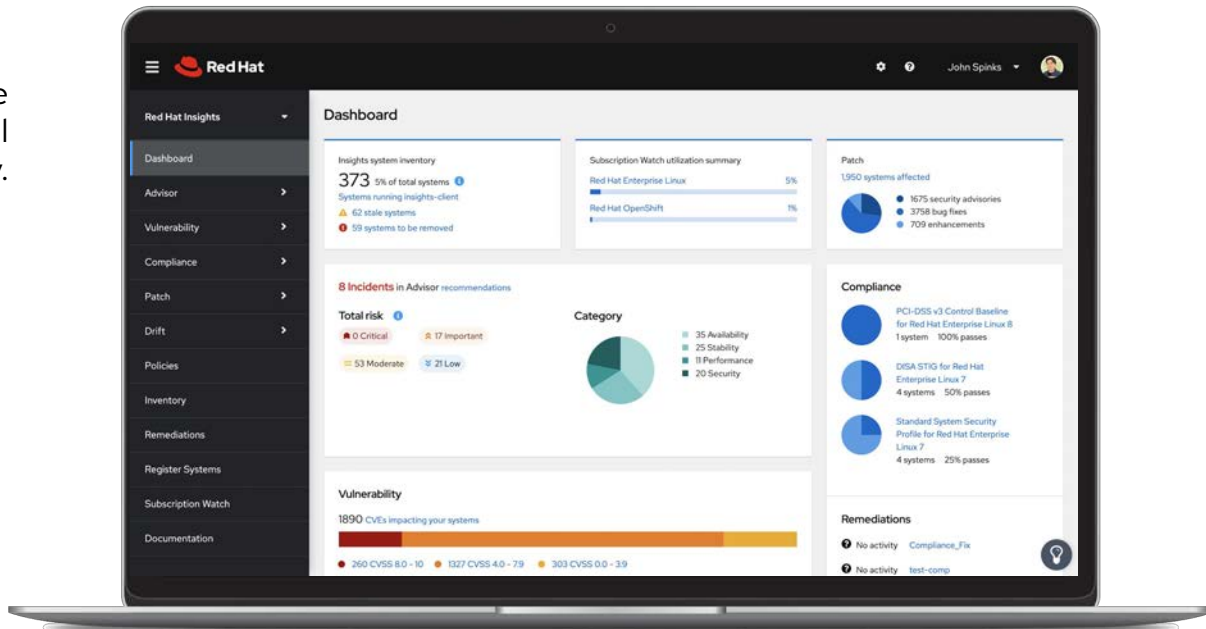
3,898 views · Dec 13, 2019

136 0 SHARE SAVE ...

Red Hat Insights

Included with Red Hat Enterprise Linux subscription, now with more value

New and expanded services provide additional security and operational efficiency.



Red Hat Insights Services



Advisor

Availability, performance, stability, and security risk analysis



Vulnerability

Assess Common Vulnerabilities and Exposures (CVEs) with advisories



Compliance

Assess and monitor compliance, built on OpenSCAP



Subscription Watch

Track progress of your Red Hat subscription usage efficiently and confidently



Drift

Create baselines and compare system profiles



Policies

Define and monitor against your own policies to identify misalignment



Patch

Analyze for Red Hat product advisory applicability to stay up to date

Vulnerability

Vulnerability

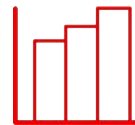
Remediate all Common Vulnerabilities and Exposures (CVEs)



Assess and monitor the risk of vulnerabilities that impact Red Hat products with operational ease



Remediate known Common Vulnerabilities and Exposures (CVEs)

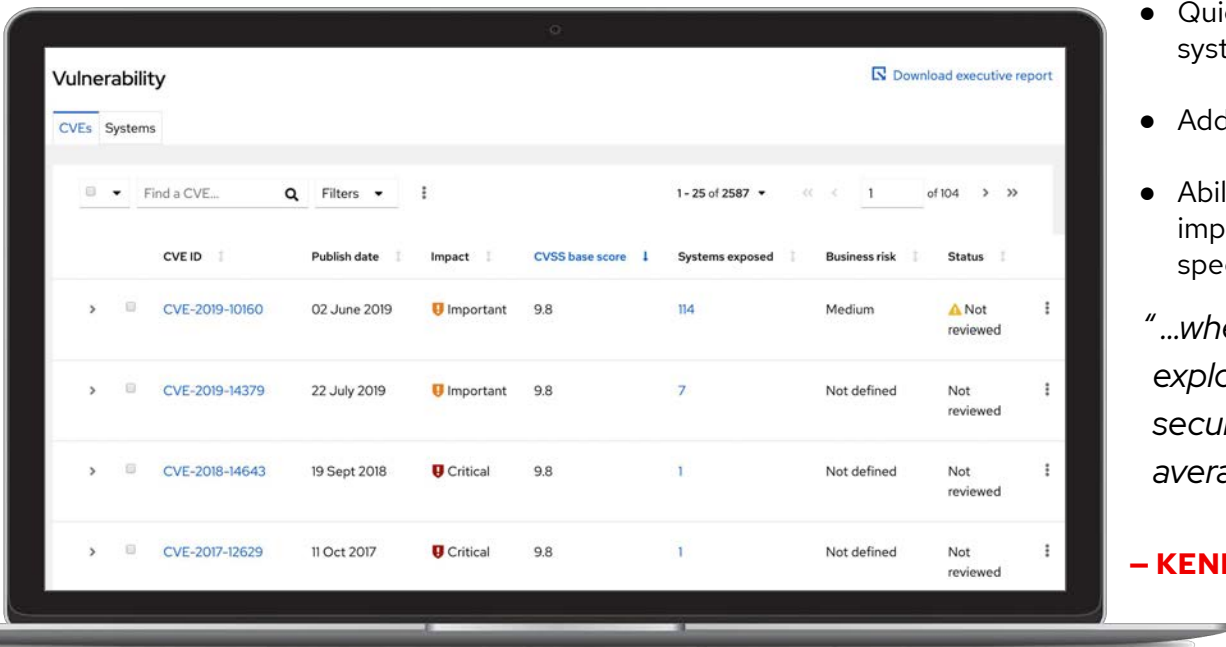


Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

Quickly identify and remediate systems impacted by specific CVEs and create a plan for resolution

Get ahead of key security risks

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



CVE ID	Publish date	Impact	CVSS base score	Systems exposed	Business risk	Status
CVE-2019-10160	02 June 2019	Important	9.8	114	Medium	Not reviewed
CVE-2019-14379	22 July 2019	Important	9.8	7	Not defined	Not reviewed
CVE-2018-14643	19 Sept 2018	Critical	9.8	1	Not defined	Not reviewed
CVE-2017-12629	11 Oct 2017	Critical	9.8	1	Not defined	Not reviewed

- Quick view of CVEs, CVSS score, impact, and systems exposed across all systems
- Add your own business risk and status
- Ability to create a remediation plan for all hosts impacted by a CVE, or for all CVEs for a specific host

*"...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



Patch

Patch

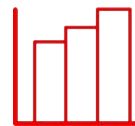
Patch systems to keep them up to date



Assess and monitor Red Hat product advisories (errata) across all deployment footprints

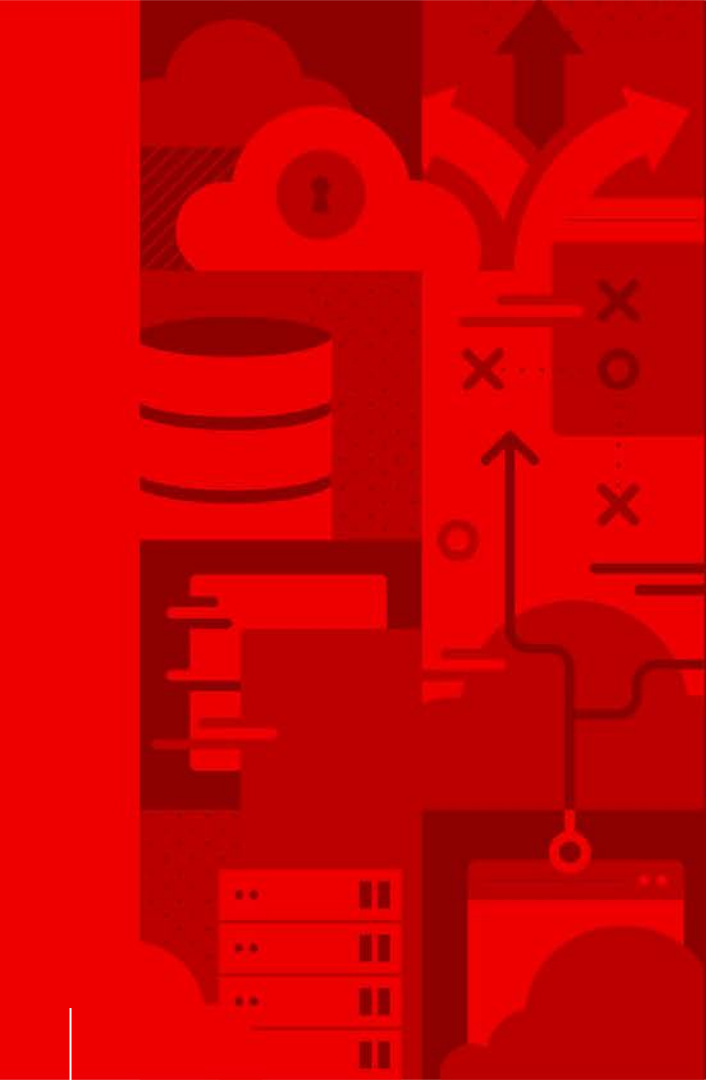


Prioritize most important advisories based on advisory type, severity, and system criticality.



Discover systems that have fallen behind your patching process

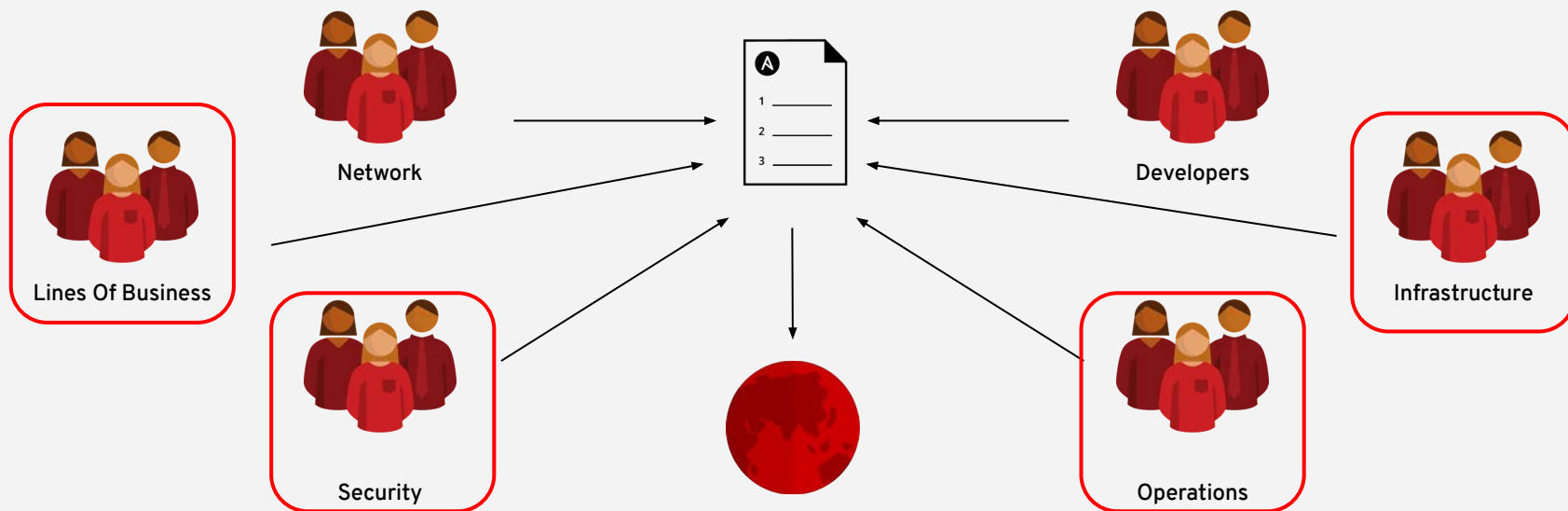
Patch will show you all available Red Hat advisories for every system registered to Insights



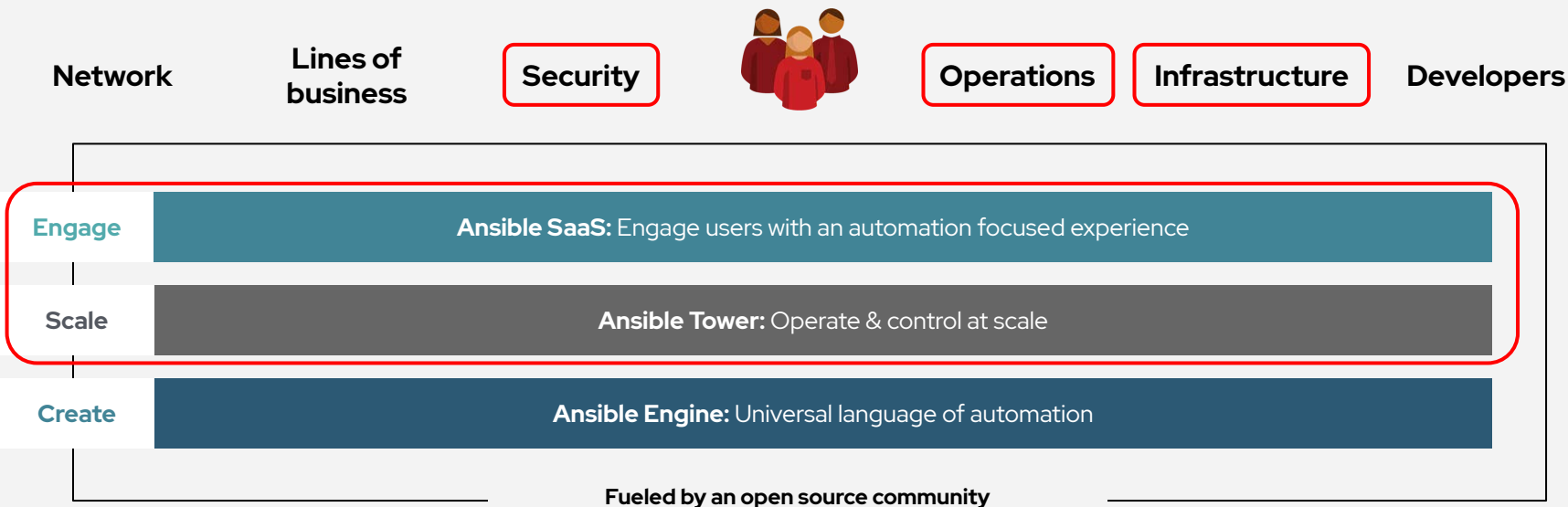
Technical Tools in the Toolbelt: Red Hat Ansible Automation Platform

Red Hat Ansible Automation Platform

Patching at scale requires automation, and when automation crosses teams,
you need an automation platform



Red Hat Ansible Automation Platform



Why Ansible?



Simple

Human readable automation
No special coding skills needed
Tasks executed in order
Usable by every team
Get productive quickly




Powerful

App deployment
Configuration management
Workflow orchestration
Network automation
Orchestrate the app lifecycle



Agentless

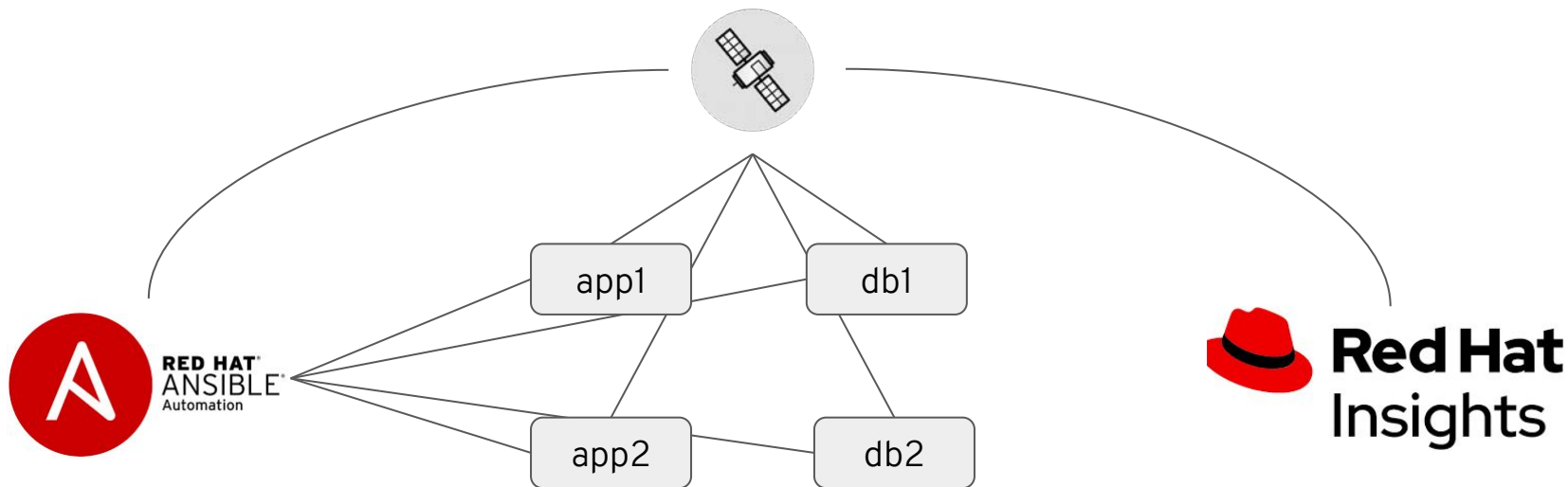
Agentless architecture
Uses OpenSSH & WinRM
No agents to exploit or update
Get started immediately
More efficient & more secure



An Example Enterprise Patching Architecture

An Example Patching Architecture

**Ansible as our orchestrator, Satellite as our content controller,
and Insights as our reporting and remediation engine**

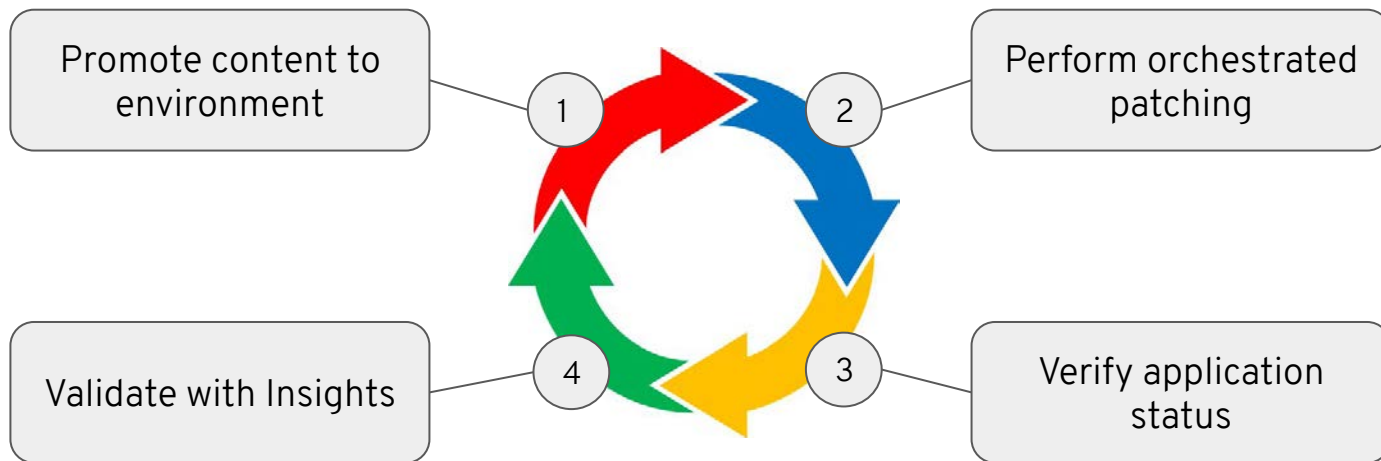




An Example Enterprise Patching Procedure

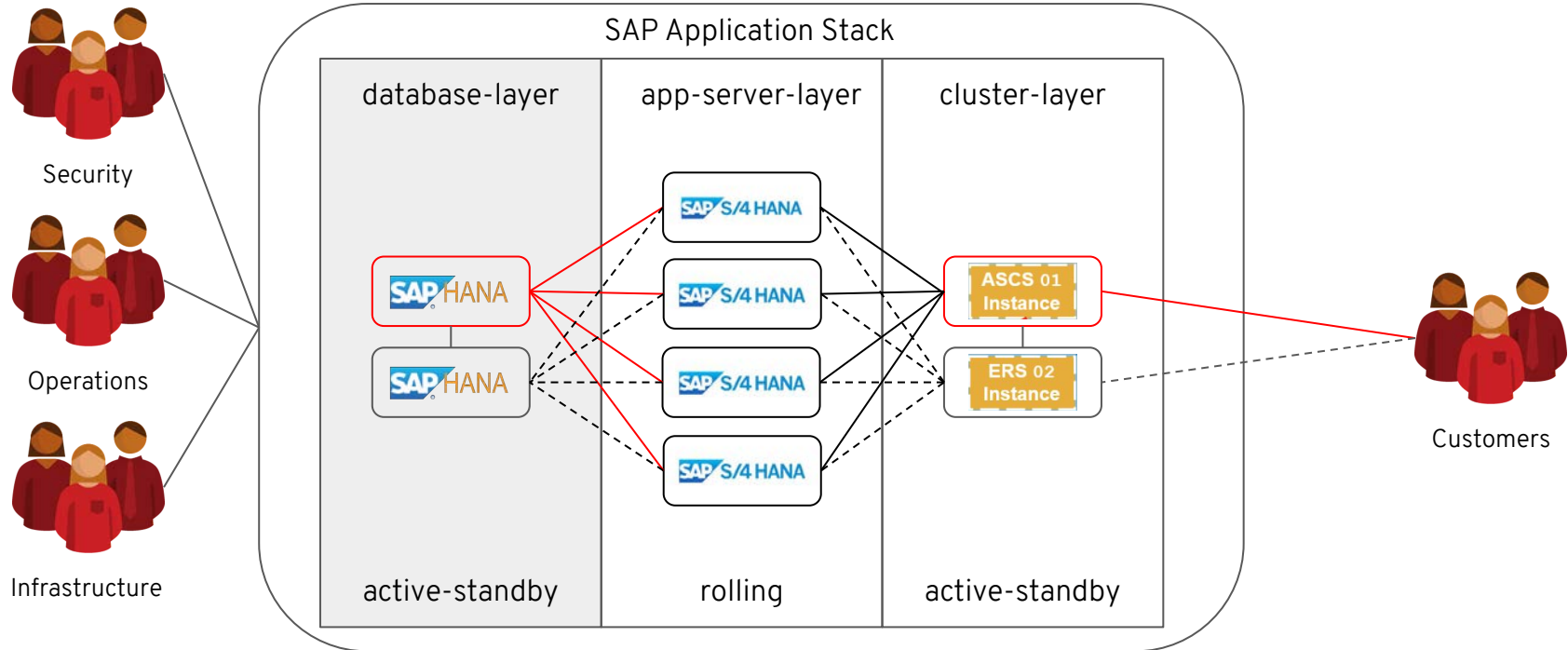
An Example Patching Procedure

Patching is a repeatable cycle



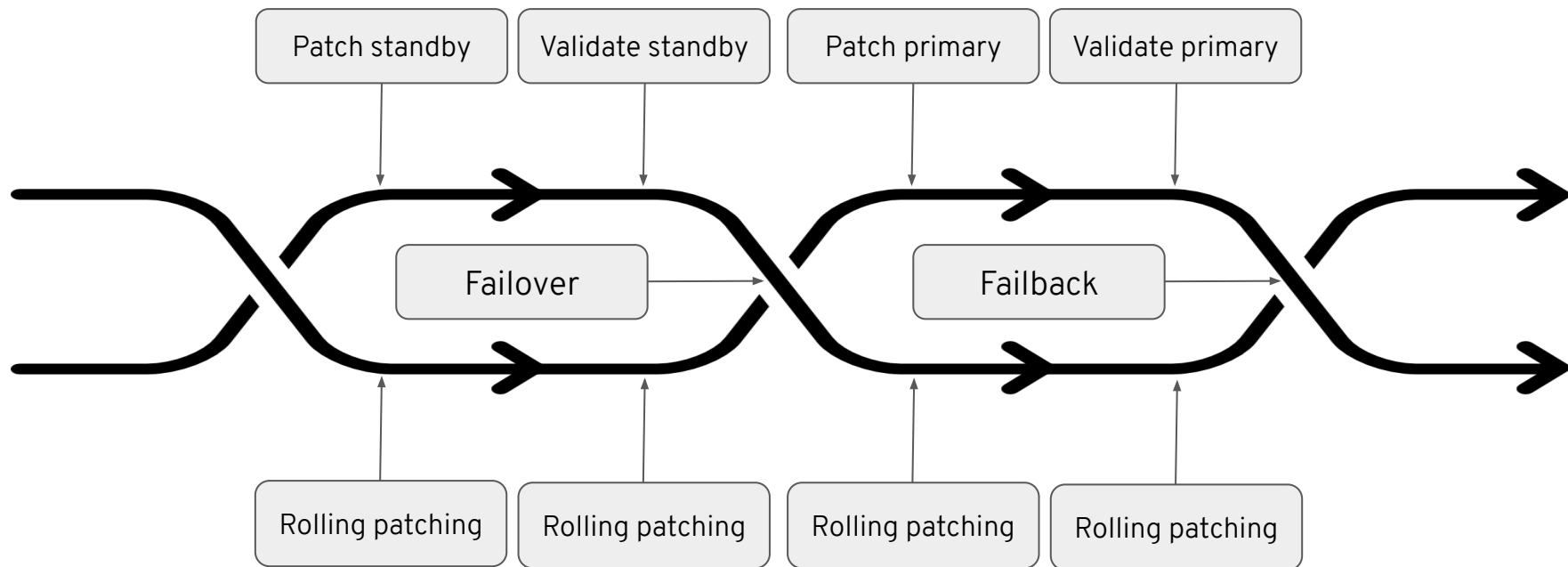
An Example Patching Procedure

How do we patch mission critical applications with minimal impact to the business?

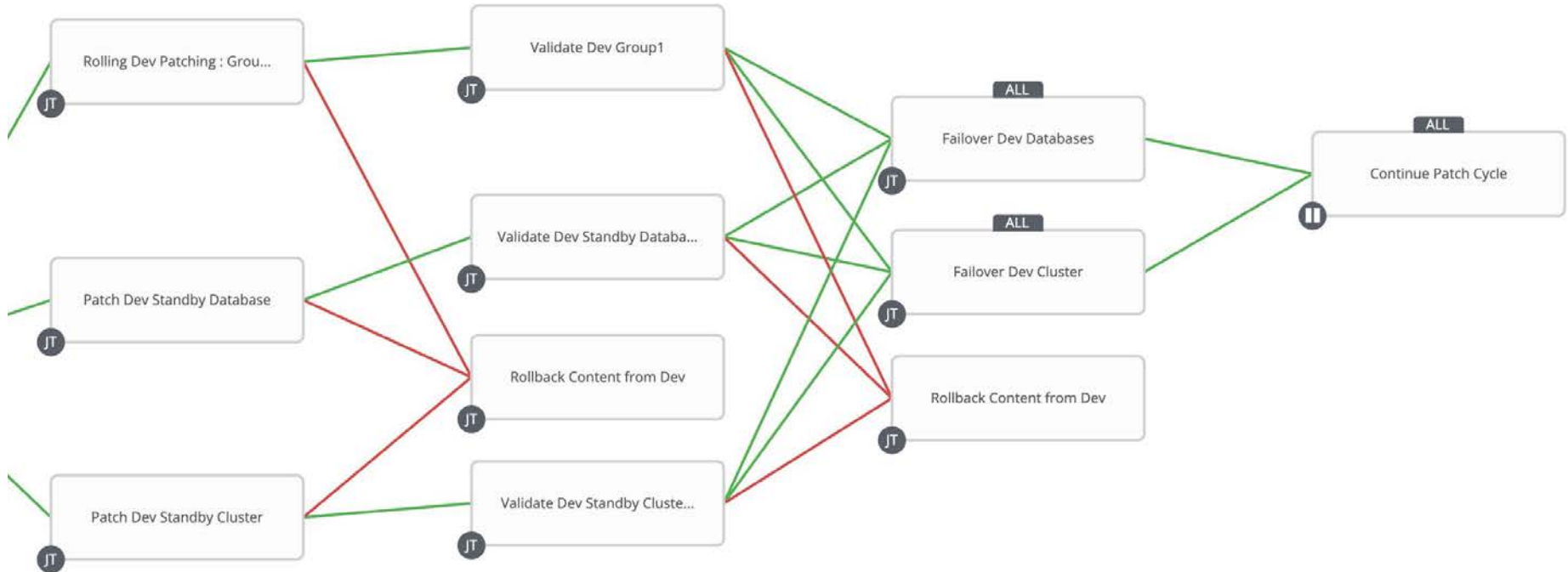


An Example Patching Procedure

Convergence and divergence orchestrated by Ansible



An Example Patching Procedure





Demo

Thank you!



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat