

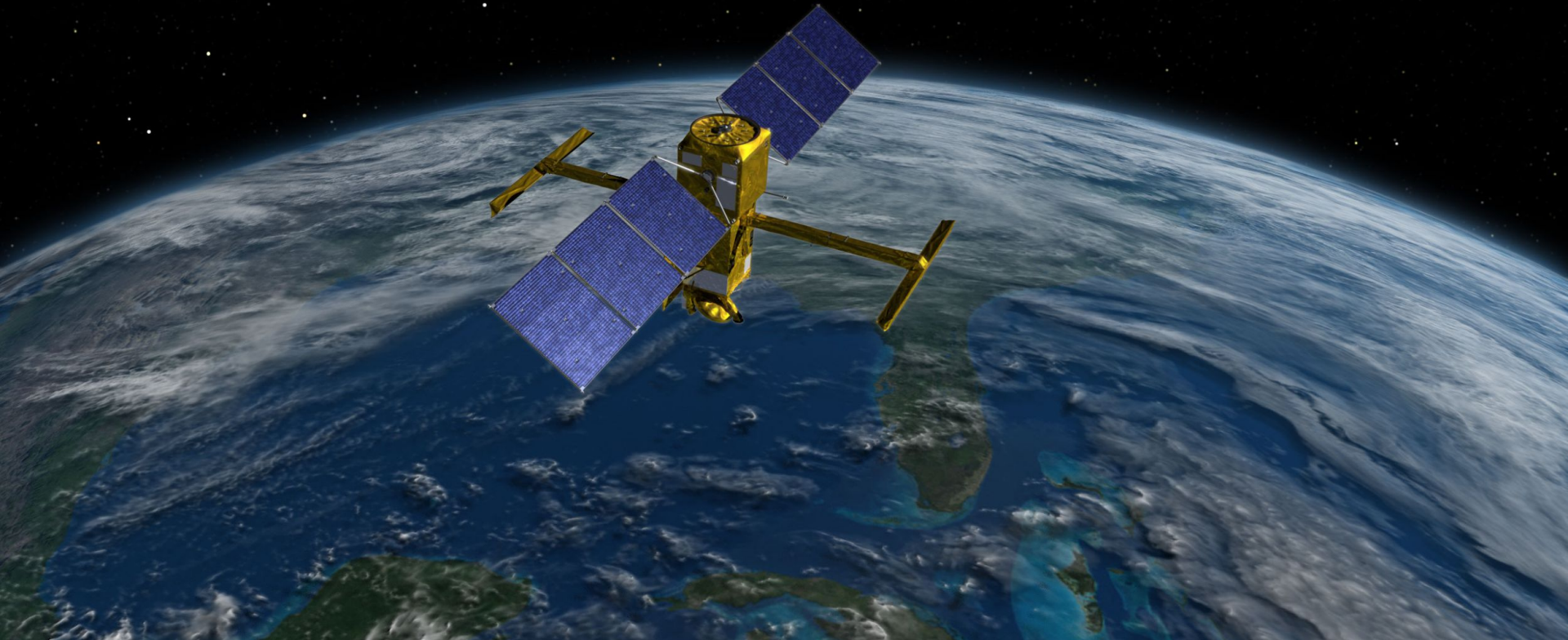


Continuous remediation with Red Hat automation

An Architecture Blueprint

Brian Dumont
Sr. Solutions Architect

INSIGHTS & AUTOMATION



Modern application infrastructure includes many elements and complexity. Keeping that infrastructure safe and compliant is a challenge.

Infrastructure vulnerability and compliance remediation can be achieved using a combination of smart management and orchestrated automation using Red Hat solutions.



Day 2 operations automation is critical

In high-performing organizations,
infrastructure delivery *is* software delivery:

API-driven
on-demand
infrastructure

Infrastructure as
code

Automation and
system integration

Software delivery performance metrics

Overview of expanded Red Hat Insights services



Advisor

Availability, performance, and stability risk analysis



Vulnerability

Assess, remediate and report on Red Hat Enterprise Linux Common Vulnerability and Exposures (CVEs)



Compliance

Assess and monitor regulatory compliance, built on OpenSCAP



Drift

Create baselines and compare system profiles



Policies

Define and monitor against your own policies to identify misalignment



Patch

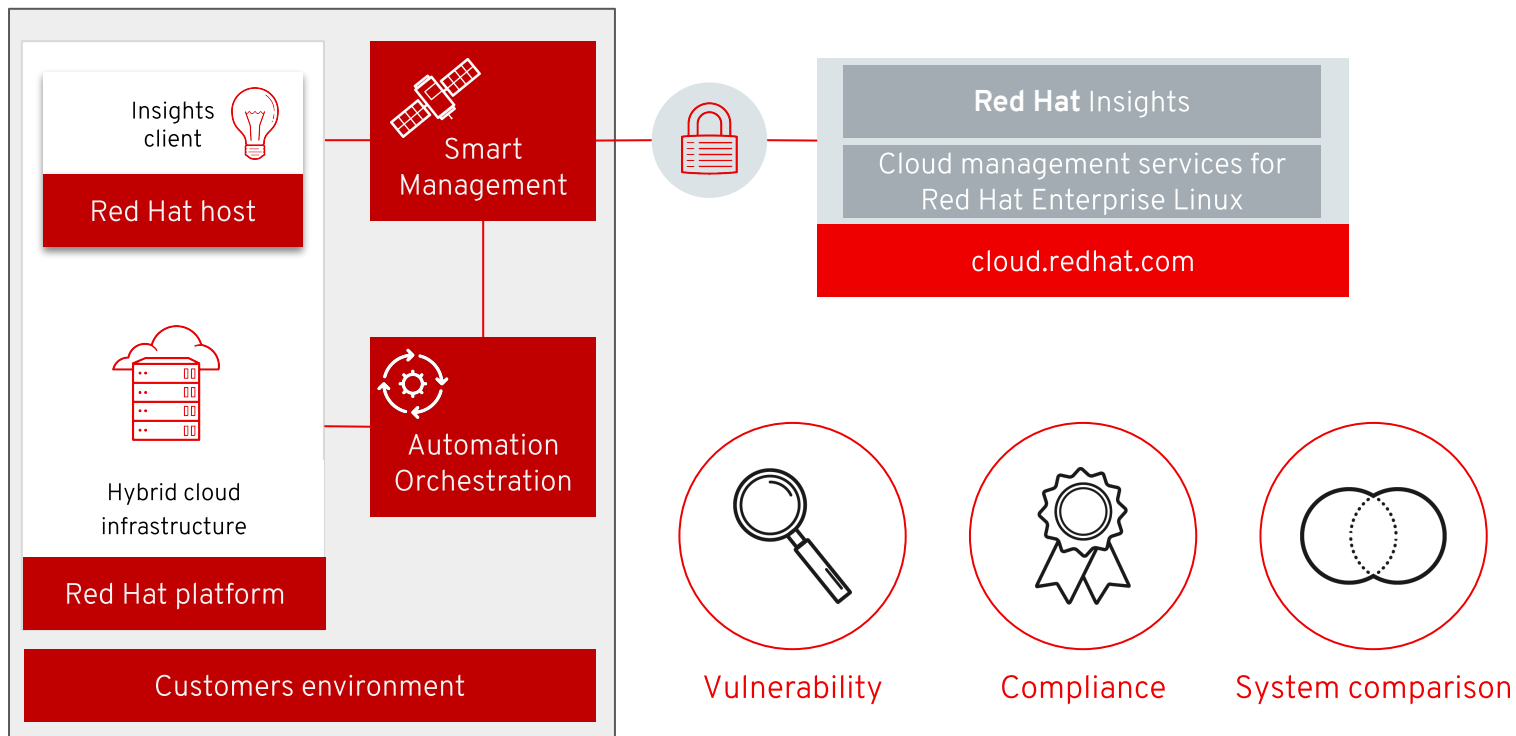
Analyze for Red Hat product advisory applicability to stay up to date

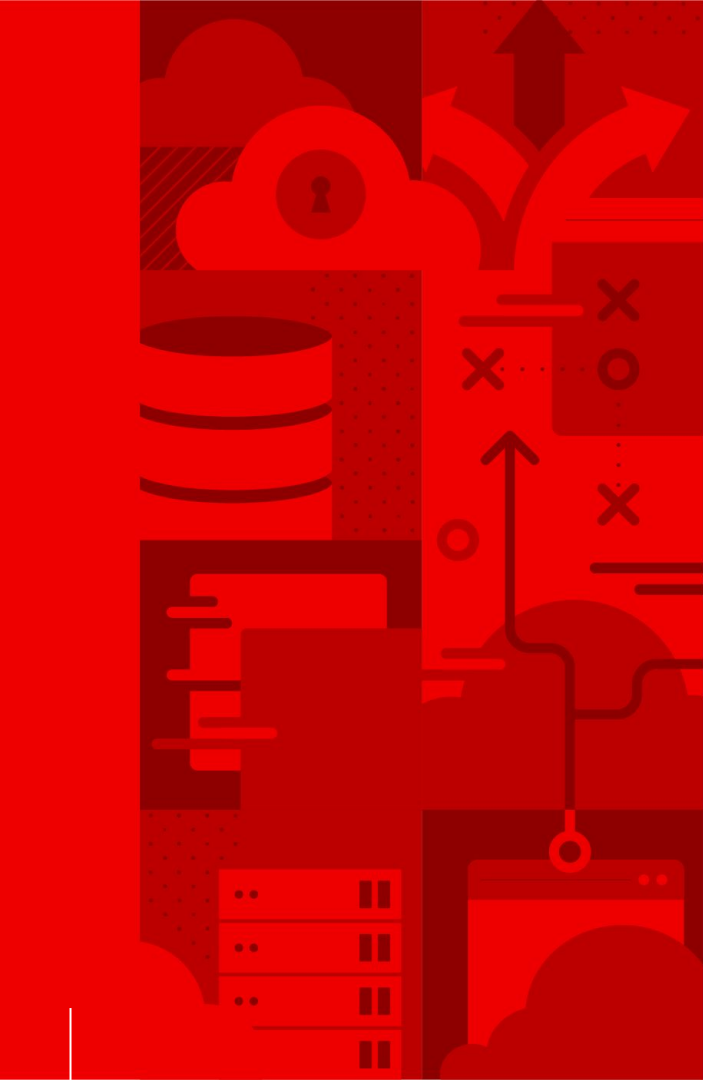


Subscription Watch

Track progress of your Red Hat subscription usage efficiently and confidently.

Red Hat Automation & Management





OpenSCAP - What is it?

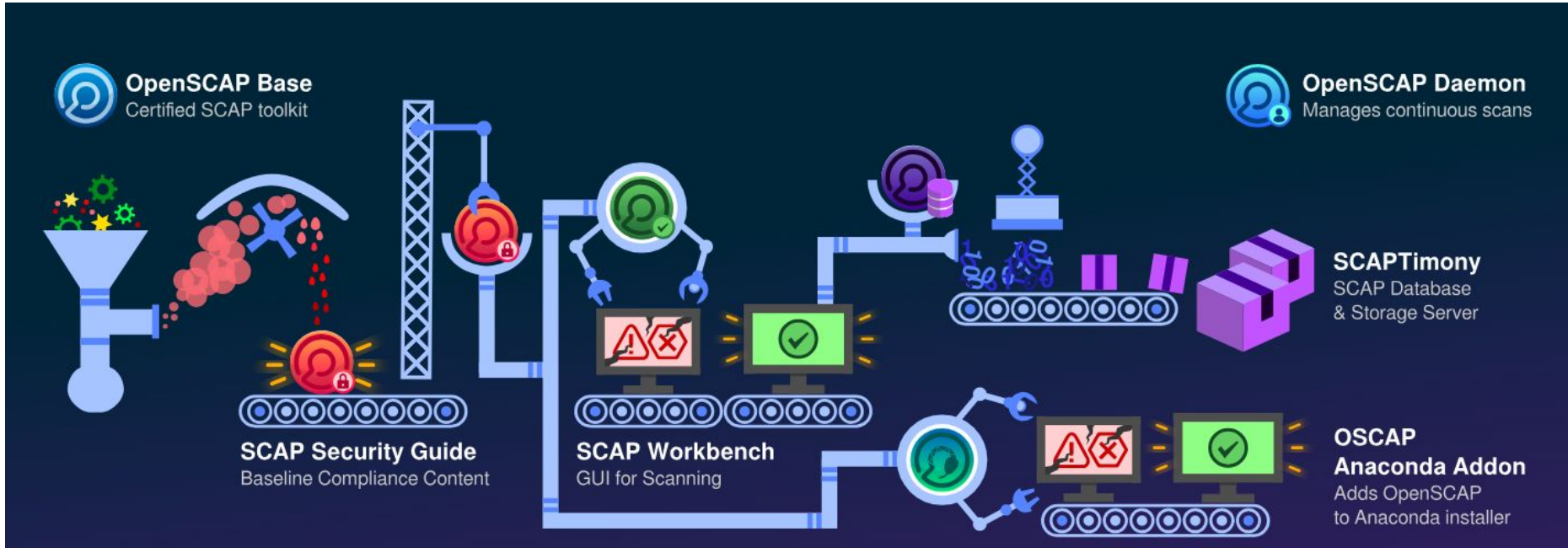
What is SCAP?

- **Security Content Automation Protocol**
- Managed by National Institute of Standards and Technology (NIST)
- Standardized method of maintaining security of systems
 - Vulnerability and configuration security baselines
- Helps comply with security standards
 - DISA STIG
 - PCI-DSS
 - HIPAA
- Red Hat natively ships NIST validated National Checklist content

What is OpenSCAP?

- Security Content Automation Protocol (SCAP) is a method for using a specified standard to enable automated policy compliance evaluations for systems.
- [OpenSCAP](#) is an open source implementation of the SCAP standard.
 - SCAP and OpenSCAP use security policies, also known as SCAP content, as the centerpoint of the compliance strategy.
 - Several security policies are included as part of the [SCAP Security Guide](#).
- You can also create your own policy or customize an existing policy to meet your needs.
 - For the purposes of Insights Compliance, you will need to (for each host):
 - Install the OpenSCAP scanner or the OpenSCAP Workbench.
 - Install the SCAP Security Guide (installed with the workbench by default)
 - Evaluate the host against the selected policy.

OpenSCAP Ecosystem



Two Types of SCAP Security Policies

SECURITY COMPLIANCE

- Proper configuration
- Hardening
- PCI-DSS
- DISA STIG
- USGCB
- HIPAA

VULNERABILITY ASSESSMENT

- Detect CVEs
- Heartbleed
- Shellshock
- Ghost
- VENOM
- ...

RHEL's Approach Toward HIPAA Compliance

- The HIPAA Security Rule establishes U.S. national standards to protect individuals' electronic personal health information
- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
- RHEL 8.3 implements automated compliance to this rule via an OpenSCAP Profile
 - `xccdf_org.ssgproject.content_profile_hipaa`

A vertical graphic on the left side of the slide, rendered in shades of red. It features various icons representing IT infrastructure and management: a cloud with a keyhole, a database cylinder, a server rack, a monitor, and several arrows indicating flow and connectivity. The background is a solid red color.

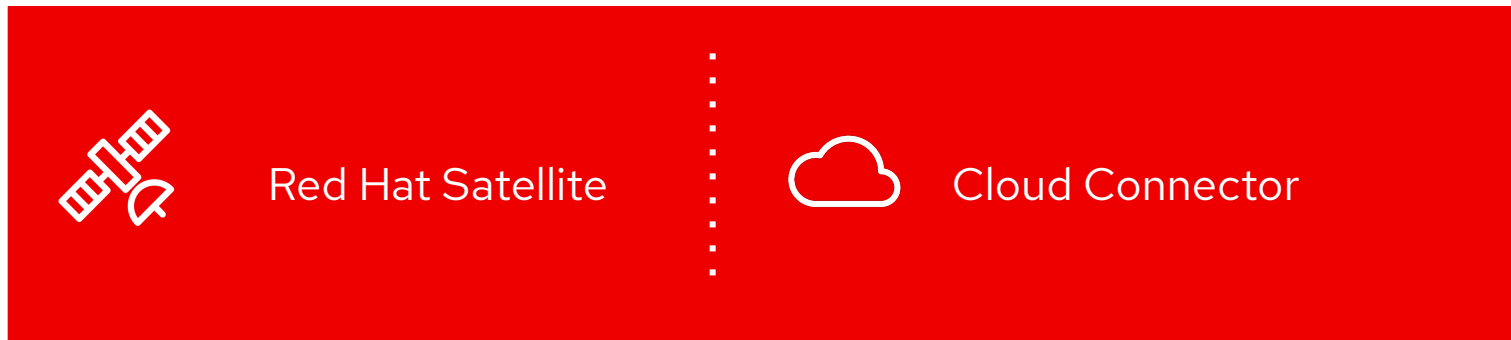
Red Hat Smart Management

What is included

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

What's included with Smart Management?

As of April 2020, Smart Management includes:



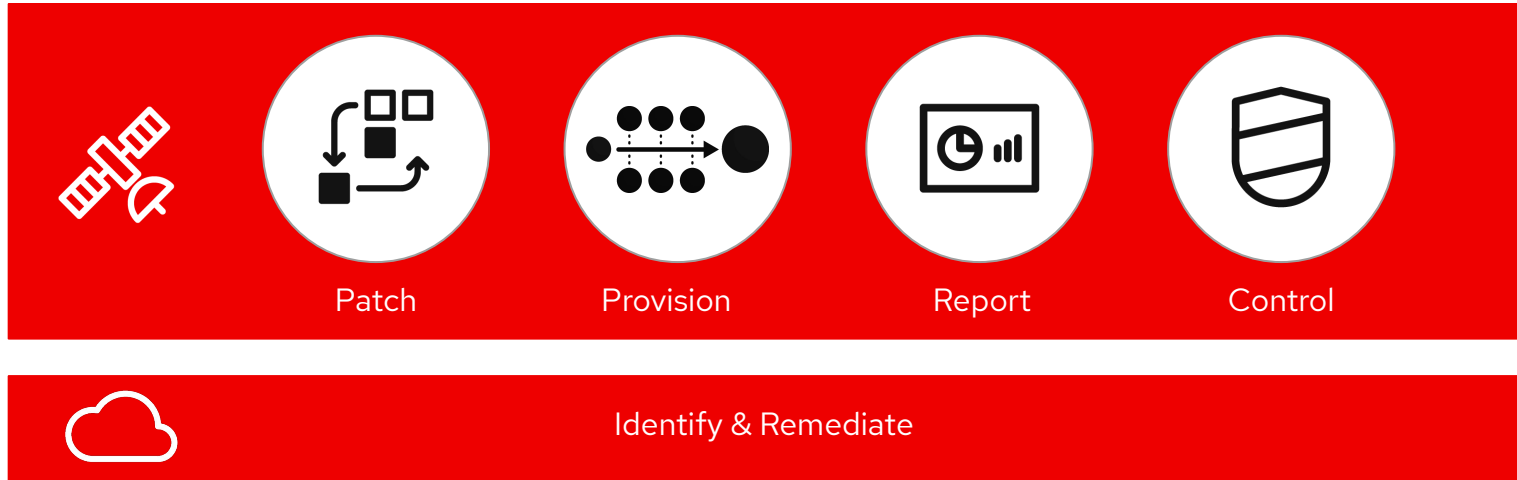
Additional functionality coming in future releases

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 by 28%*

Overcome scale, skill, and security gaps



*Source: [Satellite IDC Business Value Whitepaper](#)



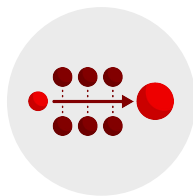
Introduction to Satellite

Capabilities and Outcomes

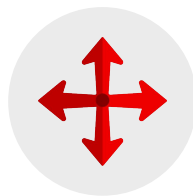
Why Red Hat Satellite?



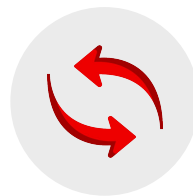
Manage Red Hat®
infrastructure



Streamlined
content management



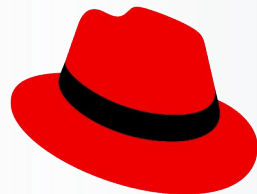
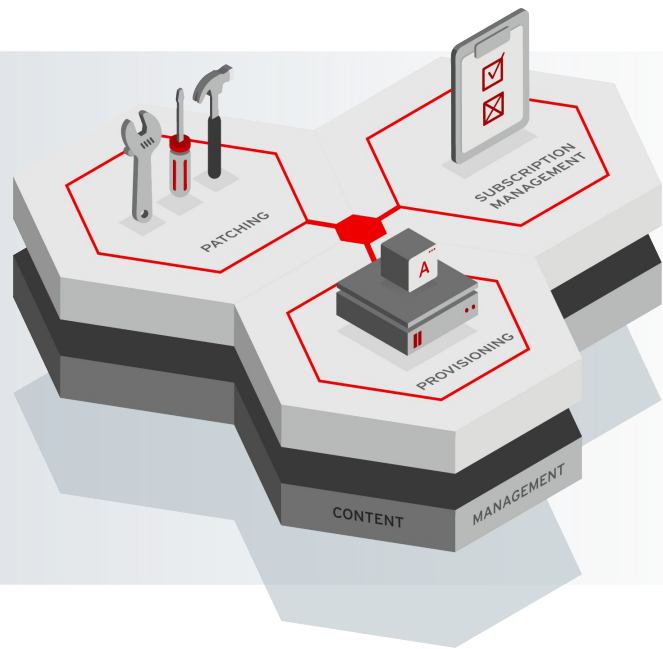
Developed to scale



Simplified
system integration

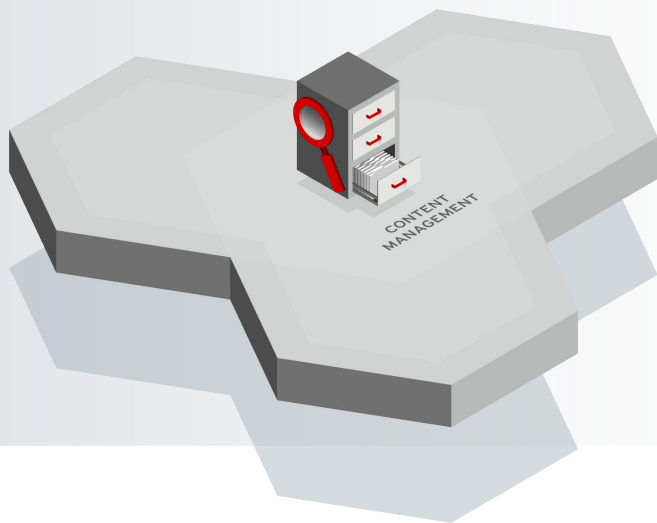


Enhanced drift
and configuration
management



Red Hat Satellite

Content Management



Content Repository any type of content made available to any host

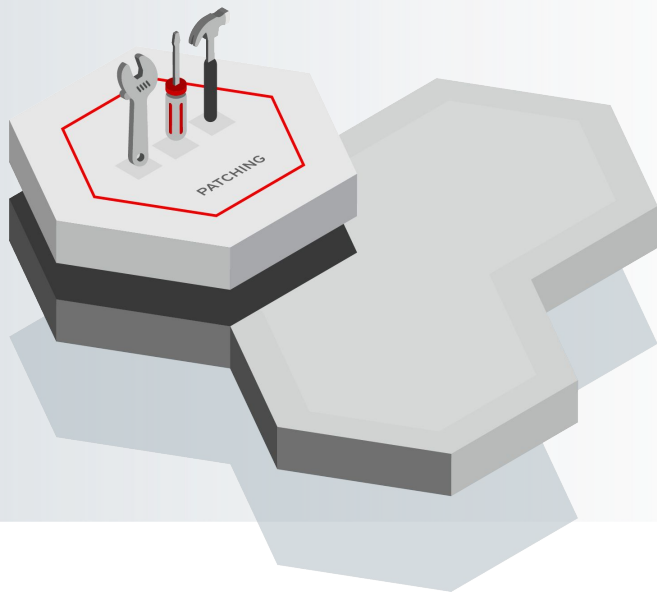


Curation of content prior to distribution



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

Patch Management



Report on hosts that need updates, fixes, or enhancements

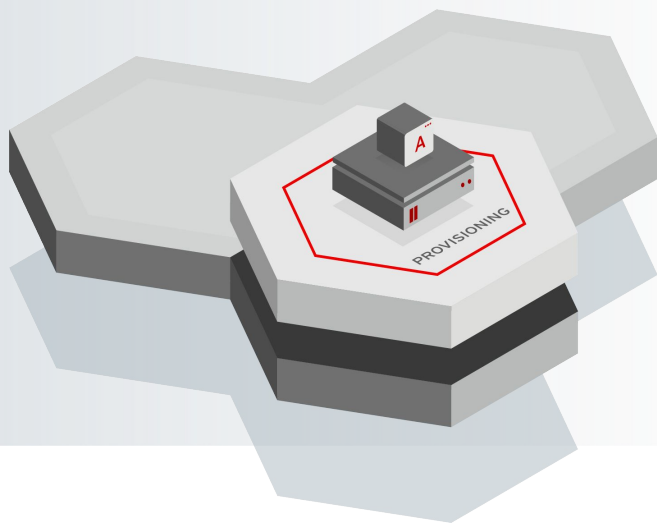


Group homogeneous systems so that you can easily work with them



Respond quickly to patching requirements using scalable automation

Provisioning Management



Provision to bare metal, virtual, private, and public clouds

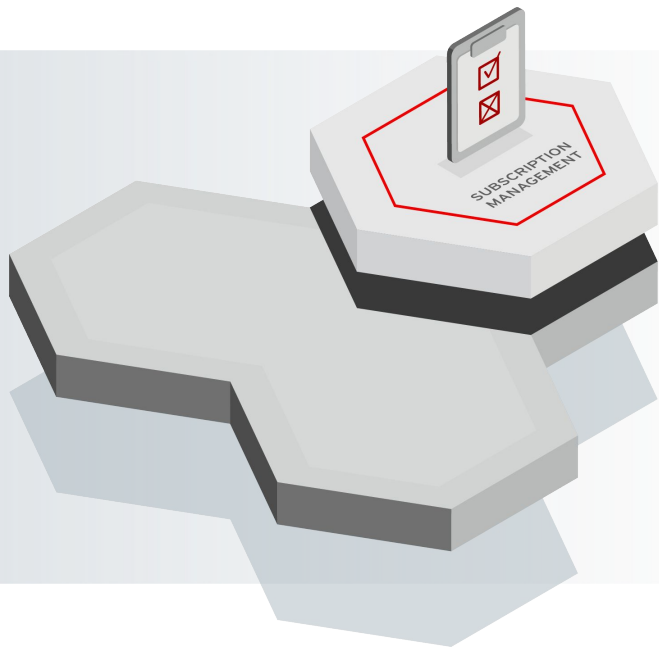


Import non-provisioned hosts



Automate using Ansible roles to perform post-provisioning steps

Subscription Management



Centrally manage subscription usage

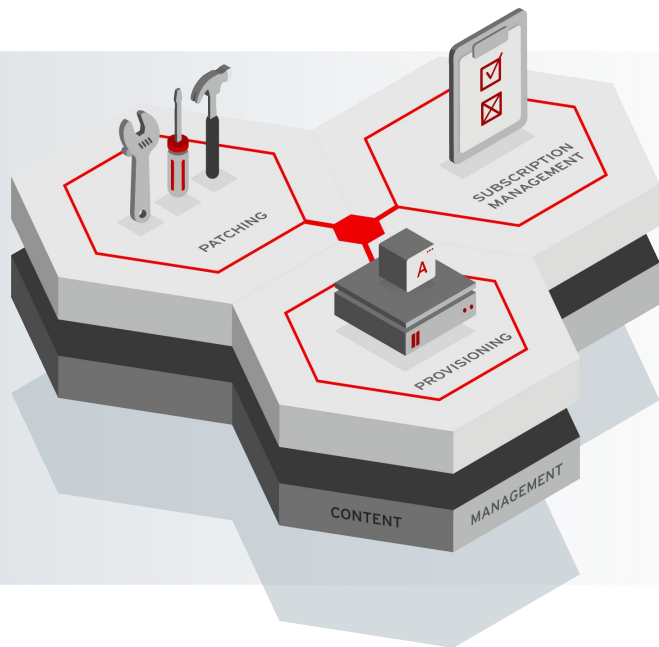


Maintain accurate inventory and utilization information



Report on subscription consumption

Additional Satellite Capabilities



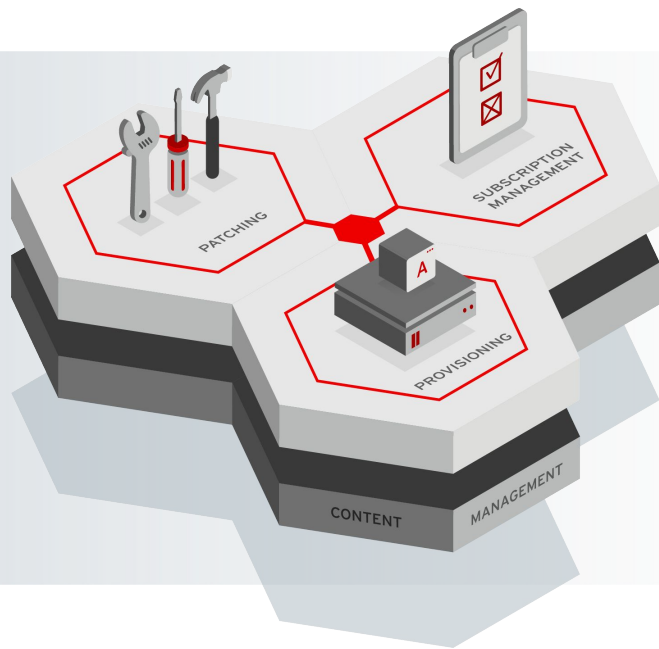
Configuration Management using Ansible



Automation through integration with Ansible Tower



Compliance using OpenSCAP policies



Standard Operating Environment hosts are the same across your environment



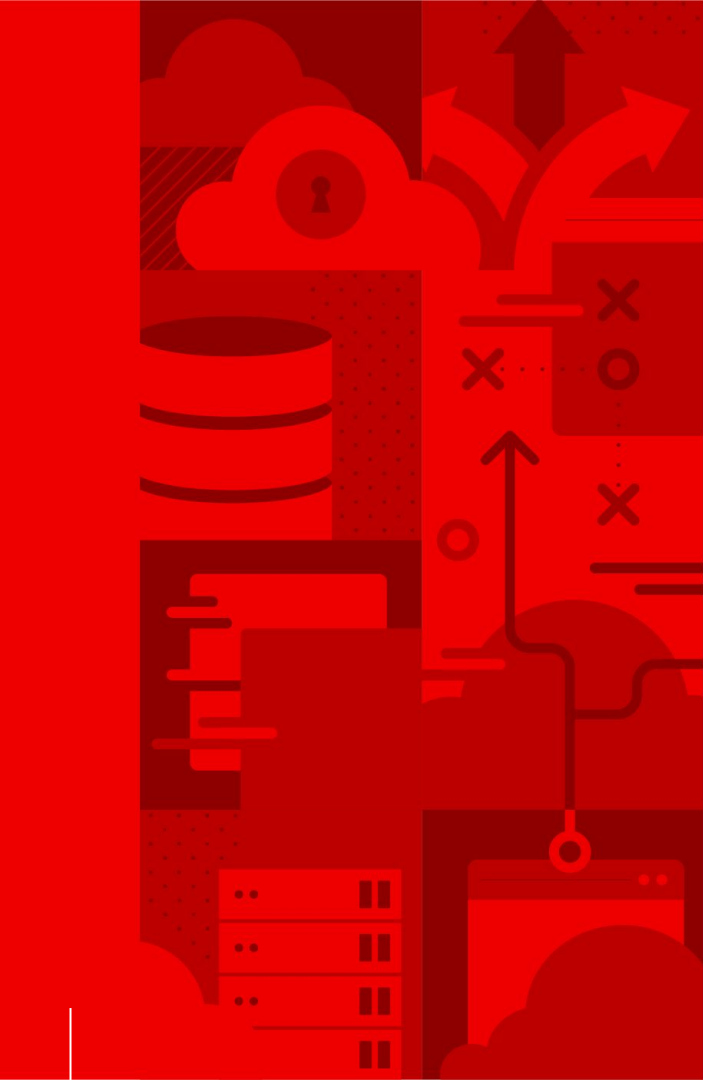
Reliable and Resilient Using Red Hat Insights



Secure your systems are patched, up to date, and compliant with security policies



Confidence in your subscription utilization



Architectural Blueprint

Generic view of the solution architecture

Red Hat Platform Management

Life-cycled content management, automated remediation, and prescriptive analytics.



CONTENT

BUILD A TRUSTED & SECURE RED HAT ENVIRONMENT

- Manage content and patches
- Provision and configure at scale
- Define and implement your SOE



ANALYTICS

PROACTIVE AUTOMATED RESOLUTIONS

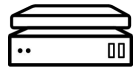
- Continuous insights
- Verified knowledge
- Proactive resolution



AUTOMATION

CENTRALIZED AUTOMATION GOVERNANCE

- Centralized control
- Team & user delegation
- Audit trail



PHYSICAL



VIRTUAL



PRIVATE CLOUD

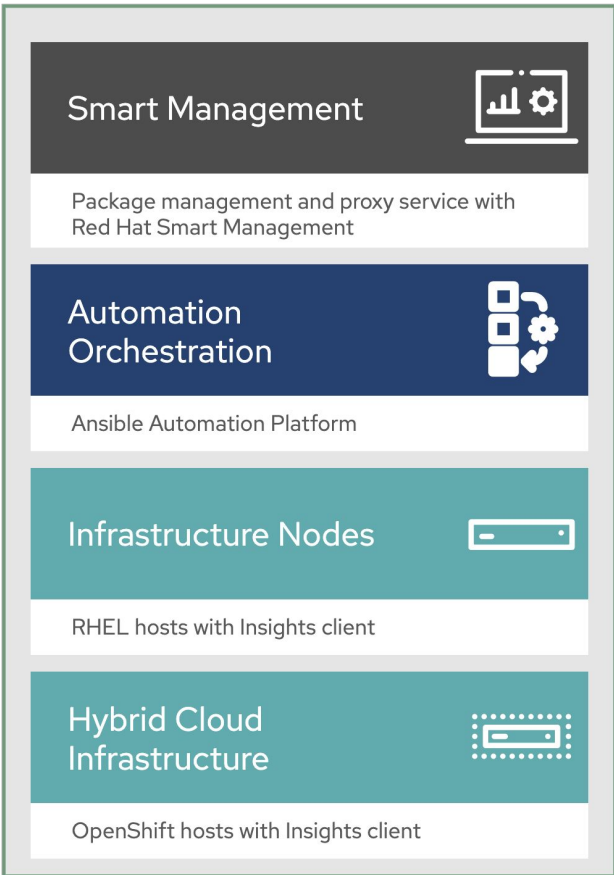


PUBLIC CLOUD

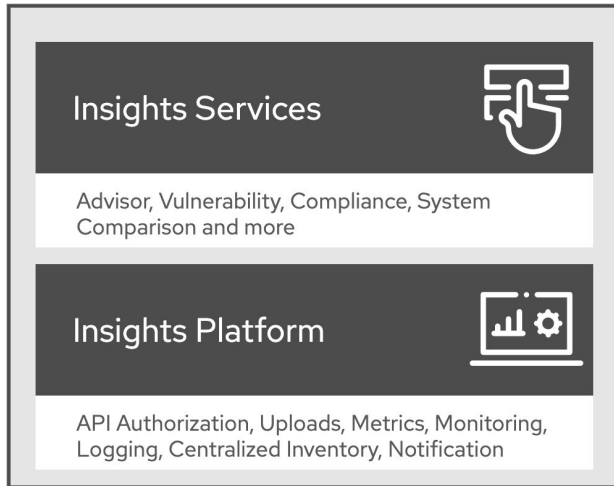
STANDARD OPERATING ENVIRONMENT (SOE)

Logical Deployment

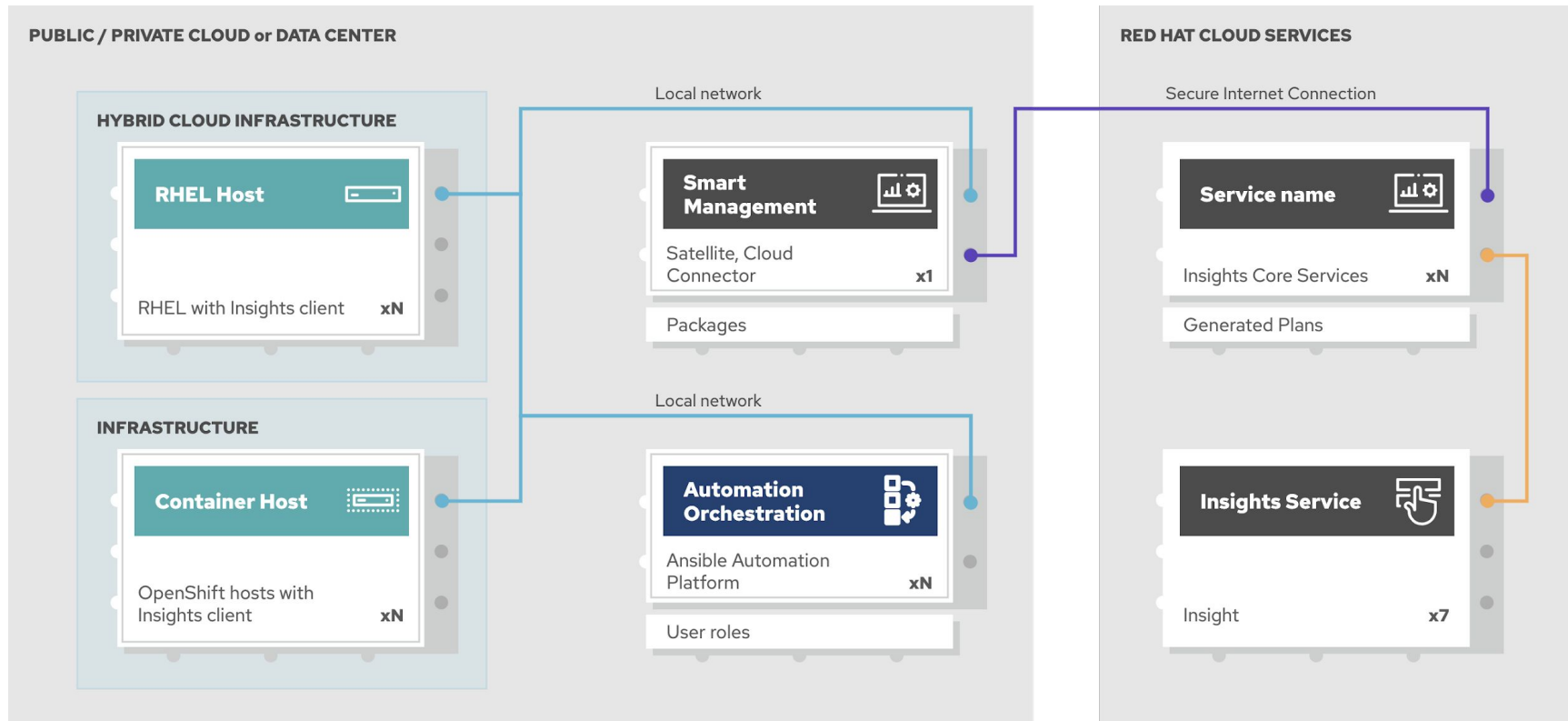
Data Center or Public Cloud



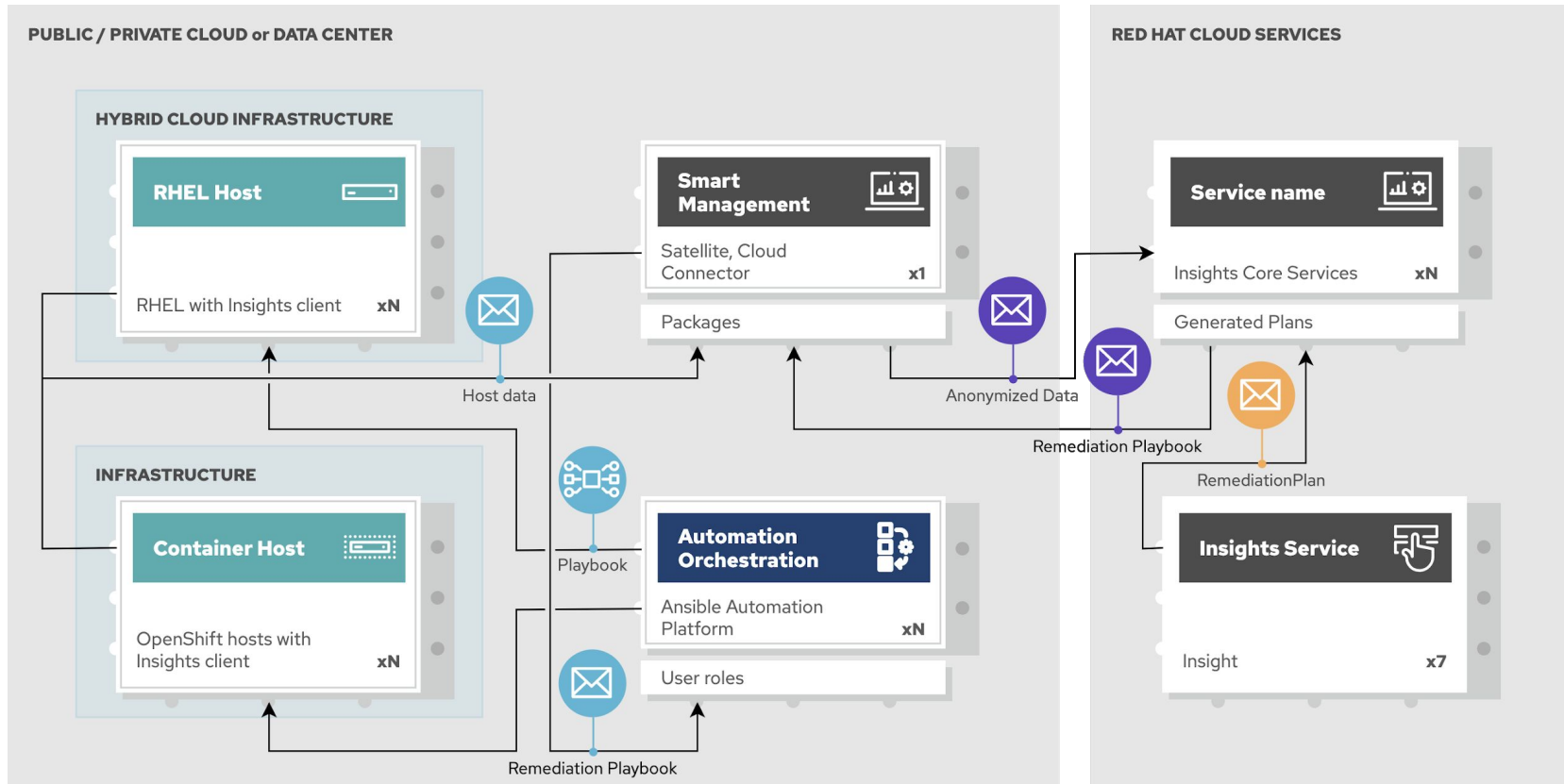
Red Hat hosted Insights



Physical Deployment Blueprint (Network)



Physical Deployment Blueprint (Data Flows)



A vertical red-themed graphic illustration on the left side of the slide. It features various icons representing cloud services, security, and infrastructure. At the top, there's a cloud with a keyhole icon, and another cloud with an upward-pointing arrow. Below these are curved arrows, a database cylinder, a server rack, and a computer monitor. The background is filled with abstract shapes, lines, and symbols like 'X' and 'O', all in shades of red and dark red.

Compliance

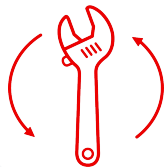
RHEL, Smart Management, Insights and
Ansible working together

Compliance

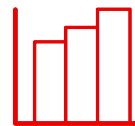
Built on OpenSCAP reporting



Assess and monitor the degree/level of compliance to a policy for Red Hat products with operational ease



Remediate known issues of non-compliance in the Red Hat environment via Ansible playbooks based on business risk & relevance



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

Easily identify and remediate systems which are out of compliance or failing specific rules checks

Compliance reports

By policy

Dashboard ⓘ

Advisor >

Vulnerability

Compliance ▾

Reports

Policies

Systems

Policies

Drift >

Subscription Watch >

Patch

Inventory

Remediations

Documentation

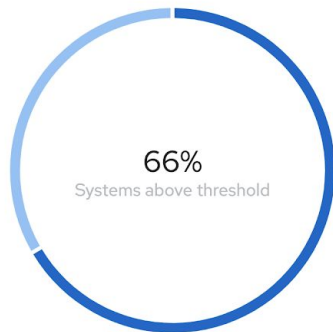
External policy
DISA STIG for Red Hat Enterprise Linux 7

2 of 3

Systems meet compliance threshold

[More details](#)

Global Expansion

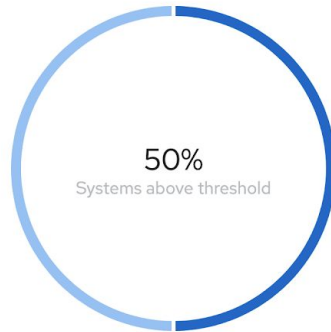


External policy
Standard System Security Profile

1 of 2

Systems meet compliance threshold

[More details](#)



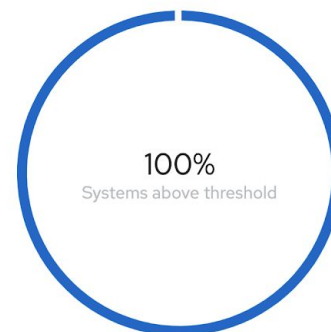
External policy
PCI-DSS v3.2.1 Control Baseline for Red Hat ...

1 of 1

Systems meet compliance threshold

[More details](#)

Test



Easily identify and remediate out of compliance systems and specific rules failing

Compliance

Policies Systems

Search by name Remediate 1 - 41 of 41


Name	Profiles	Compliance score
<input type="checkbox"/> iks8.localdomain	Standard System Security Profile for Red Hat Enterprise Linux 7	100%
<input type="checkbox"/> vm2.gsslab.pnq.redhat.com	Standard System Security Profile	96%
<input type="checkbox"/> ktoordeur-sat65-tcp-haproxy-loadbalancer.sysmgmt.lan	Standard System Security Profile	92%
<input type="checkbox"/> bkinney.rhel75test	Standard System Security Profile	98%

- Report by policy or by system
- Adjustable compliance thresholds
- Easy customization of business objectives
- Can create and tailor your own policies





Thank you

End of research for use case validation..

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

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

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

 twitter.com/RedHat