

The logo features the text "Red Hat Summit" in white on a red background. To the left, there are three overlapping wavy lines in teal, orange, and red. To the right, a trail of red and grey dots extends across the top of the page.

Red Hat
Summit

From here, anywhere

**Red Hat Summit 2020
Virtual Experience
April 28-29**

Immerse yourself in our free virtual event and find your inspiration at the intersection of choice and potential.

Register now

<http://www.redhat.com/summit>



Red Hat Insights

Proactive Analysis and Remediation

Joshua Preston
Solution Architect



Red Hat Insights assesses your Red Hat Enterprise Linux environment to help you **proactively identify and remediate threats**, avoiding outages, unplanned downtime and risks to security and compliance.

Insights Overview

Red Hat Insights

Included with all Red Hat Enterprise Linux subscriptions

Buy



Red Hat
Enterprise Linux

Get



Red Hat
Insights

- Requires an active RHEL subscription on versions 6.4 & higher

Overview of Red Hat Insights



Advisor

Availability, performance, and stability risk analysis



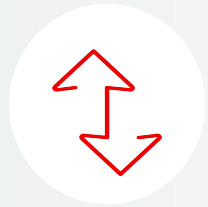
Vulnerability

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



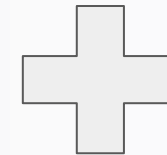
Policies

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.

Why Red Hat Insights?

Operational Efficiency



**Comprehensive analysis
with Red Hat expertise**



**Continuous
vulnerability alerts**



**Increased visibility
to security risks**

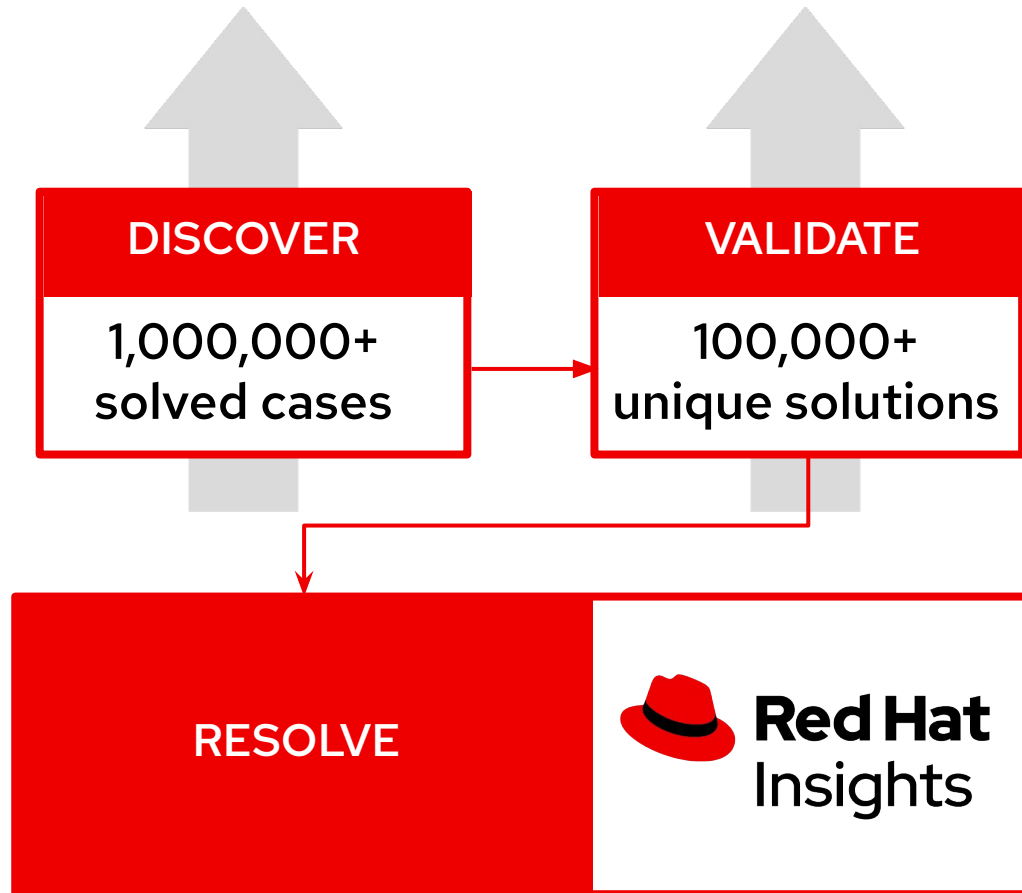


**Simple
remediation**

Single, consistent management solution across on-premise, hybrid cloud, and public cloud.

Security Risk Management

Value of experience



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

– RED HAT GLOBAL SUPPORT SERVICES

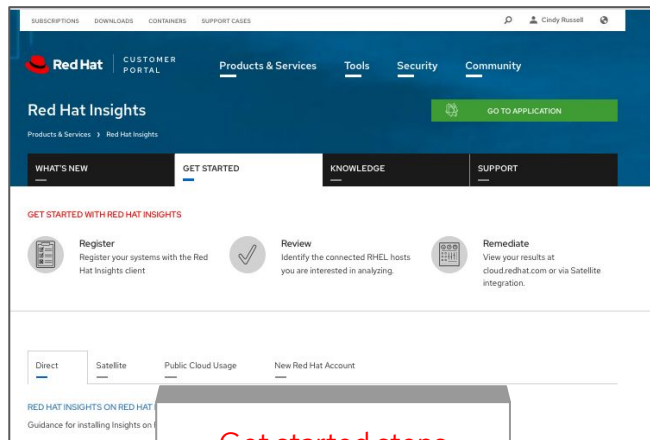
Continuous identification of new risks driven by unique industry data

Based on real-world results from millions of enterprise deployments

Three steps to advanced RHEL management

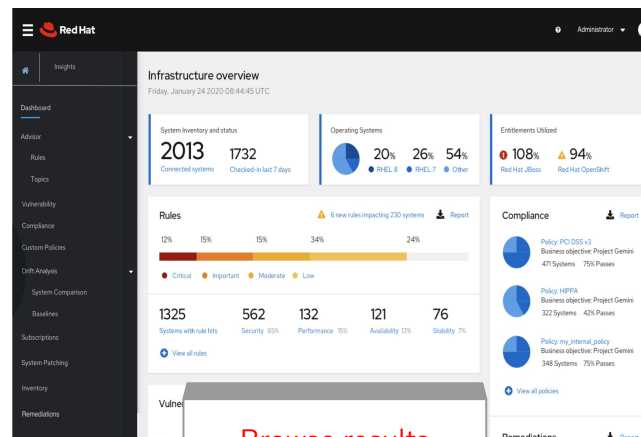
Register

Install client for Red Hat instances on-premises, virtual, cloud.



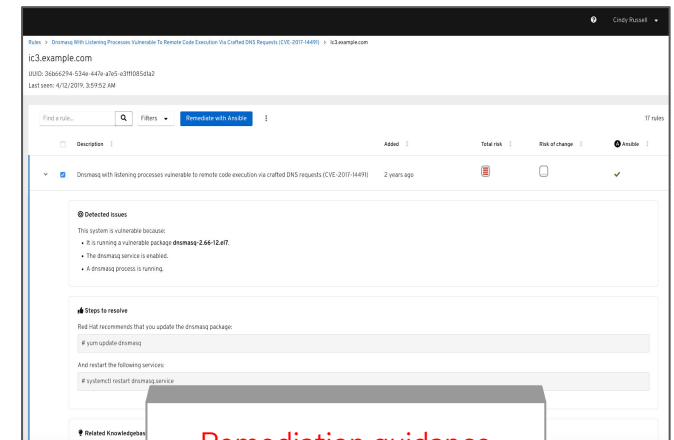
Review

Insights client runs and issues found are reported in the Insights dashboard at cloud.redhat.com



Remediate

Review issues and results in the dashboard and choose which you would like to remediate. Leverage guidance, and remediation options.

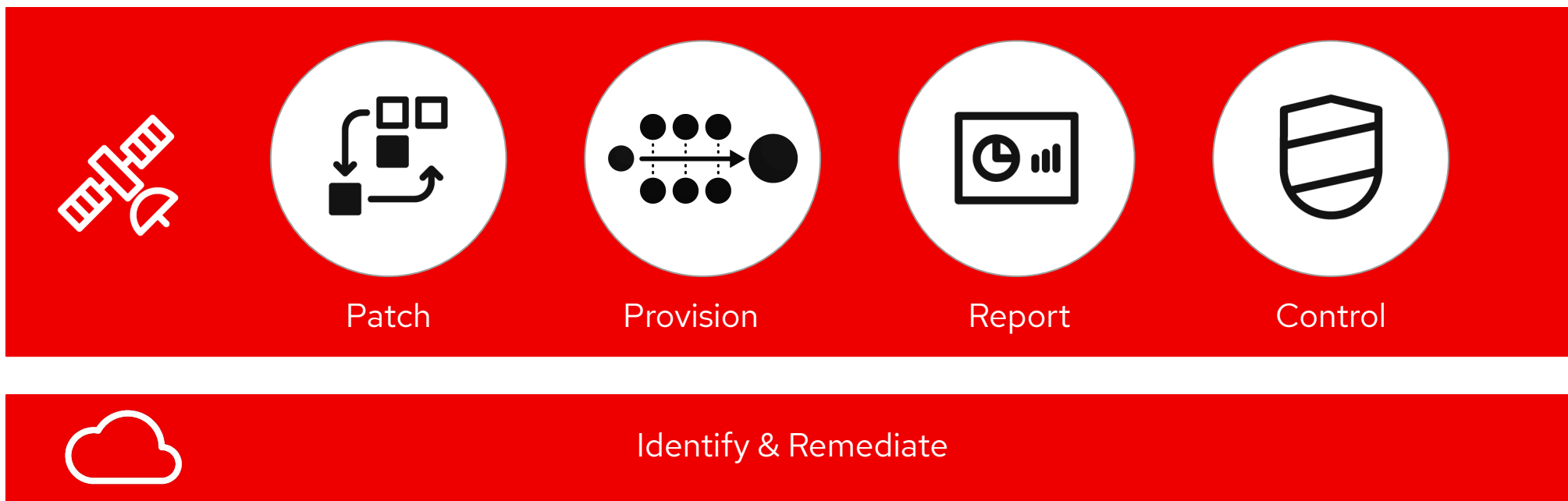


Smart Management for Red Hat Enterprise Linux

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

Improve operational efficiency by 28%*

Overcome scale, skill, and security gaps



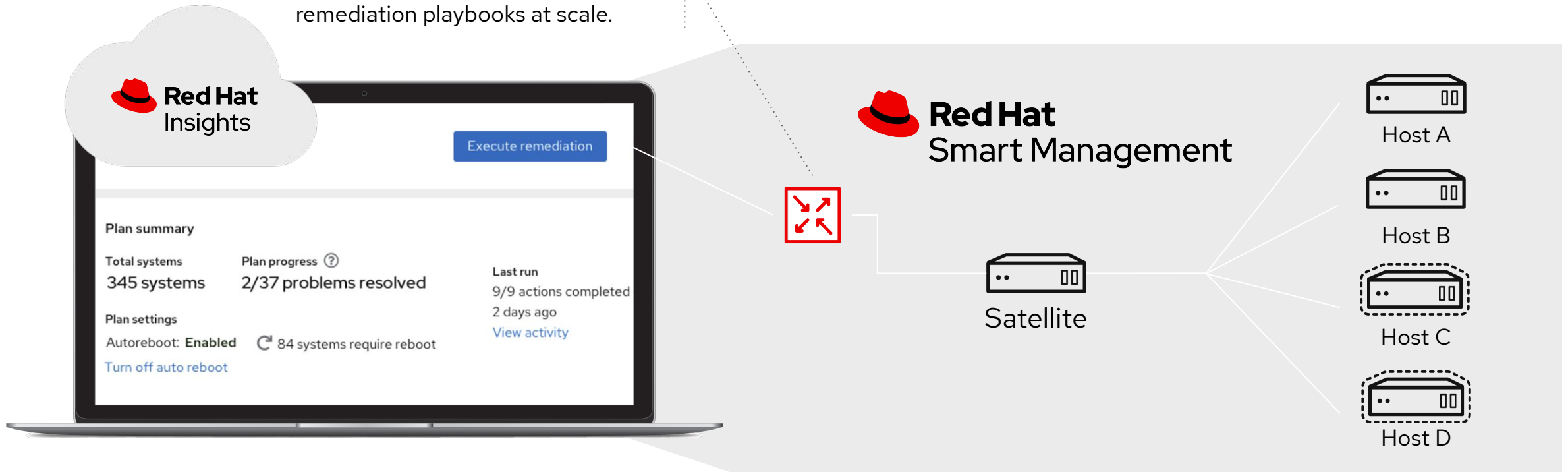
*Source: Satellite IDC Business Value Whitepaper - redhat.com/business-value-satellite

Insights and Smart Management

Smart Management subscription enables push-button remediation of issues identified by Insights.

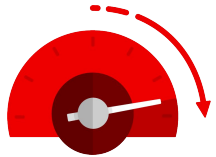
Cloud Connector

Connects your Satellite infrastructure to Insights to execute remediation playbooks at scale.



Insights Use Cases

Key use cases



Uptime and efficiency

- Manage more with fewer admins
- Move to a managed service provider
- Consolidate operations teams



Security

- Keep up with vulnerabilities
- Harden infrastructure proactively
- Reduce unreasonable demands from security teams

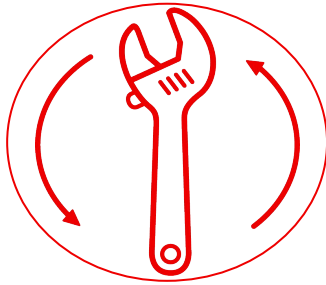
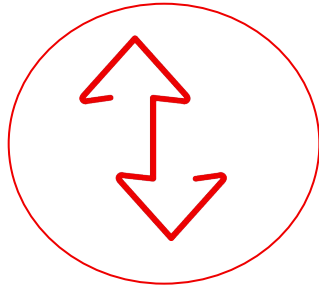
Insights combines with other tools to enhance the Red Hat Enterprise Linux investment.

Insights + technical account manager (TAM) encourages deeper customer conversations and delivers regular assessments.

Insights + Satellite identifies and prioritizes risks and patches so customers can resolve issues faster

Operational efficiency management

Putting Insights into action



**CONFIGURATION
ASSESSMENT**

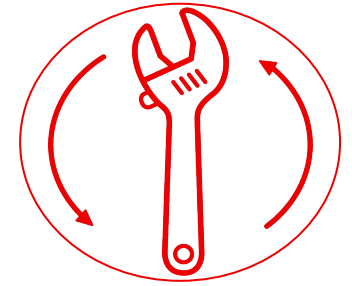
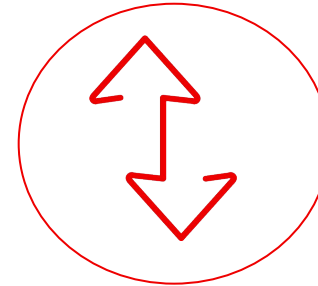
**RISK
IDENTIFICATION**

**CONTINUOUS
INSIGHTS**

**REMEDICATION
PLAN**

Security and Compliance Risk Management

Value for Customers



**INTEGRATED
MANAGEMENT**

**PROACTIVE
GUIDANCE**

**CONTINUOUS
INSIGHTS**

**REMEDIA
TION
PLAN**

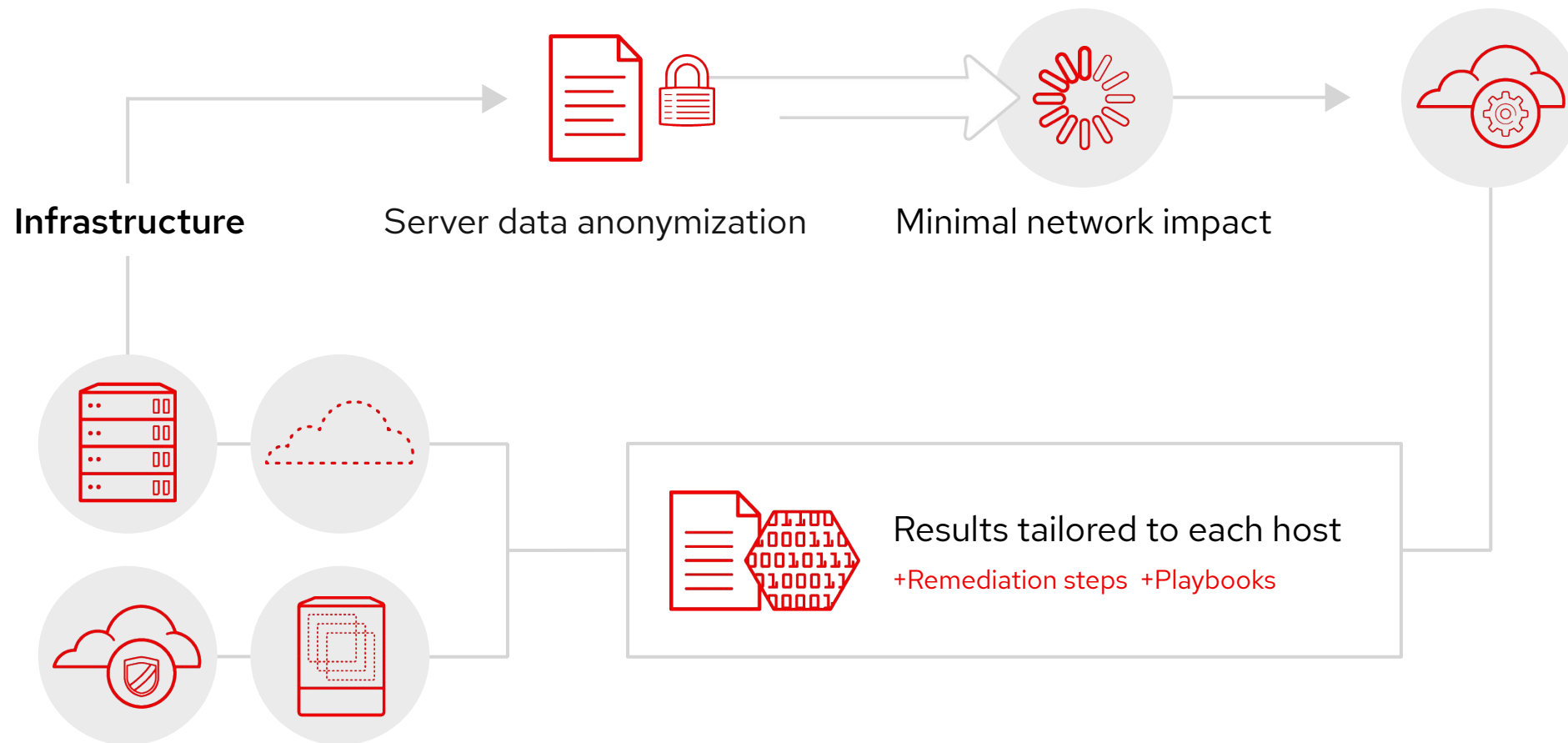
Customer Stories

- 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?
- Insights identified a misconfigured network bond, but the customer didn't use bonding. It was **accidentally enabled on a production server**. Insights was able to easily fix a problem then customer didn't even know they had!
 - Is your environment is **correctly** configured? Has it drifted?

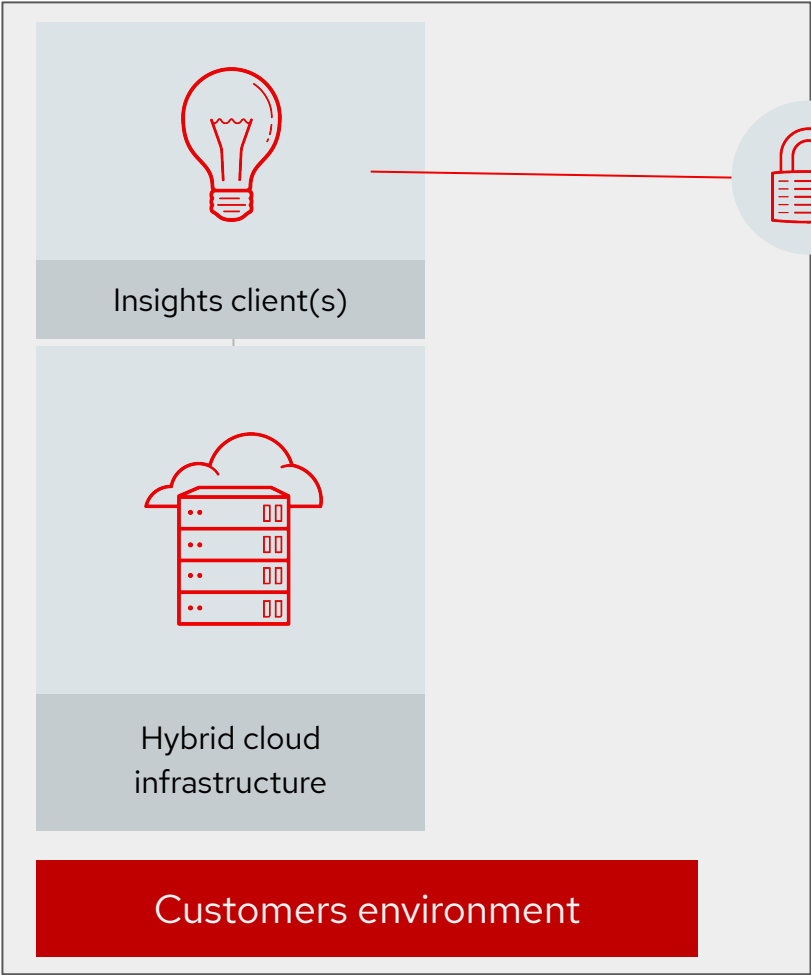
Architecture

Red Hat Insights

Insights Communication Flow



Direct Connection

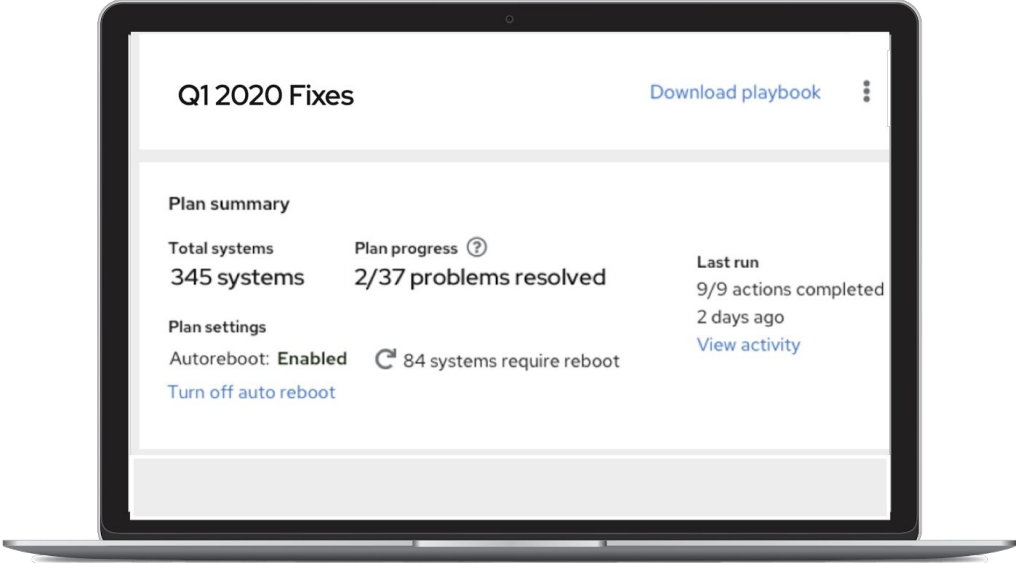


Port 443

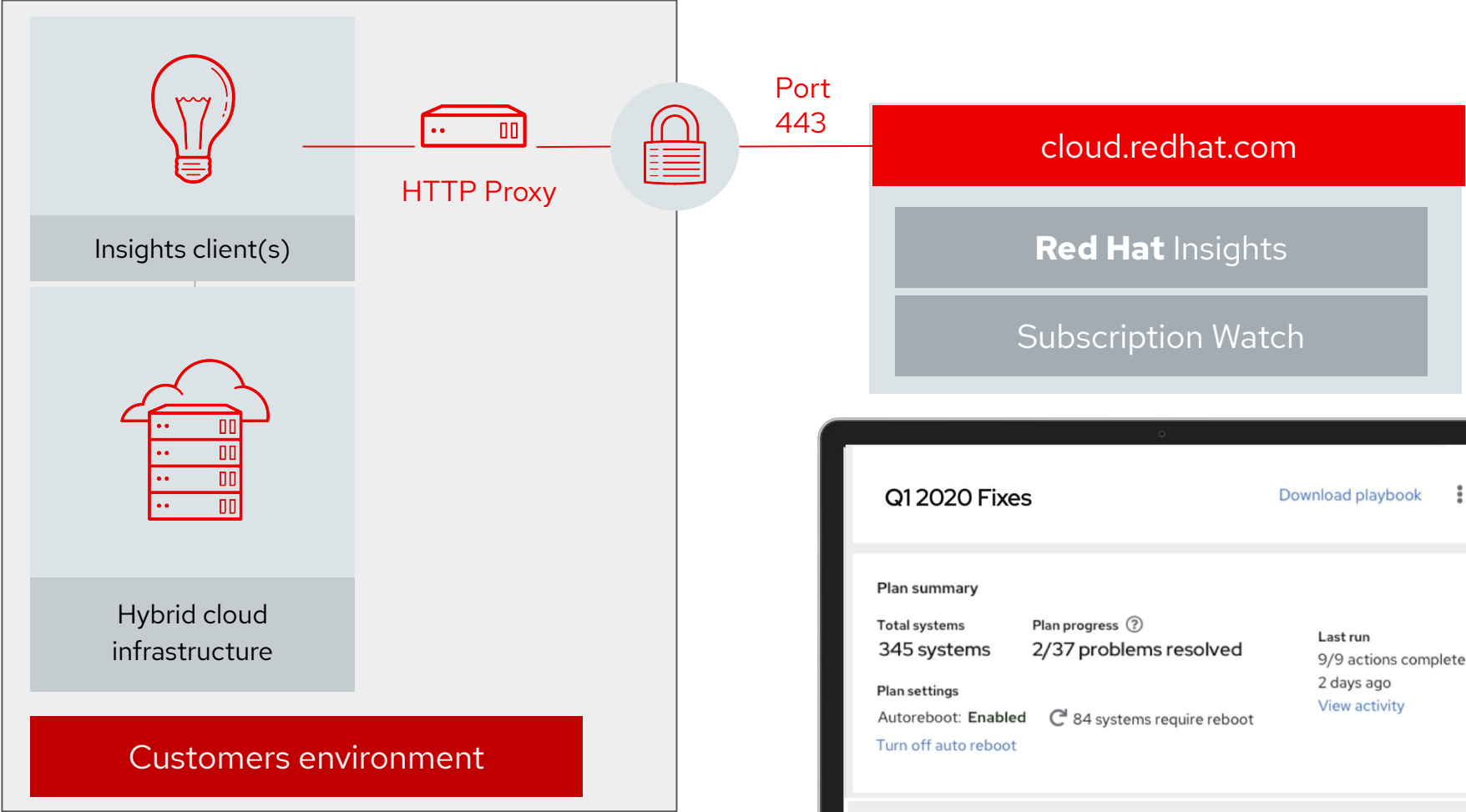
cloud.redhat.com

Red Hat Insights

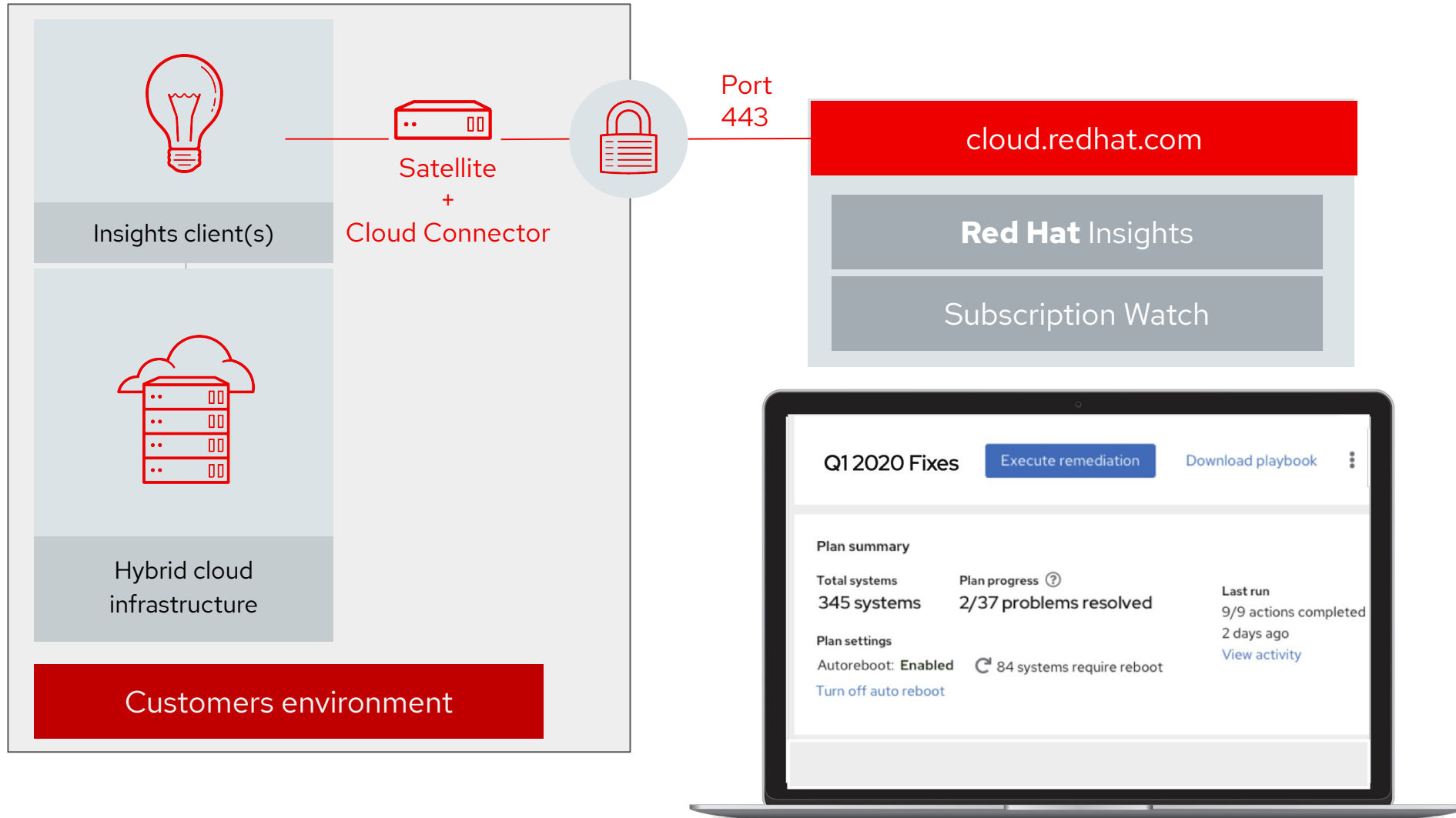
Subscription Watch



HTTP Proxy

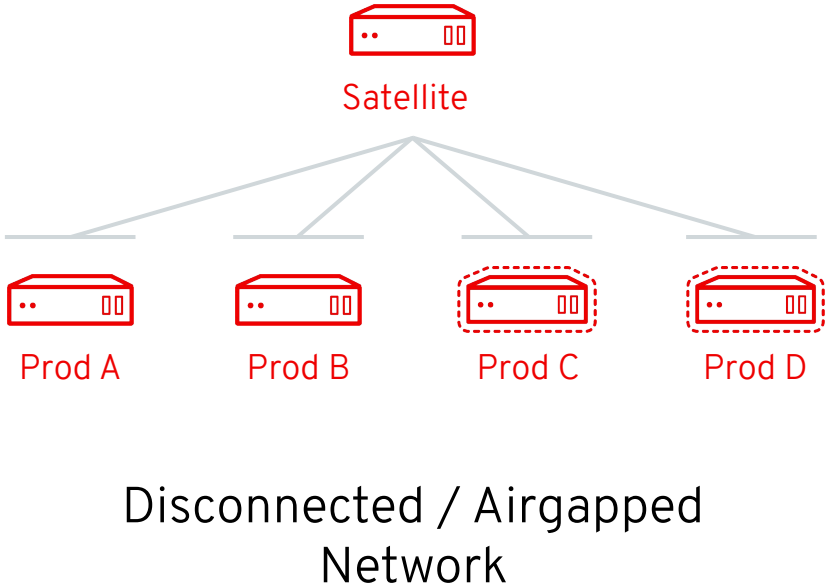
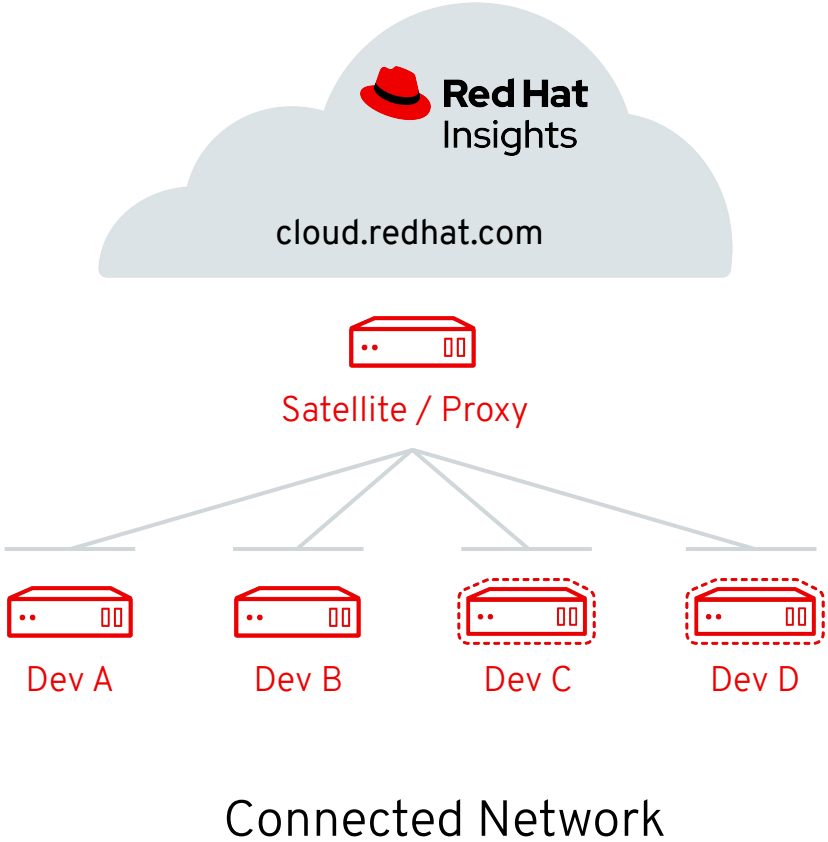


Smart Management



Insights with more Secure Environments

Connect Test/Dev environment to internet via proxy
Production remains airgapped

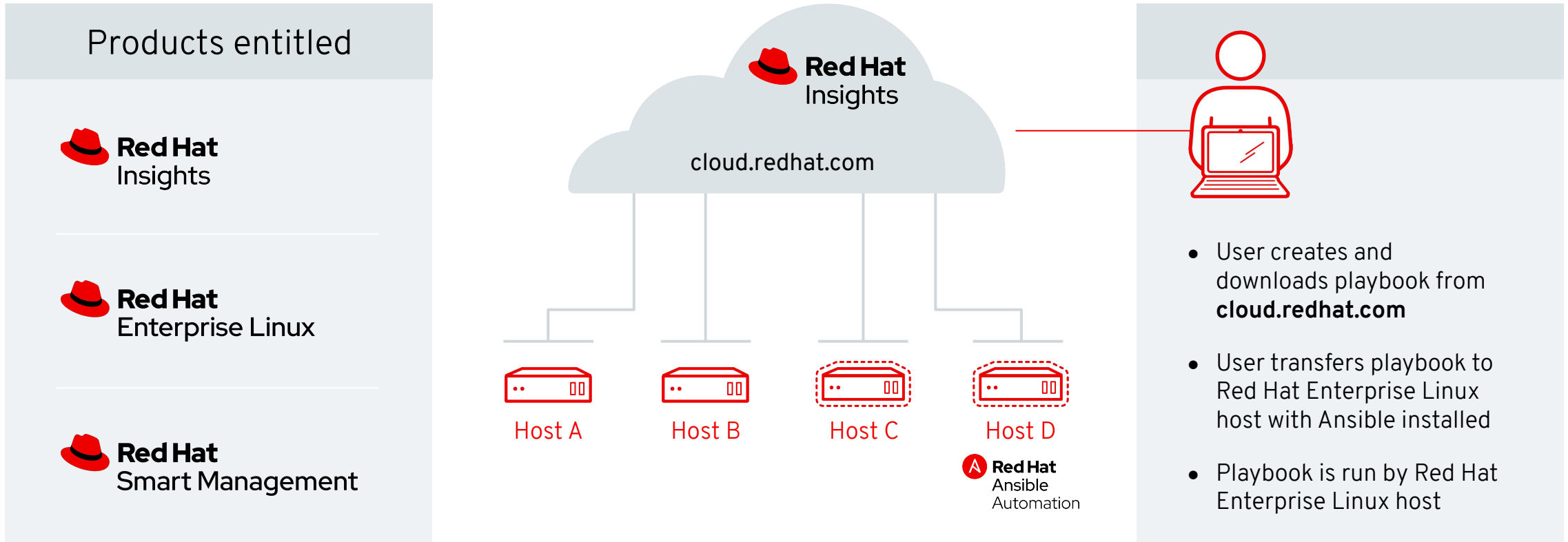


Remediation

Red Hat Insights

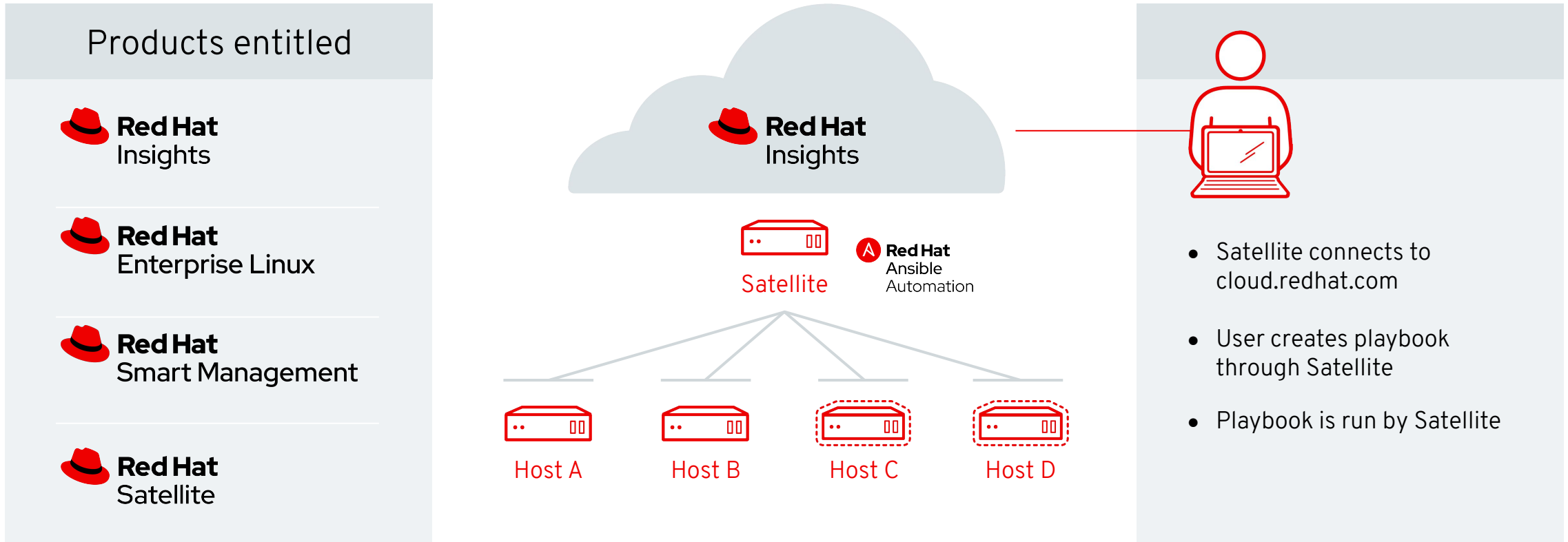
Download and run playbooks

Scenario applies to Insights and cloud management services



Build and run playbooks in Red Hat Satellite

Scenario applies to Insights only



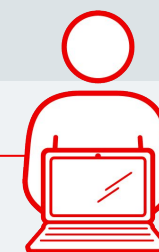
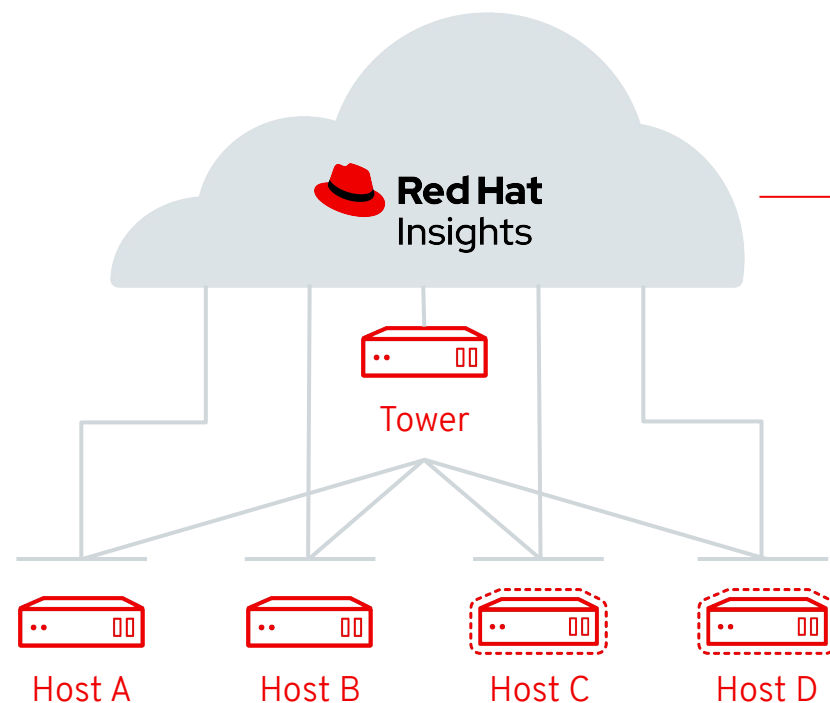
Ansible Tower + Insights Architecture

Products entitled

 **Red Hat**
Insights

 **Red Hat**
Enterprise Linux

 **Red Hat**
Ansible
Tower



- Hosts are directly connected to `cloud.redhat.com`
- User creates playbook through Ansible Tower
- Playbook is run by Ansible Tower

How to configure Red Hat Insights

Installation and registration

Simple and Straightforward



- Step #1: Run (as root) # `yum install insights-client`
- Red Hat Enterprise Linux 8 customers will not need to perform this step - the Insights client is pre-installed.

Step #2: Run (as root) # `insights-client --register`

More information including automation playbooks are available at:

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

Man page available via `$ man insights-client`

Done

us

Help!

Authentication Account Activation Key

User name

Password

Purpose Set System Purpose

Role Red Hat Enterprise Linux Server

SLA Premium

Usage Production

Insights Connect to Red Hat Insights

Options

Not registered.

Register

Anaconda Installation

Connecting to Insights is an installation option.

localhost.localdomain

Search

Networking

Podman Containers

Accounts


Services

Applications

Diagnostic Reports

Kernel Dump


SELinux

Software Updates 

Subscriptions

Terminal

Register System

URL Proxy I would like to connect via an HTTP proxy.Login Password Activation Key Organization Insights Connect this system to [Red Hat Insights](#) .

Cancel

Register



Registration Assistant

Your guide to registering your Red Hat Enterprise Linux systems.



89

To get started, please select the version of Red Hat Enterprise Linux you are trying to register. Once you've selected the appropriate major and minor versions for your systems, the Registration Assistant will provide you with instructions to register your systems via any channel available for your chosen release.

Version

Red Hat Enterprise Linux 8 - All Versions

Red Hat Insights

WHAT IS RED HAT INSIGHTS?

Red Hat Insights is a proactive management solution in Red Hat Enterprise Linux (RHEL) subscriptions. It helps you identify, prioritize, and resolve risks to your infrastructure before they become urgent issues. Insights provides ongoing analysis by using a growing list of 1,000+ rules based on Red Hat's extensive knowledge of RHEL. Delivered as-a-service, it is a single tool for managing complex RHEL environments whether they are on-premise or in the cloud. Visit the [Red Hat Insights](#) page to learn more.

Register your systems to Red Hat Insights.

Data collection

No sensitive data targeted for collection

Example files

```
/etc/redhat-release  
/proc/meminfo  
/var/log/messages  
/boot/grub/grub.conf  
/boot/grub2/grub.cfg  
/etc/modprobe.conf
```

Commands

```
/bin/rpm -qa  
/bin/uname -a  
/usr/sbin/dmidecode  
/bin/netstat -i  
/bin/ps auxcww
```

We do not collect log files, but we collect the lines that match a potential recommendation (e.g., page allocation failure.)



Deconstructing Insights Rules



Data required

- System hostname
- Version of the RHEL kernel it's running
- Confirm it's one of those specified CPUs
- Identify how long the the system has been up



How it is collected

- /bin/hostname -A
- /bin/uname -a
- /proc/cpuinfo
- /sys/devices/system/clocksource/clocksource0/current_clocksource

Rule: Kernel panic after 200+ days of uptime on certain Xeon CPUs

Description: Intel Xeon P5, P5 v2, and P7 v2 CPUs running certain Red Hat Enterprise Linux kernels are susceptible to a bug that can lead to a system panic based on accumulated uptime.

Rule on Insights:

https://cloud.redhat.com/insights/rules/tsc_xeon_reboot_uptime|TSC_XEON_REBOOT_UPTIME

Four things you should know about data collection in Red Hat Insights



- 1 Only portions of logs are collected.**
Bits of information about server configuration, recommendation match to the line of a log file.
- 2 Data uploads are customizable.**
For example, you can delete server names or IP addresses. Collection schedules are also customizable.
- 3 Information is encrypted.**
From the client's servers through transmission to the Insights service.
- 4 Data remains for a short period of time.**
Daily replace of server upload. If upload is not sent, the current upload is typically deleted after 14 days.

How long does Red Hat store data?

Typically 24 hours

Typically 2 weeks maximum*

No permanent data storage



*Some services aggregate information and keep longer to show historical trending

Common concerns, answered

I can't use Software-as-a-Service (SaaS).

Many times we find that SaaS is already being used. Services like Salesforce, ServiceNow, and New Relic are often deployed as SaaS.

We can't share our data or what data is collected.

Data collection is <1% of an SoS Report, which you likely use today. You also have full control of what is collected.

Adding new firewall rules is a long, painful process or my systems don't connect to the internet.

HTTP proxies are supported, and Satellite has one built in. You may be able to use existing approved infrastructure.

Hostname / IP are sensitive, and we are concerned about sharing information about our systems.

All data is encrypted in transit AND at rest, and you can easily redact that further.

I am located in <LOCATION>, and can't use Insights.

Many regions have restrictions around citizen data storage, e.g., GDPR, but these types of laws are unrelated to the type of data Insights collects.

We don't want an agent in the background taking up resources.

Insights is a client that runs during off hours, staggered, customizable time, is not constantly running. Items like cgroup constraints and timeouts, all can be configured.

Data collection customization

Commonly used configuration items

```
# Example options in this file are the defaults
# Change log level, valid options DEBUG, INFO, WARNING, ERROR, CRITICAL. Default DEBUG
#loglevel=DEBUG
# Attempt to auto configure with Satellite server
#auto_config=True
# Change authentication method, valid options BASIC, CERT. Default BASIC
#authmethod=BASIC
# username to use when authmethod is BASIC
#username=
# password to use when authmethod is BASIC
#password=
#base_url=cert-api.access.redhat.com:443/r/insights
# URL for your proxy. Example: http://user:pass@192.168.100.50:8080
#proxy=
# Automatically update the dynamic configuration
#auto_update=True
# Obfuscate IP addresses
#obfuscate=False
# Obfuscate hostname. Requires obfuscate=True.
#obfuscate_hostname=False
```

/etc/insights-client/insights-client.conf

- Change log level
- Configure satellite server
- Change auth level
- Configure proxy settings
- Hide IP address
- Hide hostname
- Change display name
- Eliminate timeouts

Demo

Common Questions

Four ways Red Hat Insights can help me manage my Linux environment

1

Where is my inventory?

Insights has a **single unified inventory** to centralize all registered systems.

2

What kinds of risks does Insights identify?

Each Insights service focuses on a different type of risk.

These could be CVEs, compliance issues, systems in need of patches, or Red Hat recommendations for availability or performance

3

How do I fix issues that Insights find?

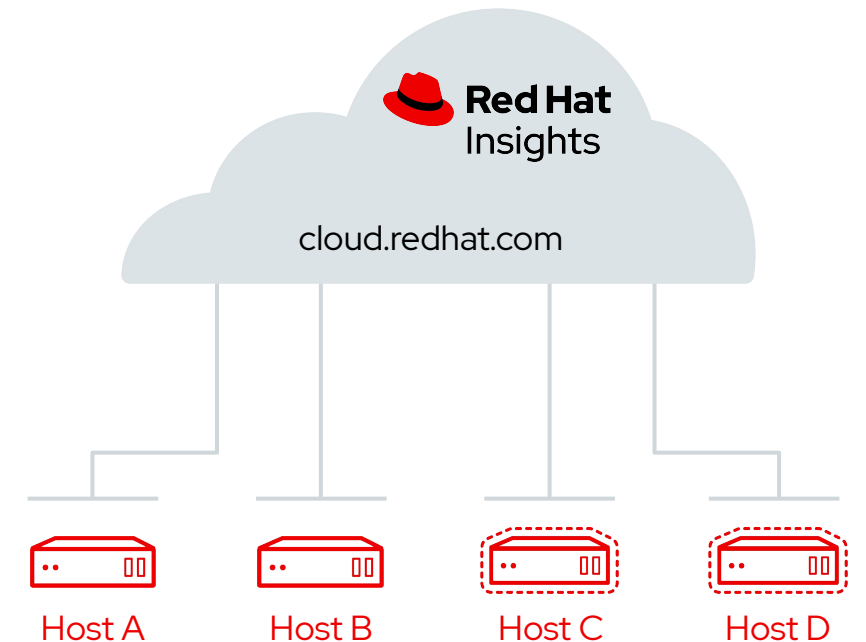
Most services provide **remediation** in the form of step-by-step instructions and in many cases an Ansible playbook.

Download the playbook and run it with Ansible Automation Platform

4

How do I fix issues that Insights finds at scale?

With **Red Hat Smart Management**, you can use the combination of Red Hat Satellite and cloud connector to enable an **“Execute Remediation”** button and run remediation playbooks from Insights.



Top 3 Insights Concerns

I can't use Software-as-a-Service (SaaS).

Often we find that SaaS is already being used.

Services like Salesforce, ServiceNow, and New Relic are often deployed as SaaS.

Hostname / IP are sensitive, and we are concerned about sharing information about our systems.

All data is encrypted in transit AND at rest, and you can easily redact that further.

I am located in <LOCATION>, and can't use Insights.

Many regions have restrictions around citizen data storage, e.g., GDPR, but these types of laws are unrelated to the type of data Insights collects.

Top 3 Insights Data Collection Concerns

At a high level, what information does Insights collect?

Red Hat Insights Security Information article:

<https://red.ht/2V6doqq>

How can my Security team review the actual Insights collection?

Generate a collection and inspect it in detail. Follow instructions in this article:

System Information Collected by Red Hat Insights

<https://red.ht/2yPIWsH>

How can I redact information from the Insights collection?

Opting Out of Sending Metadata from Red Hat Insights Client Knowledgebase article:

<https://red.ht/3ehAy4v>

Just worried about IP Address and hostname? See article on Obfuscating IP Addresses and Host Names in Red Hat Insights

<https://red.ht/2KebCgB>



Insights Services

Advisor

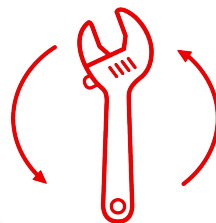
Advisor

Red Hat Recommendations based on 20+ years of supporting RHEL in areas of availability, performance, stability, and security risks.

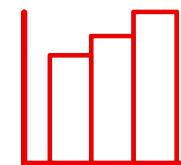
With Advisor:



Assess impact of Red Hat Recommendations on your systems



Remediate findings with prescriptive remediation steps or an Ansible playbook

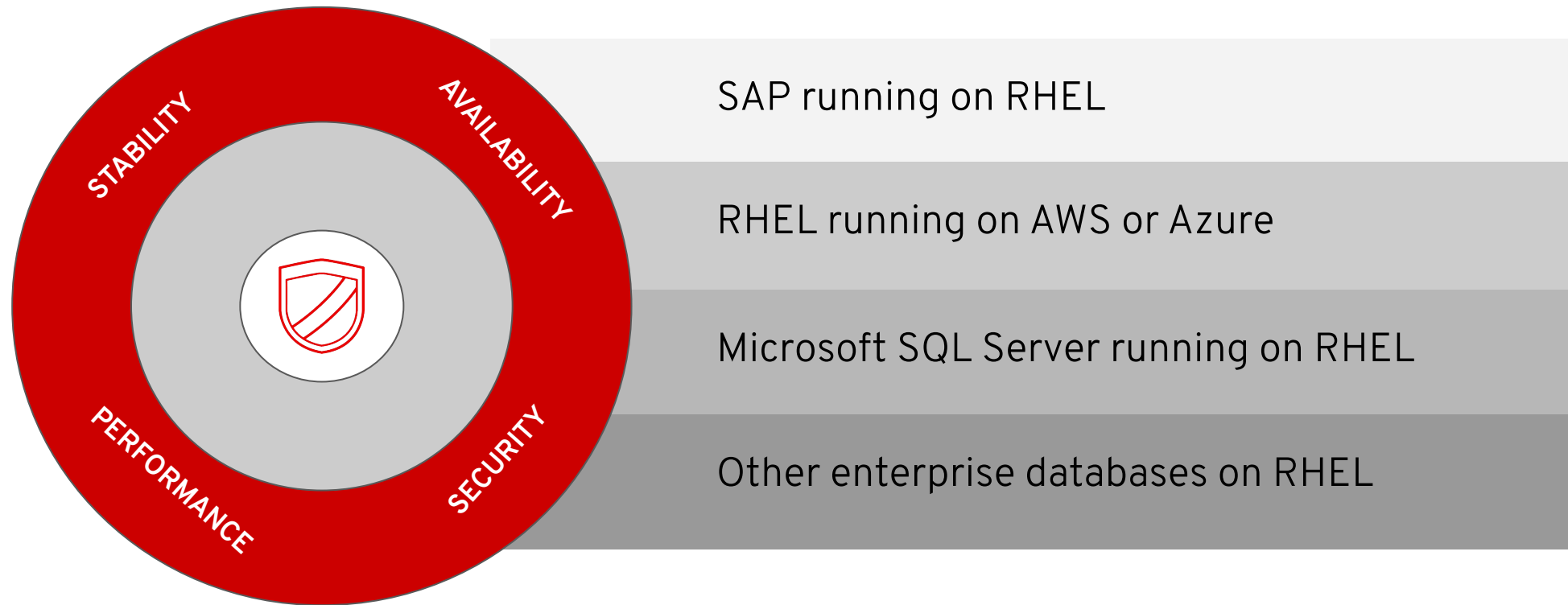


Report via JavaScript Object Notation (JSON) and Comma-Separated Values (CSV) view-based **reports** to keep relevant stakeholders informed

Reduce firefighting and focus more on strategic initiatives

Snapshot of Advisor Recommendations

The Advisor service has more than 1,100+ recommendations across several categories and workloads



Filter by tags: All systems

Recommendations

Recommendations Systems

Description Filter by description

1 - 7 of 7 1 of 1

Status Enabled Clear filters

Description	Added	Total risk	Systems	Ansible
> Database performance decreases when Transparent Huge Pages is enabled	1 year ago	Moderate	34	✓
▼ Network connections will hang when insufficient memory is allocated for the TCP packet fragmentation	7 months ago	Important	25	✓

Recommendation is disabled for 1 system. View systems

Due to a known bug in kernel, network connections hang when insufficient memory is allocated for the TCP packet fragmentation. This is a regression introduced by the fix for CVE-2019-11478.

Knowledgebase article

Total risk

Important

The likelihood that this will be a problem is Important. The impact of the problem would be Important if it occurred.

Advisor

Availability, performance, stability, and security risk analysis

Vulnerability

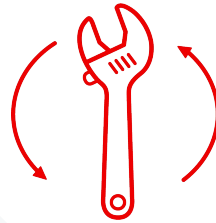
Vulnerability

Remediate all Common Vulnerabilities and Exposures (CVEs)

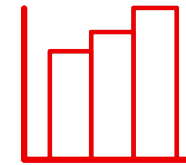
With Vulnerability:



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



Remediate known Common Vulnerabilities and Exposures (CVEs)

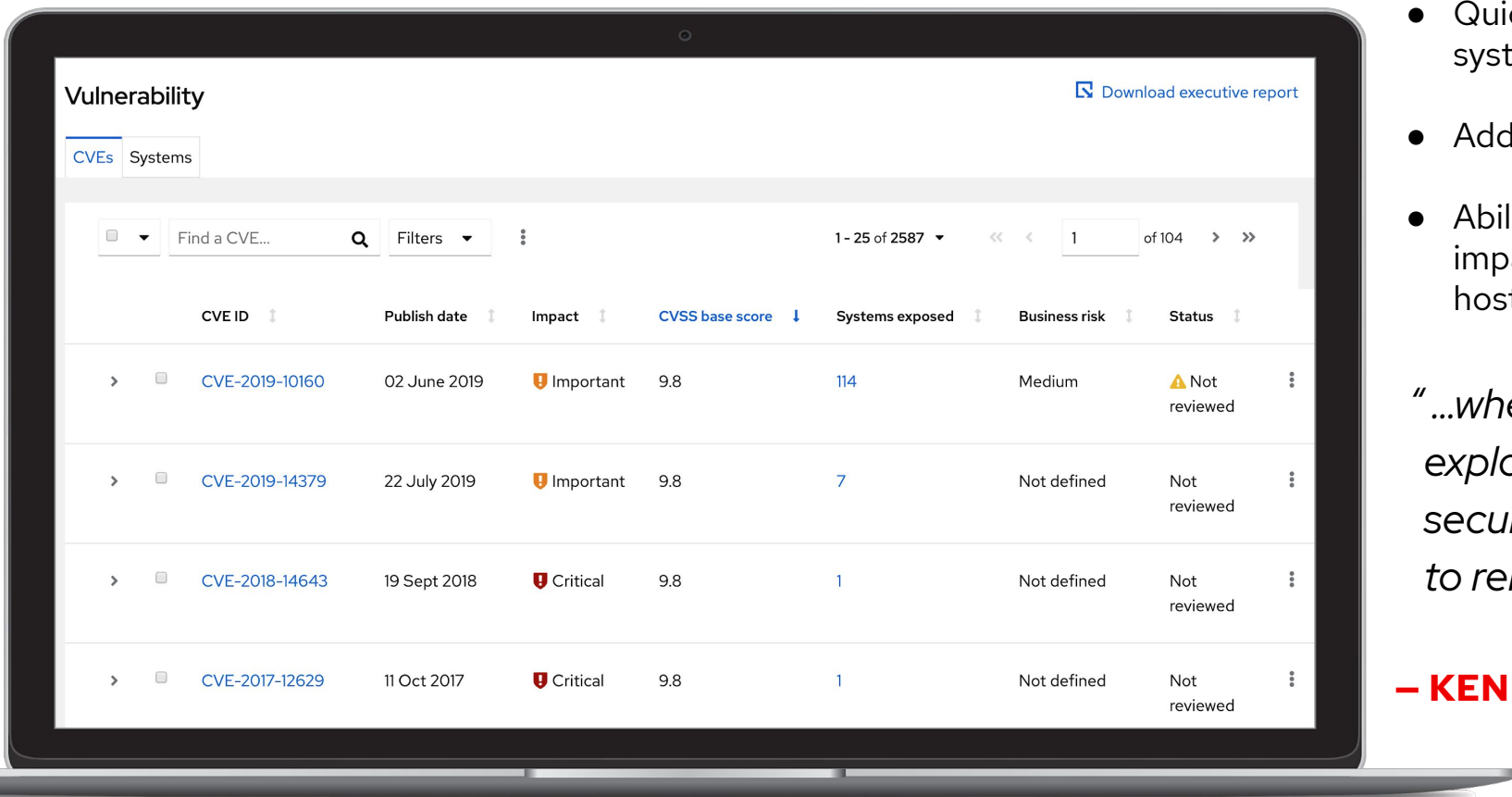


Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

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



The screenshot shows a 'Vulnerability' dashboard with a search bar and a table of CVEs. The table has the following columns: CVE ID, Publish date, Impact, CVSS base score, Systems exposed, Business risk, and Status. The data rows are as follows:

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



Vulnerability

[Download executive report](#)
[CVEs](#) [Systems](#)
 Find a CVE... 1 - 25 of 2591 1 of 104

	CVE ID ↑	Publish date ↑	Impact ↑	CVSS base score ↑	Systems exposed ↓	Business risk ↑	Status ↑
>	CVE-2019-17666	17 Oct 2019	Important	6.3	226	Low	On-hold
>	CVE-2018-3646	14 Aug 2018	Important	5.6	226	High	In-review
▼	CVE-2019-11487	21 Apr 2019	Important	7.8	211	Medium	Resolved via mitigation

Description

The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/splice.c, include/linux/mm.h, include/linux/pipe_fs_i.h, kernel/trace/trace.c, mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.

>	CVE-2019-18634	29 Jan 2020	Important	7.8	197	Not defined	Not reviewed
---	--------------------------------	-------------	-----------	-----	-----	-------------	--------------

Compliance

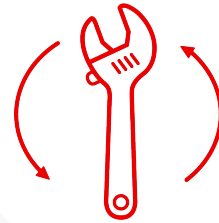
Compliance

Built on OpenSCAP reporting

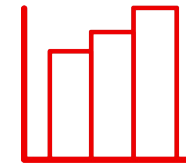
With Compliance:



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 out of compliance systems and specific rules failing

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
iks8.localdomain	Standard System Security Profile for Red Hat Enterprise Linux 7	100%
vm2.gsslab.pnq.redhat.com	Standard System Security Profile	96%
ktoardeur-sat65-tcp-haproxy-loadbalancer.sysmgmt.lan	Standard System Security Profile	92%
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

Compliance reports

By policy | By system

- 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

66%
Systems above threshold

External policy
Standard System Security Profile

1 of 2
Systems meet compliance threshold
[More details](#)

50%
Systems above threshold

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

1 of 1
Systems meet compliance threshold
[More details](#) Test

100%
Systems above threshold

What is OpenSCAP?

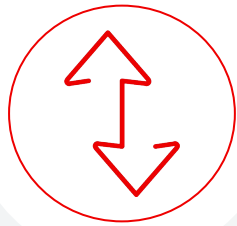
- Security Content Automation Protocol (SCAP) is a method for using a specified standard to enable automated policy compliance evaluations for systems.
- [OpenSCAP](#) is an open source implementation of the SCAP standard.
 - SCAP and OpenSCAP use security policies, also known as SCAP content, as the 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.

Drift

Drift

Create Baselines and compare system profiles

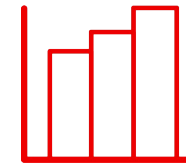
With Drift:



Create Baselines and compare system profiles and change history of one host to other hosts or to baselines.



Filter displayed profile facts, highlighting areas that match, are different, or where information is missing.



Ability to generate CSV view-based output

Set a baseline and compare systems to the baseline or to other systems to identify drift or assist in troubleshooting

Set a baseline and compare systems

System Comparison

Filter by fact View: Different Add systems or baselines 1 - 5 of 5

State Different

Fact ↓	State ↑	ic-systems 15 Jan 2020, 17:01 UTC	ic1.example.com 20 Mar 2020, 16:44 UTC	ic2.example.com 20 Mar 2020, 16:44 UTC
› yum_repos	!			
system_memory	!	3.70 GiB	3.70 GiB	994.00 MiB
› network_interfaces	!			
▼ installed_packages	!			
zlib	!	0:1.2.7-17.el7.x86_64	1.2.7-17.el7.x86_64	1.2.7-17.el7.x86_64
yum-utils	!	0:1.1.31-40.el7.noarch	1.1.31-40.el7.noarch	1.1.31-40.el7.noarch
yum-metadata-parser	!	0:1.1.4-10.el7.x86_64	1.1.4-10.el7.x86_64	1.1.4-10.el7.x86_64
yum	!	0:3.4.3-158.el7.noarch	3.4.3-158.el7.noarch	3.4.3-158.el7.noarch

- Easily create baselines
- Compare a system to a baseline
- Compare systems to other systems
- Filter on what is different, what is the same, and/or where there is not enough info

Comparison

Filter by fact

View: Different

Add systems or baselines

1 - 2 of 2

State Different

Fact ↓	State ↑	rhel8 STANDARD ★ 18 Feb 2020, 23:38 UTC	rhel8aws ☆ 27 Mar 2020, 20:55 UTC	rhel8kvm ☆ 31 Mar 2020, 20:38 UTC
os_release	!	8.1	8.0	8.2
▼ installed_packages	!			
zlib	!	1.2.11-10.el8.x86_64	1.2.11-10.el8.x86_64	1.2.11-13.el8.x86_64
yum	!	4.2.7-7.el8_1.noarch	4.0.9.2-5.el8.noarch	4.2.17-3.el8.noarch
xkeyboard-config	!	2.24-3.el8.noarch	2.24-3.el8.noarch	2.28-1.el8.noarch
xfsprogs	!	5.0.0-1.el8.x86_64	4.19.0-2.el8.x86_64	5.0.0-2.el8.x86_64
which	!	2.21-10.el8.x86_64	2.21-10.el8.x86_64	2.21-12.el8.x86_64
vim-minimal	!	8.0.1763-13.el8.x86_64	8.0.1763-10.el8.x86_64	8.0.1763-13.el8.x86_64
util-linux	!	2.32.1-17.el8.x86_64	2.32.1-8.el8.x86_64	2.32.1-17.el8.x86_64
unbound-libs	!	1.7.3-8.el8.x86_64	1.7.3-8.el8.x86_64	1.7.3-10.el8.x86_64
tzdata	!	2019c-1.el8.noarch	2019a-1.el8.noarch	2019c-1.el8.noarch

Dashboard

Advisor

Vulnerability

Compliance

Policies

Drift

Comparison

Baselines

Subscription Watch

Patch

Inventory

Remediations

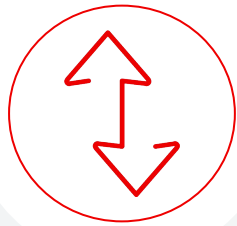
Documentation

Policies

Policies

Create Policies to identify misalignment

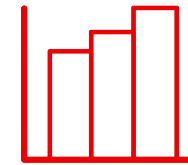
With Policies:



Create Policies to meet your custom needs, such as all hosts need a specific NTP configuration.



Analyze environment configurations and identify systems that are not aligned.



Trigger alert or action when a system does not match the policy.

Create your own custom policies to suit your organization's specific requirements

Define and monitor against your own policies to identify misalignment

Policies

- Dashboard
- Advisor >
- Vulnerability
- Compliance >
- Policies**
- Drift >
- Subscription Watch >
- Patch
- Inventory
- Remediations
- Documentation

Name Filter by name
Create policy
1 - 10 of 18

	Name	Trigger actions	Last triggered
>	<input type="checkbox"/> Ensure deprecated packages are not installed on RHEL8	✉️	✅ about 1 hour ago
>	<input type="checkbox"/> Ensure Cirrus VGA virtual GPU type is not used on Virtual Machines (deprecated)	✉️	✅ about 1 hour ago
▼	<input type="checkbox"/> Ensure libsecret is installed in place of libgnome-keyring (deprecated)	✉️	✅ about 1 hour ago

Description

The libgnome-keyring library has been deprecated in favor of the libsecret library, as libgnome-keyring is not maintained upstream, and does not follow the necessary cryptographic policies for RHEL8. The new libsecret library is the replacement that follows the necessary security standards.

Last updated 02 Apr 2020 | Created 02 Apr 2020

Conditions

```
facts.os_release > 8 and not (facts.installed_packages contains ['libsecret'] and not facts.installed_packages contains ['libgnome-keyring'])
```

Trigger actions

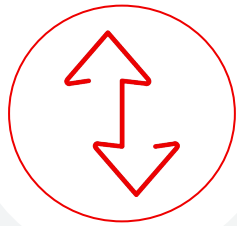
- ✉️ Send Email
- 🔗 Send to Hook

Patch

Patch

Patch systems to keep them up to date

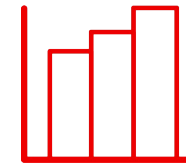
With Patch:



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

Patch

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

- Dashboard
- Advisor >
- Vulnerability
- Compliance >
- Policies
- Drift >
- Subscription Watch >
- Patch**
- Inventory
- Remediations
- Documentation

Patch

- Applicable advisories
- Systems

Search

Q

1 - 25 of 4517 < >

Name	Publish date	Type	Applicable systems	Synopsis
> RHSA-2020:0984	26 Mar 2020	Security	59	Important: ipmitool security update
> RHSA-2020:0981	26 Mar 2020	Security	1	Important: ipmitool security update
▼ RHSA-2020:0980	26 Mar 2020	Security	8	Moderate: rh-postgresql10-postgresql security update

Description

PostgreSQL is an advanced object-relational database management system (DBMS). The following packages have been upgraded to a later upstream version: rh-postgresql10-postgresql (10.12). Security Fix(es): * PostgreSQL: stack-based buffer overflow via setting a password (CVE-2019-10164) * PostgreSQL: ALTER ... DEPENDS ON EXTENSION is missing authorization checks (CVE-2020-1720) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

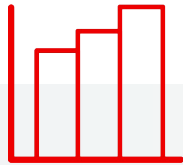
[View packages and errata at access.redhat.com](#)

Subscription Watch

Subscription Watch

Understand your subscription utilization

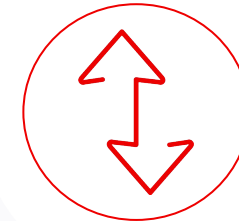
With Subscription Watch:



Account-level view of subscription utilization over time



Aggregated reporting helps your architects understand what they have and procurement understand what they're paying for..



Streamline operations four footprints, four architectures; one account and one report.

Subscription tracking and visibility to operate efficiently and confidently

Subscription Watch

Track progress of your Red Hat subscription usage efficiently and confidently

Red Hat Enterprise Linux

Filter by SLA

Red Hat Enterprise Linux

All

ARM

IBM Power

IBM Z systems

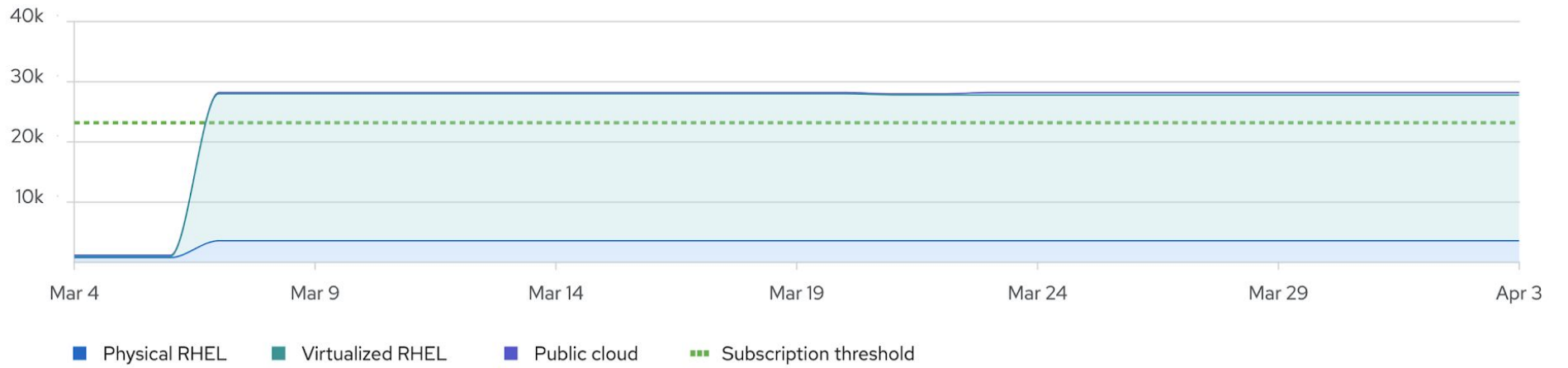
x86

Red Hat OpenShift

Documentation

CPU socket usage

Daily



Resources & Next Steps

Red Hat Insights: Additional resources and next steps

ALREADY A RED HAT® ENTERPRISE LINUX® CUSTOMER?

You have Red Hat Insights at no additional cost:

https://red.ht/insights_start

WOULD YOU LIKE TO LEARN MORE ABOUT RED HAT INSIGHTS?

<https://redhat.com/insights>

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

Watch the [intro video](#)

Read the [Insights blog](#)

Insights Resources

Webpages and Docs:

- Red Hat Insights product webpage - <https://www.redhat.com/insights>
- Get Started with Insights - <https://access.redhat.com/products/red-hat-insights/#getstarted>
- Red Hat Insights Documentation - https://access.redhat.com/documentation/en-us/red_hat_insights/1.0/
- IDC Analyst Whitepaper: value of Red Hat Insights and predictive analytics - <https://www.redhat.com/en/resources/idc-whitepaper-optimizing-infrastructure-management-with-predictive-analytics>
- Insights blog: <https://www.redhat.com/en/blog/channel/red-hat-insights>
- Red Hat Insights archived Blog Site - <https://access.redhat.com/blogs/insights>

Security Links:

- Insights Security page: <https://access.redhat.com/insights/security>
- System info collected by Insights: <https://access.redhat.com/articles/1598863>
- Opting out of Sending metadata from the Insights Client: <https://access.redhat.com/articles/2025273>

Videos:

- Introduction to Red Hat Insights Video: <https://youtu.be/MdT4xrllvpY>
- Installation and Registration of Red Hat Insights Video: <https://youtu.be/BOhQ9larUb8>
- Find it. Fix it. Before it breaks. Satellite, Insights, and Ansible: <https://youtu.be/mCBhUuxRCqA>

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://www.linkedin.com/company/red-hat)



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



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



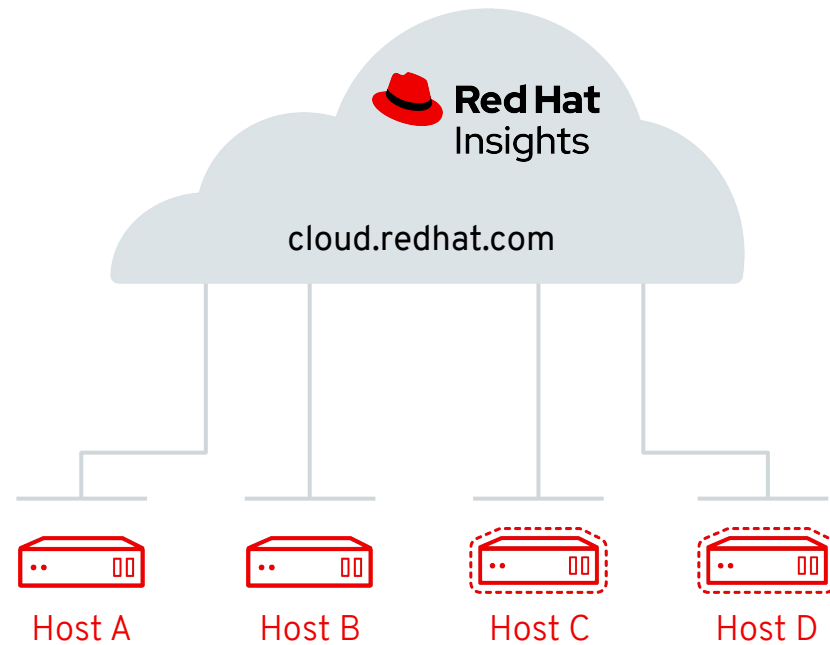
twitter.com/RedHat



Insights Client Communication Flow

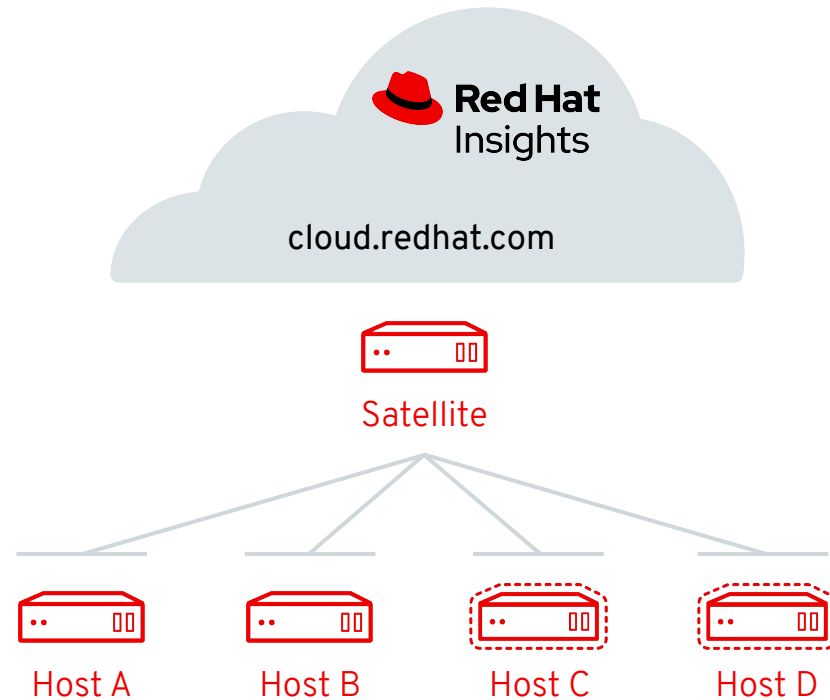
Default Insights Client behavior

Each host connects directly to cloud.redhat.com



Insights Client when connected to Satellite

Insights Client uses Satellite as a proxy
No additional config needed



Insights Client when connected to HTTP Proxy

Insights Client can be configured with HTTP Proxy

Configure a HTTP Proxy in the insights-client.conf

/etc/insights-client/
insights-client.conf

Change:

```
proxy=http://user:pass@  
192.168.100.50:8080
```

