

Red Hat
Summit

Connect

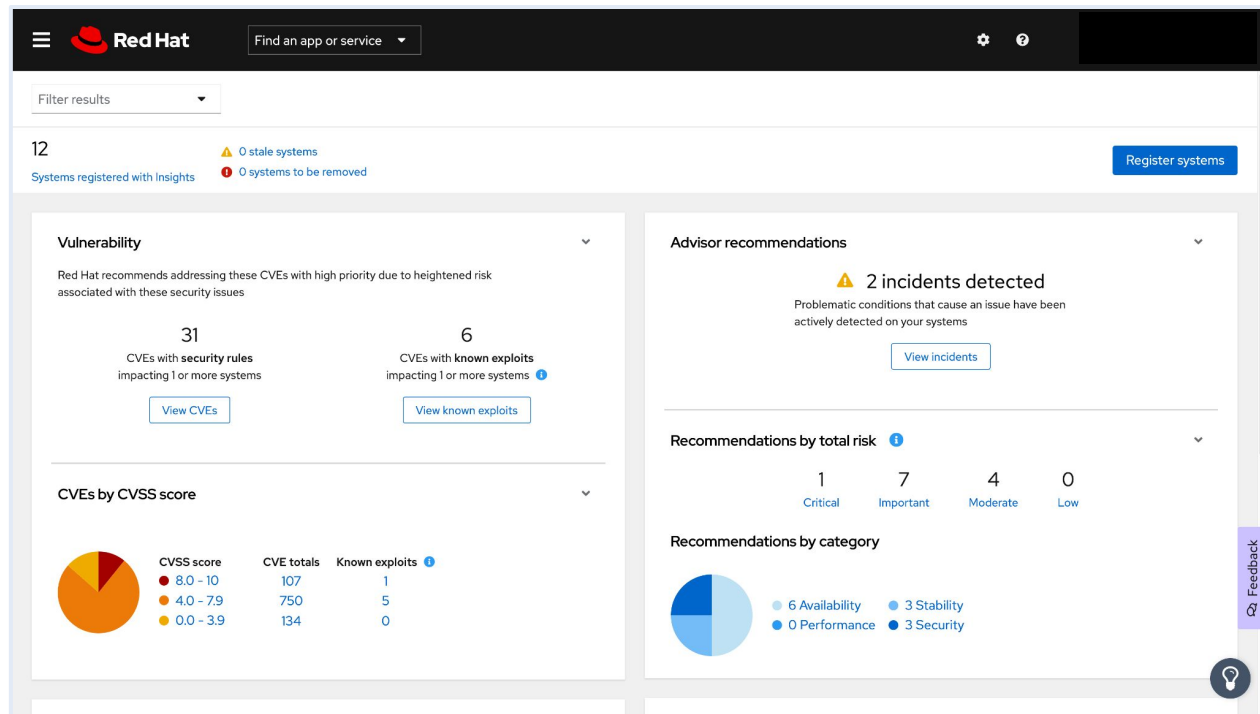
Czy na pewno nie potrzebuję
dodatkowego admina w mojej
organizacji?

Red Hat Insights.

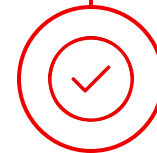
Zbigniew Parys
Senior Solution Architect

What is Red Hat Insights?

Helping you better manage your hybrid and cloud environments



Predicting risks



Recommending actions



Analyzing costs

What does Red Hat Insights do?

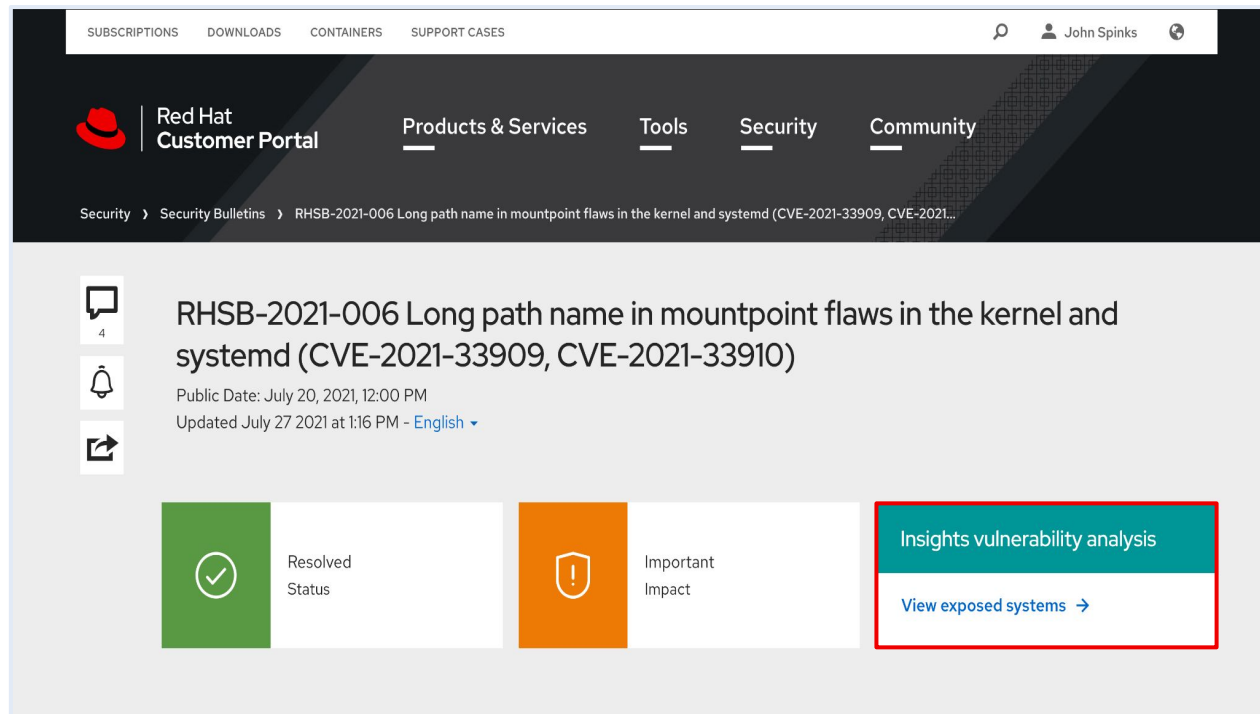
A cloud analytics platform that helps you better manage your hybrid and cloud environments



- ▶ **Gathers** configuration and utilization data from your Red Hat® products
- ▶ **Analyzes** the data based on Red Hat knowledge and expertise
- ▶ **Generates** and prioritizes insights for you to take action

How does Red Hat Insights help me?

Use Red Hat's expertise and knowledge to evaluate your systems



Red Hat subscriptions include knowledge of:



>1 Million
Customer support cases



>1,000
Red Hat support personnel



>115,000
Knowledge base and solution articles

How does Red Hat Insights help me?

Use Red Hat's expertise and knowledge to evaluate your systems



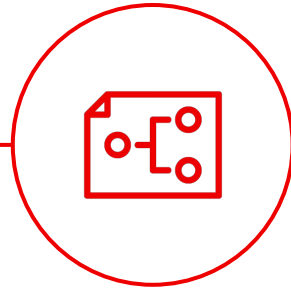
- ▶ Configuration review to make sure systems are setup correctly
- ▶ Easily identify interoperability issues from the hypervisor or cloud, through the OS, and through the application stack
- ▶ Centralized view of all CVEs, patches, and compliance risks
- ▶ Identify drift to make sure systems are the same
- ▶ Know how many subscriptions you are using in seconds

How does it benefit my business?



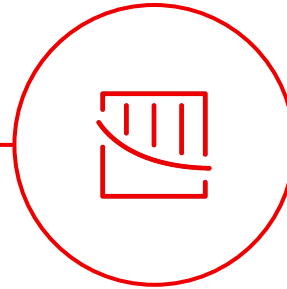
Understand

Clearly understand your security risk profile



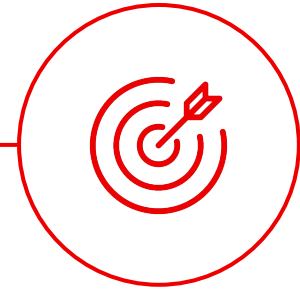
Plan

Stay ahead of critical operational issues



Reduce

Time to find and resolve issues from hours to minutes

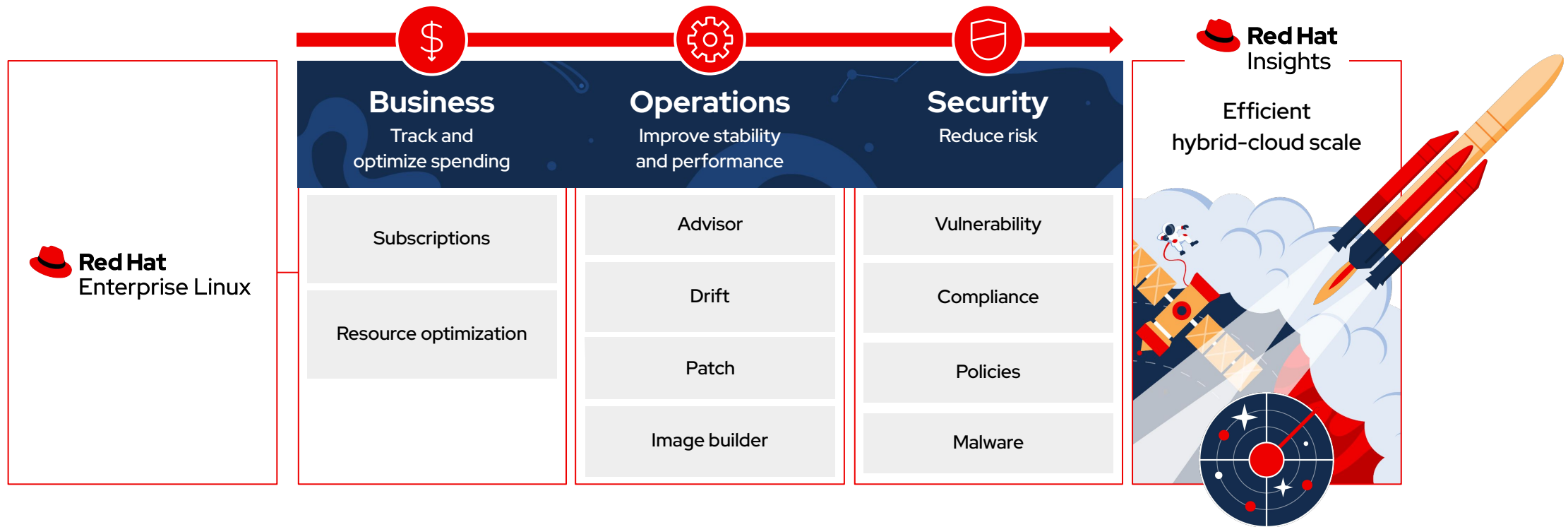


Innovate

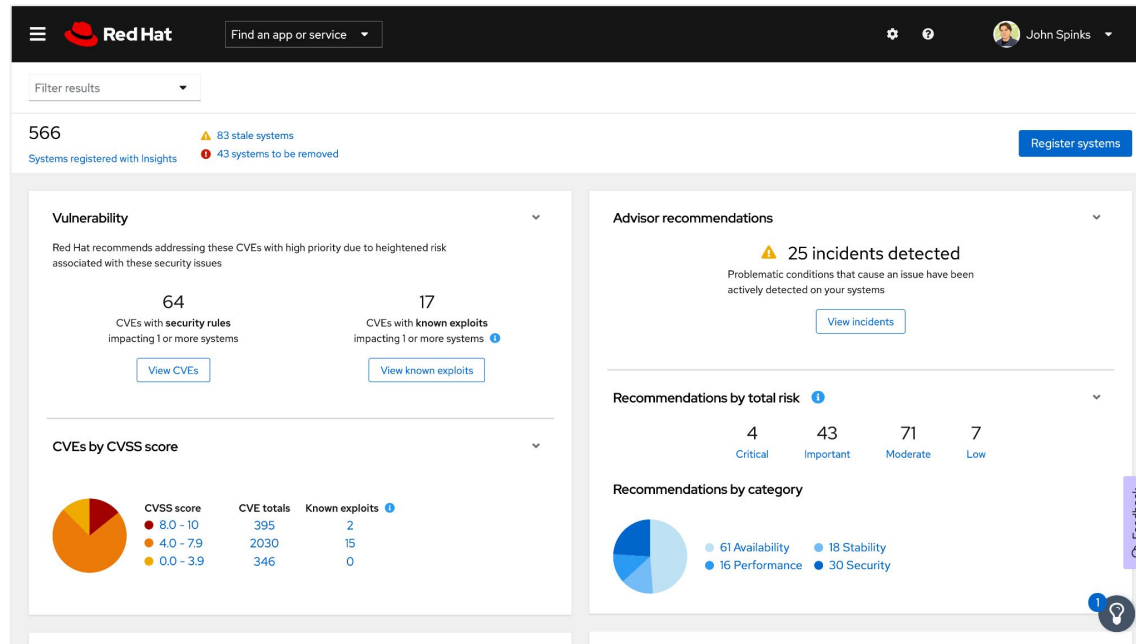
Free up resources to focus on innovation and new capabilities

Red Hat Insights for Red Hat Enterprise Linux

For all your hybrid-cloud challenges



What's New Highlights



New services:

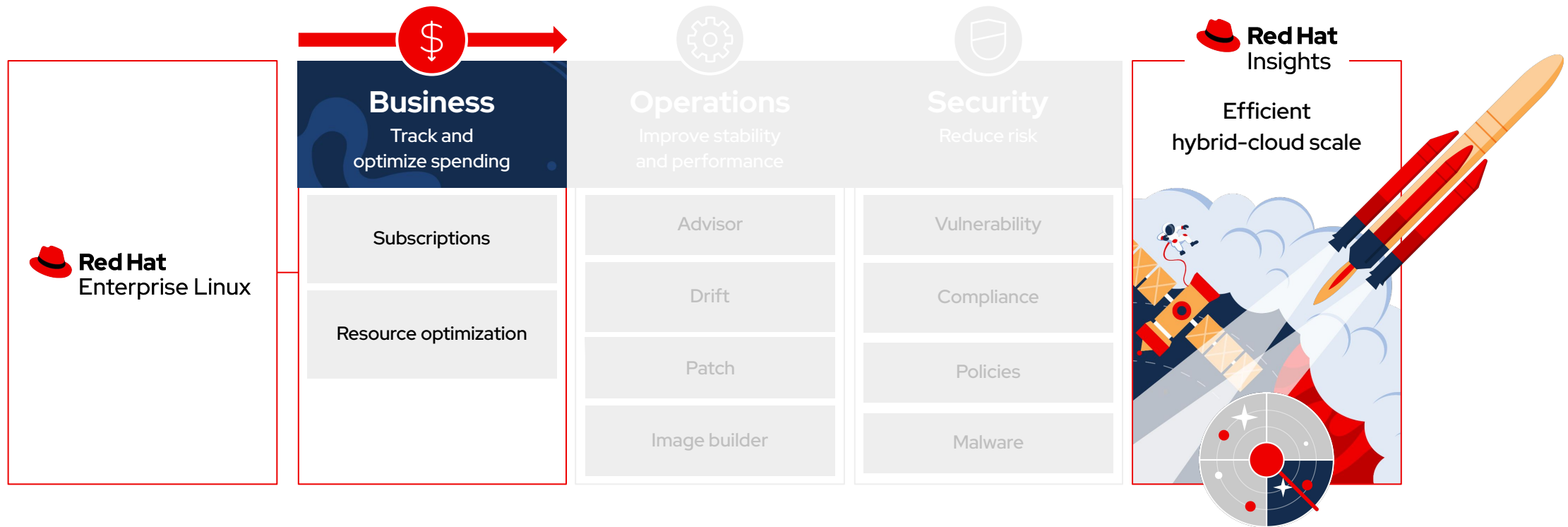
- ▶ Resource Optimization (Beta)
- ▶ Image Builder (Beta)

New Features:

- ▶ Advisor - New recommendations for Ansible automation controllers
- ▶ Advisor - expanded Microsoft SQL recommendations
- ▶ Vulnerability - Enhanced vulnerability analysis via use of OVAL feed
- ▶ ...and more!

Red Hat Insights for Red Hat Enterprise Linux

For all your hybrid-cloud challenges



Subscriptions

Simple, immediate understanding of your account wide hybrid-cloud Red Hat Enterprise Linux subscription profile

- ▶ Account level view of subscription utilization
- ▶ Aggregated host level reporting
- ▶ Where subscriptions are being consumed
 - physical, virtual, or in the public cloud (and which public cloud)

What's New!

- Current subscriptions tab
- Activation keys visible from [Red Hat connector dashboard](#)
- Data export via CSV or JSON
- Auto-registration for GCP

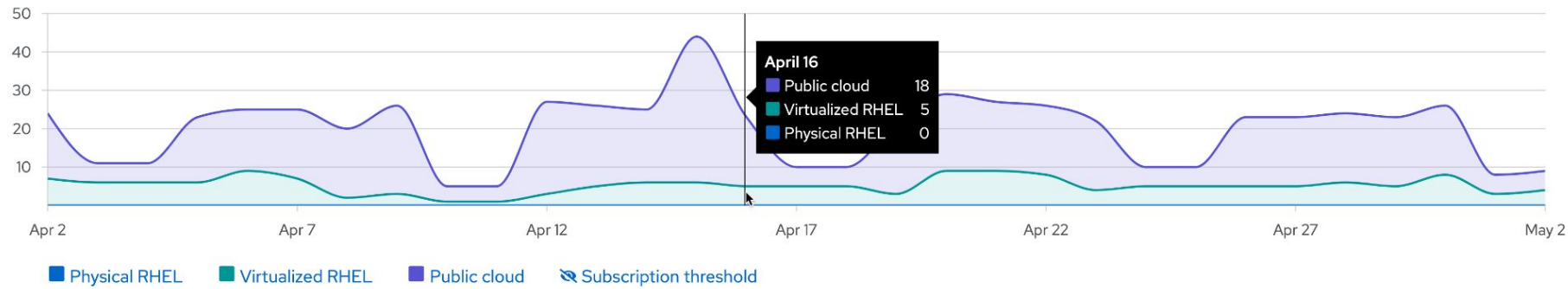
Subscriptions: Awareness of subscription utilization across your entire Red Hat Enterprise Linux estate



Business

CPU socket usage

Daily



Current systems | Current subscriptions

Filter by name

1 - 88 of 88

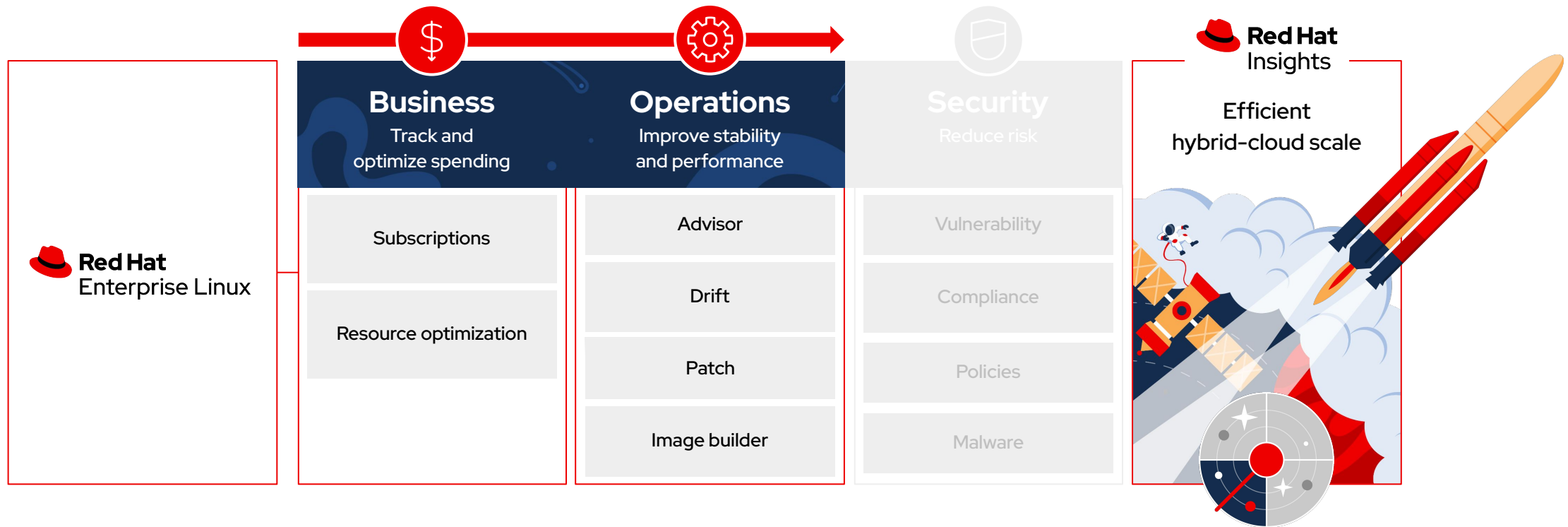
Name	Type	Subscribed sockets	Last seen
[blurred]	Public cloud AWS	1	19 hours ago
[blurred]	Public cloud AWS	1	19 hours ago
[blurred]	Virtual	1	19 hours ago
[blurred]	Public cloud AWS	1	19 hours ago
[blurred]	Public cloud AWS	1	19 hours ago
[blurred]	Virtual	1	19 hours ago

Feedback



Red Hat Insights for Red Hat Enterprise Linux

For all your hybrid-cloud challenges



Advisor

Identifies availability, performance, stability, and security risks

- ▶ Analyzes Insights data to provide recommendations
- ▶ These recommendations cover everything from the physical layer up to the application layer.
- ▶ Provides predictive findings and prescriptive information on how to resolve.
- ▶ Automate remediation via Ansible Automation playbooks

What's New!

- New topic for DB2
- Recommendation impact date
- Updated recommendation events
- Update recommendations for RHEL 9
- Export list of systems impacted by a recommendation

Advisor: Availability, performance, stability, and security risk analysis



Filter results ▼

Advisor recommendations

[Download executive report](#)

Name ▼ Filter by name

1 - 20 of 124 ◀ ▶

Systems impacted 1 or more × Status Enabled × [Reset filters](#)

Name ↑ ↓	Added ↑ ↓	Total risk ↑ ↓	Risk of change ↑ ↓	Systems ↓	Ansible ↑ ↓
> System is not able to get the latest recommendations and may miss bug fixes when the Insights Client Core egg file is outdated	4 months ago	Moderate	Low	124	✓
< Decreased security when unencrypted protocols used	8 months ago	Important	Very Low	57	No

Legacy network services are used to transmit unencrypted data. This data can be intercepted by a malicious actor.

[View 57 affected systems](#)

Total risk

Important

The total risk of this remediation is **important**, based on the combination of likelihood and impact to remediate.



Risk of change

Very Low

The risk of change is **very low**, because the change takes very little time to implement and there is minimal impact to system operations.

System reboot is **not** required.

Feedback



Patch

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

- ▶ See list of advisories and a list of systems where they need to be applied
- ▶ Look at a specific system and see what advisories are applicable
- ▶ See packages and which systems they are on as well as if an upgrade is needed
- ▶ Remediation playbooks are available to patch systems

What's New!

- Patch sets (apply same patches across multiple systems)
- Reporting against patch sets
- Updates for some 3rd party repos (RHUI, Azure, EPEL)



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

Filter results

Patch advisories

Advisory Filter by name or syn... Remediate 1 - 20 of 1213

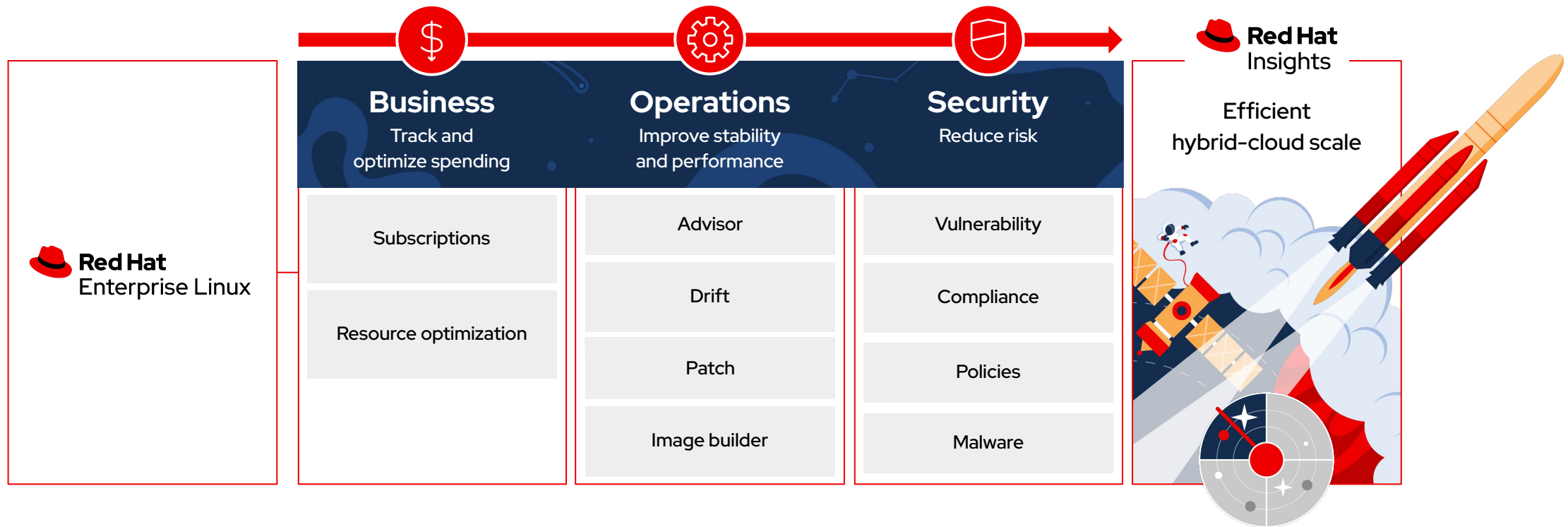
Name	Synopsis	Type	Applicable systems	Publish date
<input type="checkbox"/> RHBA-2021:2590	cloud-init bug fix and enhancement update	Bugfix	10	29 June 2021
<input type="checkbox"/> RHBA-2021:2586	rsyslog bug fix and enhancement update	Bugfix	10	29 June 2021
<input checked="" type="checkbox"/> RHBA-2021:2581	openldap bug fix and enhancement update	Bugfix	10	29 June 2021
Description OpenLDAP is an open-source suite of Lightweight Directory Access Protocol(LDAP) applications and development tools. LDAP is a set of protocols used to access and maintain distributed directory information services over an IP network. The openldap packages contain configuration files, libraries, and documentation for OpenLDAP. Bug Fix(es) and Enhancement(s): * got undefined symbol: EVP_md2, version OPENSSL_1_1_0 after upgrading from openldap-2.4.46-11 to openldap-2.4.46-15 (BZ#1972742) View packages and errata at access.redhat.com				
<input type="checkbox"/> RHBA-2021:2577	subscription-manager bug fix and enhancement update	Bugfix	10	29 June 2021
<input type="checkbox"/> RHBA-2021:2576	NetworkManager bug fix and enhancement update	Bugfix	10	29 June 2021
<input type="checkbox"/> RHSA-2021:2575	Moderate: lz4 security update	Security	10	29 June 2021
<input type="checkbox"/> RHSA-2021:2574	Moderate: rpm security update	Security	10	29 June 2021

Feedback



Red Hat Insights for Red Hat Enterprise Linux

For all your hybrid-cloud challenges



Vulnerability

Remediate common vulnerabilities and exposures (CVEs)

- ▶ Triage, prioritize, and remediate CVEs that impact your registered systems
- ▶ Threat intelligence
 - CVEs with known public exploits
 - Deep threat intelligence on specific high-profile branded CVEs
- ▶ Customize and triage CVEs based on your company's definitions of risk
- ▶ Customized reporting with the right dataset based on stakeholder profile
- ▶ Automate remediation via Ansible Automation playbooks for vulnerabilities

What's New!

- Deep threat intelligence through known exploit feature
- Expose threat intelligence through security rules
- Enhanced vulnerability analysis via use of OVAL feed
- Filtering by RHEL version
- RBAC improvements
- Tag and OS filtering on reports

Vulnerability: Remediate all common vulnerabilities and exposures (CVEs)



Filter results ▾

CVEs

▾ **Known exploit** ▾ Filter by Known exploit ▾ 1-17 of 17 ▾ < >

Systems exposed 1 or more ✕ Known exploit Has a known exploit ✕ [Clear filters](#)

CVE ID	Publish date	Severity	CVSS base score	Systems exposed	Business risk	Status	
<input type="checkbox"/> CVE-2021-3156 Known exploit Security rule	26 Jan 2021	Important	7.8	87	Not defined	Not reviewed	
<input checked="" type="checkbox"/> CVE-2020-9850 Known exploit	09 July 2020	Moderate	9.8	20	Not defined	Not reviewed	
<p>CVE description</p> <p>A logic issue was found in webkitgtk that affected WebKitGTK versions before 2.28.3 and WPE WebKit versions before 2.28.3. This flaw allows a remote attacker to cause arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.</p> <p>View more information about this CVE</p>							
<input type="checkbox"/> CVE-2019-13272 Known exploit Security rule	15 July 2019	Important	7.8	3	Not defined	Not reviewed	
<input type="checkbox"/> CVE-2019-9213 Known exploit	26 Feb 2019	Important	5.5	3	Not defined	Not reviewed	

Feedback

BETA Service: Malware

Pattern matching malware scanner


- ▶ Leverages YARA, a popular malware detection tool
- ▶ Developed along with IBM's X-Force Incident Response and Threat Intelligence Services



Malware: Pattern matching malware scanner

Filter by status ▾

Malware detection



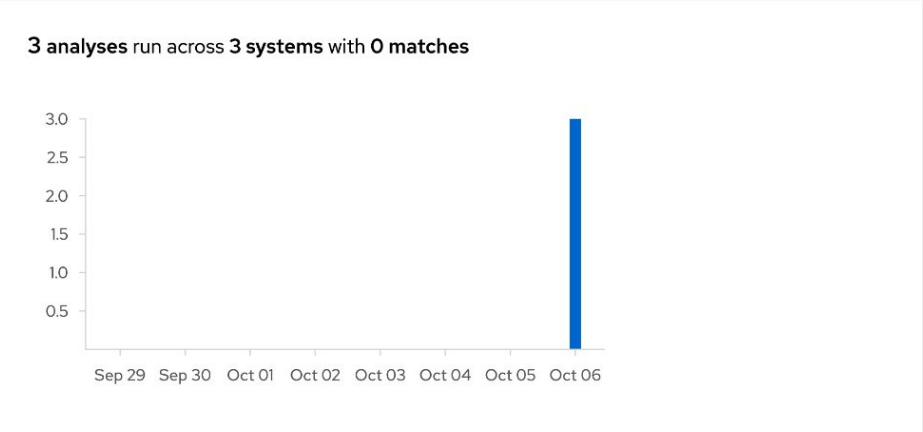
No active malware matches found

Last check: 07 Oct 2021

0
Matched signatures

114
Enabled signatures

0
Disabled signatures



Signature ▾ Filter by signature 🔍

1 - 10 of 114 < >

Signature name ↑	Last status ↑	Systems ↑	Matched ↓
> XFTI_Defray911_Linux_Ransomware	Not matched	0	Never
> XFTI_Defray911_Loader	Not matched	0	Never

Feedback



Four things you should know about data collection in Insights



You control what data is sent

You have granular controls over the data you send. In addition to automatically removing sensitive data, you can also filter by file, command, or string.

Personally identifiable information is not targeted

Insights does not target Personally Identifiable Information (PII) and adheres to Red Hat policies and guidelines aligned to the European Union's General Data Protection Regulation (GDPR).

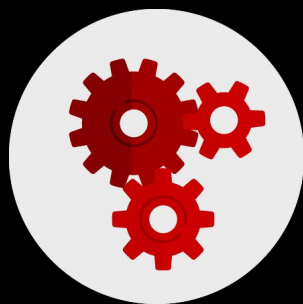
Raw log files are not collected.

Bits of information about server configuration, rule match to the line of a log file.

All Information is encrypted!

From the time collected on the client server to transmission to the Insights service.

Deconstructing what Insights collects



Data required

- System hostname
- Version of the RHEL kernel it's running
- Confirm it's one of those specified CPUs
- Determine system uptime
- Determine the clock source



How it is collected

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

Advisor Recommendation:

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.

Link on Insights:

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

See EXACTLY what Insights collects – without sending to Red Hat

insights-client --no-upload

```
# insights-client --no-upload
```

```
Starting to collect Insights data for <host>
```

```
Archive saved at /var/tmp/dfbbfuuy/insights-<host>-<date/time>.tar.gz
```

- ▶ Collection file size on RHEL8 host above: **158 kb**

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.

Demo

Red Hat
Summit

Connect

Thank you



[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