Automating Security & Compliance for Red Hat Hybrid Environments
TODAY’S PRESENTERS

John Spinks
Senior Principal Technical Marketing Manager

Mohit Goyal
Senior Principal Product Manager
WHAT WE’RE TALKING ABOUT TODAY

Security Trends and Challenges

Red Hat Insights for Security and Compliance Use Case

Demo

Q & A
The challenge

Stay ahead of threats across a dynamic IT environment with the same resources

- **Infrastructure growth**
  - Workloads spread across diverse infrastructure
  - On-premises and multi-cloud

- **Fewer** resources to manage environment

- Threat landscape continues to **evolve**
  - Sophisticated hackers constantly innovating
  - Compliance regulations on the rise
**Improving** security and compliance is the most popular and most compelling reason for companies to optimize their server operating system.

### Reasons to optimize

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved security and compliance</td>
<td>70%</td>
</tr>
<tr>
<td>Cost reduction</td>
<td>59%</td>
</tr>
<tr>
<td>Shift more budget to innovation</td>
<td>54%</td>
</tr>
<tr>
<td>None of these</td>
<td>1%</td>
</tr>
</tbody>
</table>

### Most compelling reason

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved security and compliance</td>
<td>50%</td>
</tr>
<tr>
<td>Cost reduction</td>
<td>25%</td>
</tr>
<tr>
<td>Shift more budget to innovation</td>
<td>25%</td>
</tr>
<tr>
<td>Other (please specify):</td>
<td>0%</td>
</tr>
</tbody>
</table>
Security concerns and ease of use are the most common reasons for a company to change their server operating system.

Which of the following reasons, if any, would you change your server operating system?

- Security concerns: 44%
- Ease of use: 42%
- Improved monitoring of performance: 41%
- Compatibility with devices: 39%
- Easier to adjust infrastructure: 37%
- Better access to support: 37%
- Speedier internet access: 35%
- Ability to scale: 35%

Q6.4 For which of the following reasons, if any, would you change your server operating system? Select all that apply.
Total respondents: n=407.
Red Hat Insights

Included with Red Hat Enterprise Linux subscription

**Operational and vulnerability management**
- for RHEL environments

**Included with active subscriptions**
- For Red Hat Enterprise Linux, versions 6.4 and higher

**Risk analysis**
- Performance, security, compliance, availability, stability and workload-specific

**Simplified management**
- Patching efficiency, system comparison and alerting for internally-defined policies
Expanded 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

- **Subscriptions**
  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
Security and compliance management

Creating value for customers with Red Hat Insights

- Red Hat Insights
- Red Hat Smart Management
- Red Hat Ansible Automation Platform

- Integrated management
- Proactive guidance
- Continuous insights
- Remediation playbooks
Insights and Smart Management
Put insights into action via push-button remediation

**Cloud Connector**
Connects your federated Satellite infrastructure to Insights to execute remediation playbooks at scale.

*Multiple Satellites are supported, but optional*
Insights: Vulnerability

Remediate all Common Vulnerabilities and Exposures (CVEs)

Vulnerability offers

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 and PDF reports to keep relevant stakeholders informed

Quickly identify and remediate systems impacted by specific CVEs and create a plan for resolution
Insights: Deep threat analysis with security rules

Understand and prioritize critical vulnerabilities with heightened exposure

Curated rules that are hand-written based on Red Hat Product Security criteria

Deep understanding of Red Hat Enterprise Linux, only from Red Hat teams

Coverage of critical security vulnerabilities
Insights: Compliance

Built on OpenSCAP reporting

Compliance offers

- **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
## Insights: Reporting and workflows

Eliminate time-consuming and manual “management by spreadsheet” tasks

- Executive Report
- By system
- By vulnerability/CVE
- Custom (coming!)
- Variety of formats
  - CSV, PDF, JSON

### Executive report: Vulnerability

This is an executive summary of vulnerabilities (CVEs) identified by Red Hat that may impact your Red Hat Enterprise Linux (RHEL) servers.

The vulnerability service analyzed 106 RHEL systems and identified 1,595 CVEs that impact 10 of the systems.

#### CVEs by severity

<table>
<thead>
<tr>
<th>CVSS score range</th>
<th>Number of CVEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0 - 10.0</td>
<td>112 (7% of total)</td>
</tr>
<tr>
<td>4.0 - 7.9</td>
<td>1190 (75% of total)</td>
</tr>
<tr>
<td>0.0 - 3.9</td>
<td>293 (18% of total)</td>
</tr>
</tbody>
</table>

#### CVEs published by time frame

<table>
<thead>
<tr>
<th>Time frame</th>
<th>Number of CVEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 7 days</td>
<td>3</td>
</tr>
<tr>
<td>Last 30 days</td>
<td>16</td>
</tr>
<tr>
<td>Last 90 days</td>
<td>57</td>
</tr>
</tbody>
</table>

#### Top 3 CVEs in your infrastructure

<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>CVSS score</th>
<th>Systems exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-8616</td>
<td></td>
<td>A flaw was found in BIND, where it does not sufficiently limit the number of</td>
</tr>
</tbody>
</table>
Insights Demo
Future Insights use cases: Vulnerability and Compliance

- Reporting! Reporting! Reporting!
- Alerting & notification
- Granular RBAC to delegate permissions to stakeholders
- Identify CVEs w/ known exploits
- Integration between Vulnerability & Patch services
- ...

This information is for discussion purposes only and is subject to change without prior notice and the roadmap contained herein is not guaranteed to be up to date.
Additional resources and next steps

**READ THE RED HAT INSIGHTS SECURITY BRIEF**
Read the Red Hat Insights security brief:

**RED HAT® ENTERPRISE LINUX® CUSTOMER CAN GET STARTED**
You have Red Hat Insights at no additional cost:
[red.ht/insights_start](red.ht/insights_start)

**HEAR FROM CUSTOMERS**
Red Hat Insights customers discuss the benefits:
[bit.ly/April_panel](bit.ly/April_panel)
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
facebook.com/redhatinc
youtube.com/user/RedHatVideos
twitter.com/RedHat