RED HAT INSIGHTS

Security & Proactive Response with Insights

William Nix
Principal Technical Marketing Manager
Management Business Unit, Red Hat Insights

WHY WE BUILT A NEW PRODUCT

SECURITY IS

RISK MANAGEMENT

COMPLEXITY CREATES RISK

80 %

Carnegie Mellon University

Commercial application outages are caused by software failure and operational complexity.

336 k/hr

Gartner®

The median cost of downtime for a production application for a large enterprise

65 %

CompTIA®

Customers thought they were behind in training and capabilities needed to manage their next gen infrastructure.

RED HAT INSIGHTS

COMPLEXITY CREATES RISK

DO NOT BECOME

A STATISTIC

RED HAT INSIGHTS

ANALYZING INFRASTRUCTURE RISK

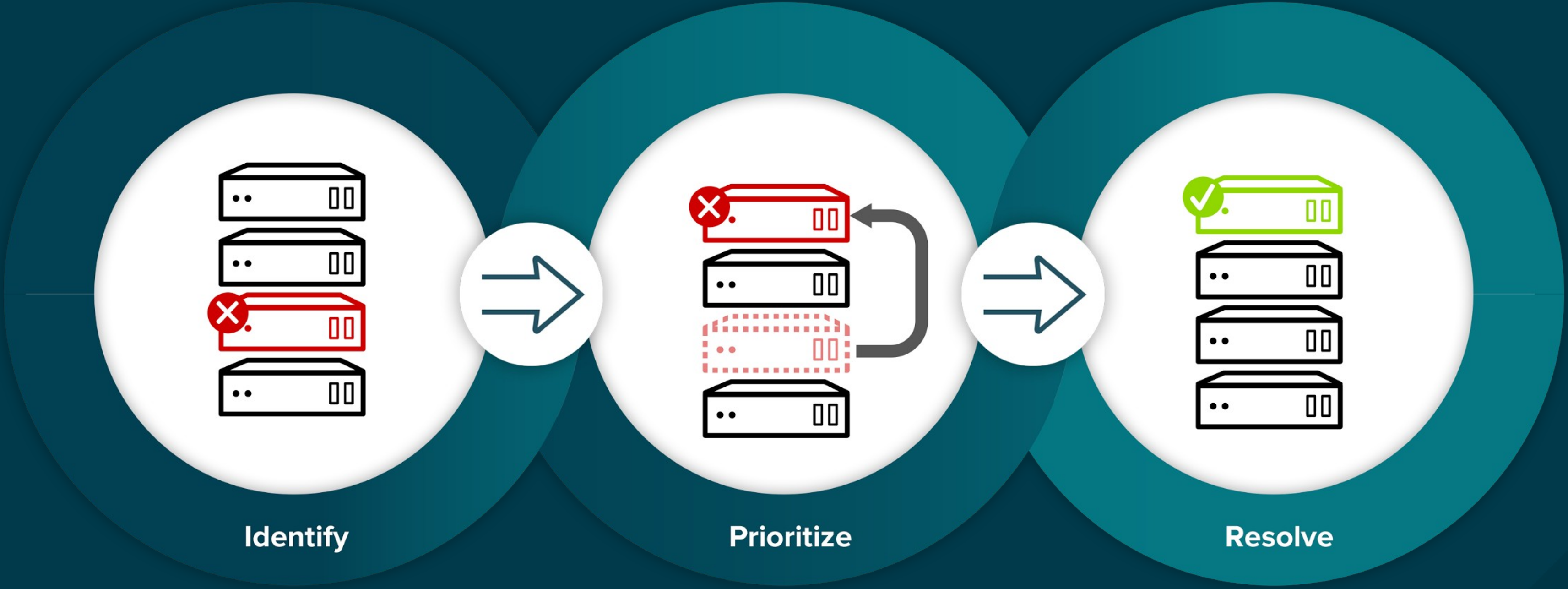
TOOLS - Are you comfortable that your tooling and processes will scale as your environment scales?

RESPONSE - Are you confident that you can quickly respond when vulnerabilities strike?

COMPLIANCE - Are you certain that your systems are compliant with various infosec and audit requirements?

RED HAT® INSIGHTS

MANAGING INFRASTRUCTURE RISK



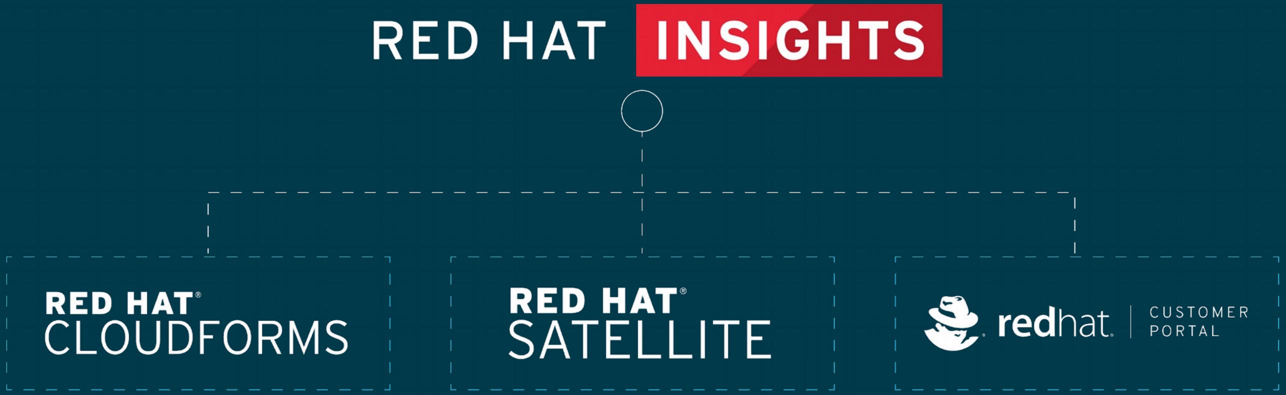
HOW INSIGHTS WORKS

MODERN SYSTEMS MANAGEMENT

Red Hat Insights (RHI) is based on four main concepts:

- Proactive Systems Management
- Lightweight Data Collection
- Clear, Tailored, and Actionable Intelligence
- Insights Powered By Red Hat

INTEGRATED INTO TOOLS YOU ALREADY USE



RED HAT INSIGHTS

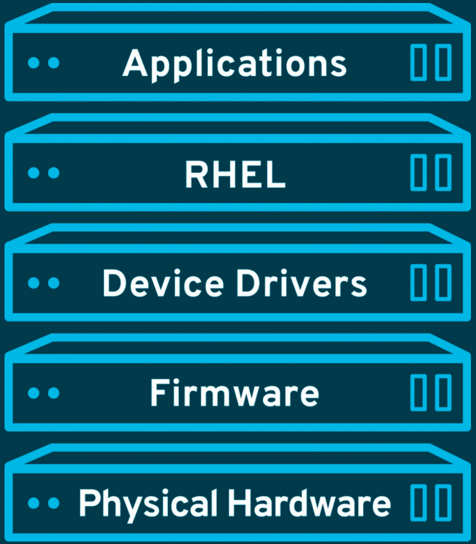
RED HAT CLOUDFORMS

RED HAT SATELLITE

redhat CUSTOMER PORTAL

RED HAT INSIGHTS

FULL STACK ANALYSIS


Applications

RHEL

Device Drivers

Firmware

Physical Hardware

splunk>
ORACLE
EMULEX An Avago Technologies Company
EMC²
Chelsio Communications Accelerate
QUALCOMM
DELL
HITACHI Inspire the Next
SOLARFLARE
lenovo
intel
hp
Microsoft
Mellanox TECHNOLOGIES
AMD
BROADCOM.
NEC
cisco
FUJITSU
IBM
vmware

RED HAT INSIGHTS

REAL WORLD RESULTS

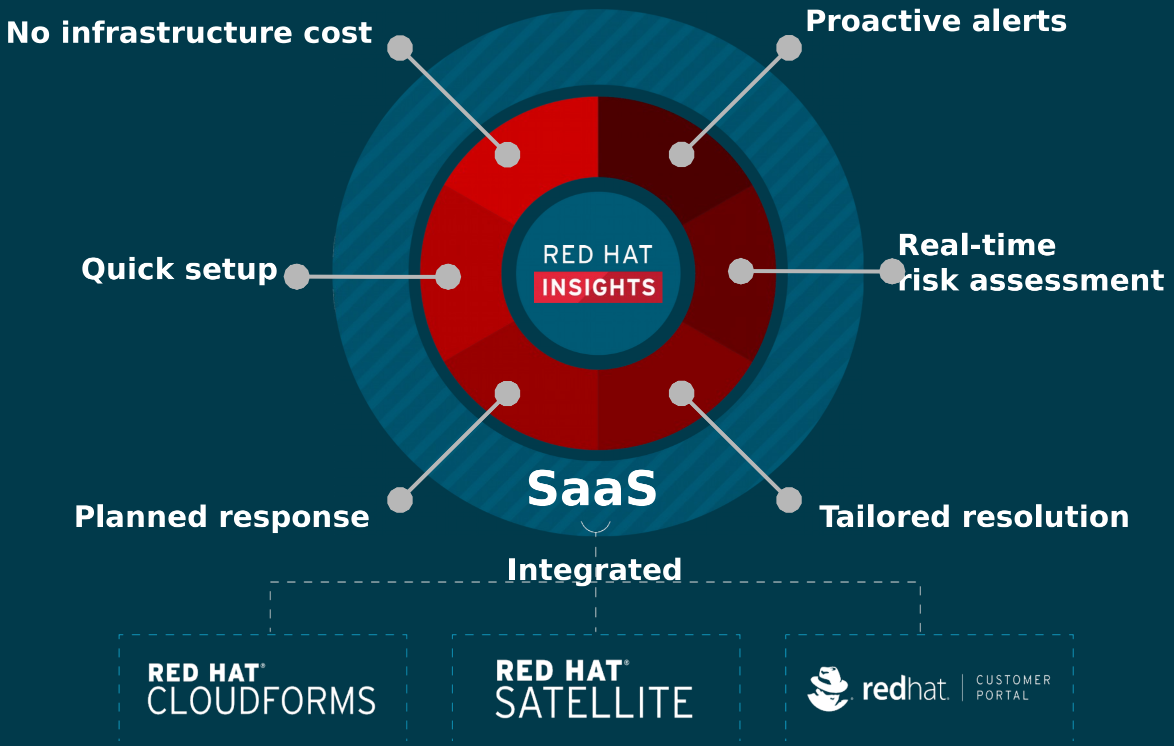
“Insights helps our teams be more proactive at resolving critical issues before they occur. The reliability of Insights *saves us time and labor intensive tasks.*

We no longer have to look at individual systems because we have one system with insight into our entire infrastructure.”

-- Jason Cornell, AutoTrader / Cox Automotive

RED HAT INSIGHTS

Operational analytics from Red Hat empowers you to prevent downtime and avoid firefighting while responding faster to new risks.



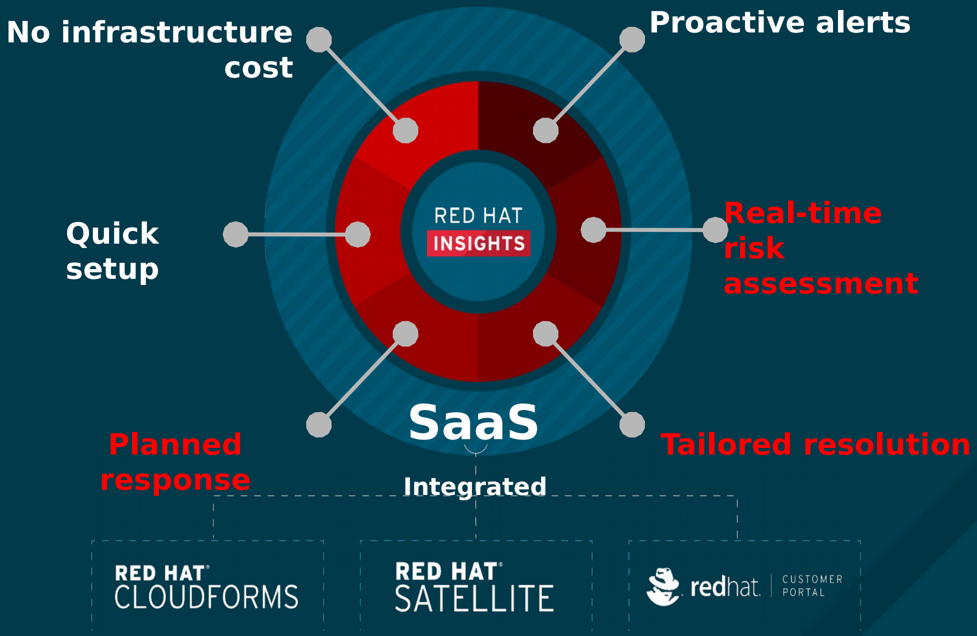
RED HAT INSIGHTS

Operational analytics from Red Hat empowers you to prevent downtime and avoid firefighting while responding faster to new risks.

MOVES YOU FROM REACTIVE TO PROACTIVE SYSTEMS MANAGEMENT

DELIVERS ACTIONABLE INTELLIGENCE FROM THE OPEN SOURCE LEADER

INCREASES VISIBILITY OF INFRASTRUCTURE RISKS AND THE LATEST SECURITY THREATS



Insights requires no additional infrastructure to manage. Simply install the RPM and begin analyzing for problems.

RHEL 6.4+, RHEL 7+

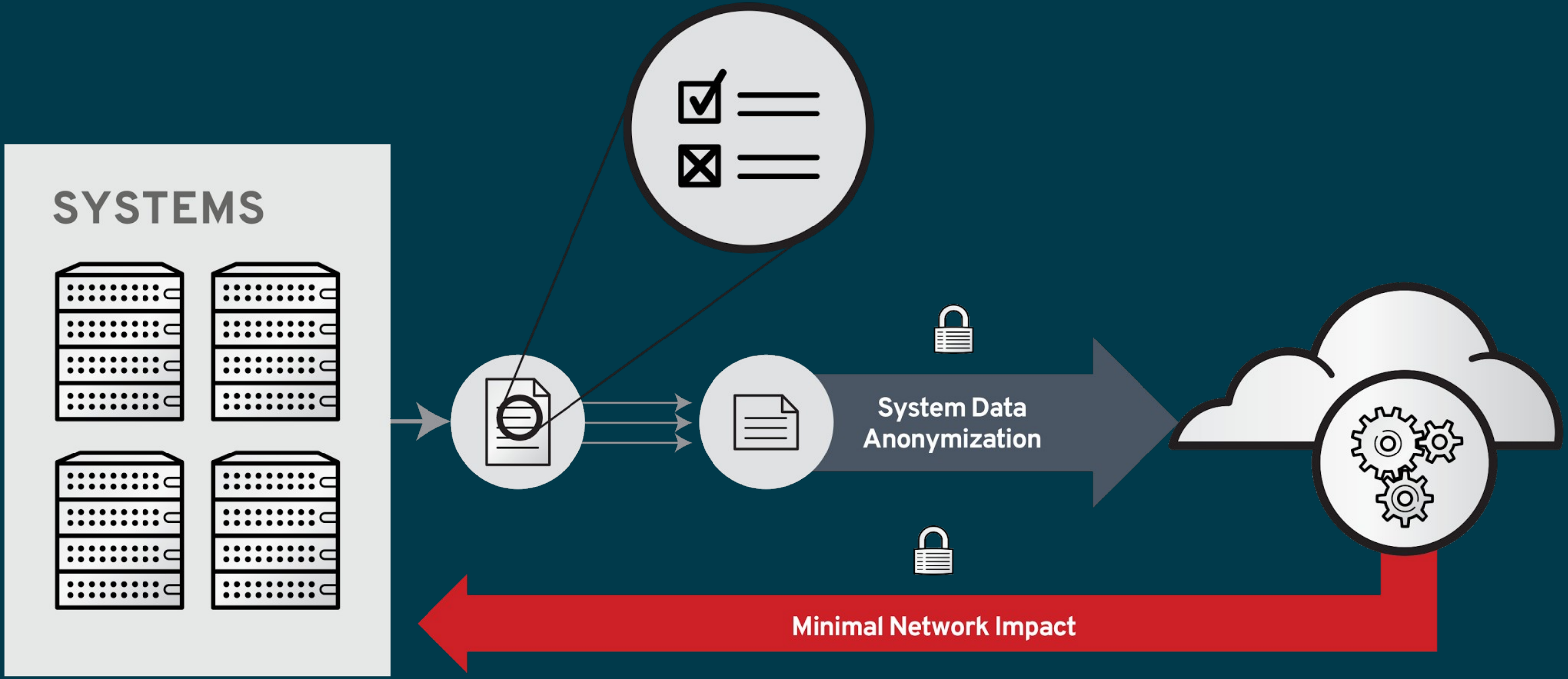
```
# yum install redhat-access-insights
```

```
# redhat-access-insights --register
```

Insights can be registered and report directly, or via an SSL proxy (typically Red Hat Satellite)

RED HAT® INSIGHTS

Insights requires no additional infrastructure to manage. Simply install the RPM and begin analyzing for problems.



RED HAT® INSIGHTS

Insights is a service, so that means we are able to ...

- The ability to quickly alert on new problems arising across the board
- Adapt to many changing infrastructure configurations
- We’re able to provide real-time risk assessment in Red Hat infrastructure
- Iterate quickly and add new features and functionality based on feedback

RED HAT INSIGHTS

What’s new released at Summit 2016

Container analysis

Identify risks in container platforms, images, and containers

Continuous stream of updated checks

Simple remediations steps and guidance with awareness of state of container lifecycles

OpenStack and RHEV support

Analysis of individual nodes, cluster manager, and overall cluster state

Data collection and communication via OSP Director and RHEV-Manager

Action plans

Identify, prioritize, and share maintenance plans to better bridge the gap between assessment and action

Insights recommended action plans, when new critical issues hit

Early Access Mode

Test out and provide feedback on new features while still in development

Switch seamlessly between stable and early access mode without re-registering systems

Security Response

RED HAT INSIGHTS

INSIGHTS FOR SECURITY RESPONSE

Stay ahead of your security team

- Start planning your remediation before the security team starts asking questions
  - Insights helps you answer those question when they arise

- Plan your response around the most critical vulnerabilities and systems

- Know that issues were remediated properly
  - Insights check-ins

RED HAT INSIGHTS

INSIGHTS FOR SECURITY RESPONSE

Working with Red Hat Product Security

- Red Hat Product Security writes rules before embargo is lifted
- Insights Rule is Released on the day that the embargo is lifted
- Customers can start planning their response the day the vulnerability becomes public, with trusted guidance from Red Hat Software and Security engineers

RED HAT INSIGHTS

INSIGHTS FOR SECURITY RESPONSE

Planning a response to DROWN OpenSSL Vulnerability

- OpenSSL DROWN (CVE-2016-0800)
- Special DROWN (CVE-2016-0800) + (CVE-2015-0293)
  - Much more efficient attack if you are vulnerable to both.

INSIGHTS FOR SECURITY RESPONSE

Prioritizing Special over General DROWN in the following categories:

- A service on a publicly routable IP address
- A service on a private IP address
- A server with the version of OpenSSL vulnerable to DROWN, but no known services are listening on route-able IP address.

RED HAT® INSIGHTS

INSIGHTS FOR SECURITY RESPONSE

Assurance of remediation

- Run the Insights client to force a re-check of the system
- Wait until the next automatic check in

RED HAT® INSIGHTS

What’s coming in the next 12 months ...

Site-guidance

Track site-wide trends in security response, technical debt, and deployment agility

Get site-wide recommendations based on statistically validated industry trends

Full CVE Analysis

Identify all of the Red Hat Security Errata that would apply to a host.

Currently Red Hat Insights detects the highly publicized vulnerabilities and those categorized as Critical by Red Hat Product Security

Compliance Checks

Leverage OpenSCAP to display compliance checks for PCI-DSS and STIG.

Ansible Playbooks

In a movement toward “fix-it for me” technology, we will begin generating Ansible playbooks which can be downloaded and used for remediation.

Begin monitoring your infrastructure, for free, at https://access.redhat.com/insights