RED HAT AUTOMATED SECURITY AND COMPLIANCE FOR TELECOMMUNICATION SERVICE PROVIDERS

AUTOMATION ACROSS I.T. AND NETWORKS FOR IMPROVED AND PROACTIVE SECURITY

OVERVIEW

According to Gartner, "Security teams are suffering from staff shortages, an increase in the volume of alerts and threats, and the ever-present need to do more with less."[1]

INTRODUCTION

As networks and infrastructures grow and become more complex, automation is needed to ensure that deployments and distributed architectures are secure, compliant, and performing as expected. Inconsistent patching and configurations are hard to manage in this complex, hybrid environment, with Windows and Linux® operating systems, virtualized infrastructure, public and private cloud infrastructures, and containers. As this mixed environment grows, complexity and risk increase with reduced visibility and control, making manual security and compliance monitoring increasingly difficult—you cannot control or secure what you cannot see. On top of all this, relationships are often strained between development, operations, and security teams, and security teams are often the last to know about configuration changes and issues.

When vulnerabilities are identified, it takes time to resolve issues and automate fixes, and issues that linger are the ones that get organizations in trouble. In fact, Gartner[2] has identified known vulnerabilities as the biggest issue facing industries. When fixes are eventually applied, organizations then struggle with the documentation that is needed for what was remediated, when, by whom, and the issues that were resolved. Service providers must also adhere to industry security standards, such as PCI-DSS, which requires scanning, maintenance, and remediation processes to be in place and documented for compliance.

AUTOMATION TO ADDRESS SECURITY AND COMPLIANCE

To address security and compliance concerns, service provider focus is on data-driven IT and network process automation across the entire environment. This automation includes:

- Operating systems (OS)
  - Package management
  - Patch management
  - OS hardening to a security compliance baseline at provisioning time for consistency and OS immutability
- Infrastructure and security as code
  - Repeatability, ability to share and verify, and help with passing security and compliance audits
  - Everyone in the organization can speak the same scripting/programming language, which is easy to quickly learn and use

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

redhat.com

1 *Chuvakin, Anton; Barros, Augusto Barros. "Preparing Your Security Operations for Orchestration and Automation Tools." gartner.com: Gartner, February 22, 2018. https://www.gartner.com/doc/3860563/preparing-security-operations-orchestration-automation*

2 *Moore, Susan. "Focus on the Biggest Security Threats, Not the Most Publicized." gartner.com: Gartner, November 2, 2017. https://www.gartner.com/smarterwithgartner/focus-on-the-biggest-security-threats-not-the-most-publicized/*

- System provisioning
  - Integration with IT service management (ITSM), for example, ServiceNow
  - Storage provisioning
- Workflows
  - Simplified services management
- Continuous security and monitoring with Day 2 security operations
  - Patch management
  - Vulnerability identification and management (health checks, etc.)
  - Proactive governance of security, control, and compliance policies
  - Remediation: fix generation and automation

SECURITY AND COMPLIANCE AUTOMATION CHALLENGES

Manually checking systems for security and compliance is problematic for many reasons:

- Time consuming, tedious, boring
- Prone to human error
- Improper actions and simple configuration changes lack audit trail information
- Not repeatable, shareable, or verifiable
- Difficult to pass audits due to incomplete and inconsistent change log information
- Ineffective or nonexistent communication between operations and security teams

Service providers must determine where manual tasks are performed and how often, and must implement an automation strategy with the most robust and flexible automation technologies available. Selecting the right automation technologies is key for rapid implementation and being able to expand automation across devices and services in the network.

INTELLIGENT SECURITY AUTOMATION WITH RED HAT

Red Hat® technologies offer a holistic, end-to-end software stack automation strategy, from a security-hardened operating system to automation software to dozens of vendor integrations (AWS, Cisco, Juniper, VMware, etc.), encompassing both IT and networking automation needs.

Having an entire stack of Red Hat technologies is not required, but the power of security and compliance automation is amplified when Red Hat products are combined. In the case of security and compliance automation, the combination of Red Hat Enterprise Linux, Red Hat Ansible® Automation, Red Hat Satellite, Red Hat Insights, and is particularly powerful.

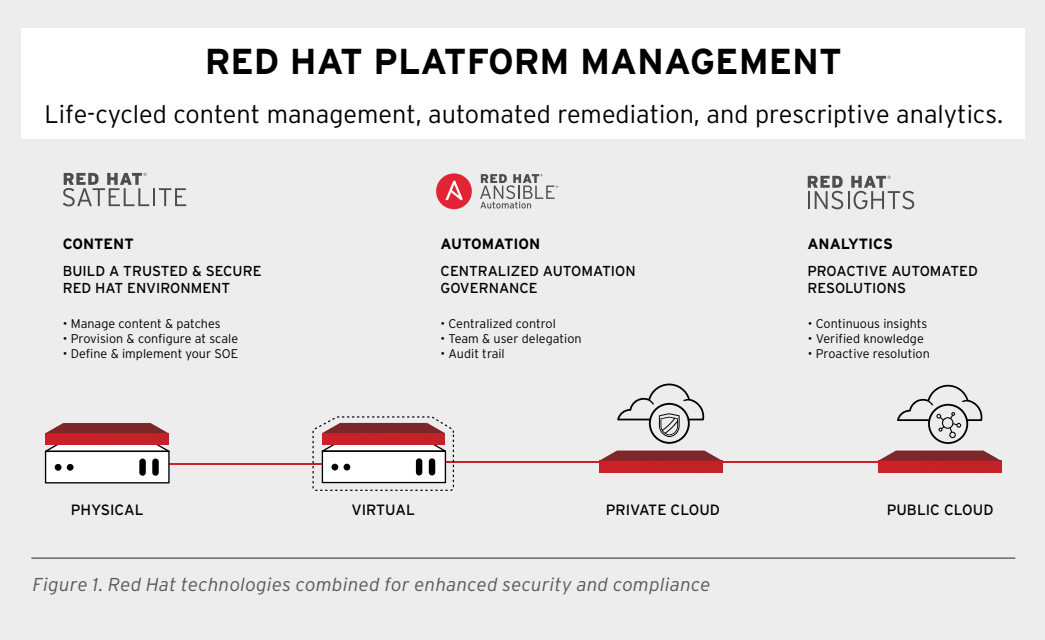


Figure 1. Red Hat technologies combined for enhanced security and compliance

These Red Hat technologies work in concert for additional security and compliance benefits:

RED HAT ENTERPRISE LINUX

Red Hat Enterprise Linux provides security technologies to combat vulnerabilities, protect data, and meet regulatory compliance. You can automate regulatory compliance and security configuration remediation across systems and within containers with OpenSCAP, Red Hat's National Institute of Standards and Technology (NIST)-certified scanner that checks and remediates against vulnerabilities and configuration security baselines, including:

- PCI-DSS
- DISA security technical implementation guide (STIG)
- Criminal Justice Information Services (CJIS) Security Policy
- Commercial cloud services (C2S)
- Health Insurance Portability and Accountability Act (HIPAA)
- NIST 800-171
- Operating System Protection Profile (OSPP) v4.2
- Red Hat Corporate Profile for Certified Cloud Providers

To better meet the varied security needs of hybrid computing, Red Hat Enterprise Linux 7.5 provides enhanced software security automation to mitigate risk through integration of OpenSCAP with Red Hat Ansible Automation. This integration supports the application of pregenerated Red Hat playbooks and supported Ansible Playbooks to remediate systems for compliance with security baselines, the creation of new Ansible Playbooks from a specific security profile, and the creation of Ansible Playbooks directly from OpenSCAP scans, which can then be used to implement remediations more rapidly and consistently across a hybrid IT environment.

Red Hat Enterprise Linux system roles also help with automated security. These system roles are a collection of Ansible roles and modules that provide a stable and consistent configuration interface to remotely manage Red Hat Enterprise Linux 6.10 and later versions. For example, the SELinux system role can be used to correctly and consistently configure Security-Enhanced Linux (SELinux) across Red Hat Enterprise Linux systems.

By automating common management tasks, fewer users require direct superuser access to hosts, reducing attack surface area. Using SELinux, automated management tasks can be assigned privileges specific to that task, which guards against privilege escalation bugs.

RED HAT ANSIBLE AUTOMATION

Red Hat Ansible Automation, which includes Red Hat Ansible Tower, is a simple, powerful, and agentless IT automation technology that provides a common automation platform across the organization, providing the following security and compliance benefits:

- Traceability and repeatability for compliance
- Drastically reduced time spent on repetitive and mundane tasks
- Reduced risk of downtime by having a consistent approach to managing infrastructure
- Minimized risk of systematic errors through automated analysis, detection, and resolution
- Accelerated time to revenue by bringing technology into service faster
- Lowered costs through reduced efforts
- Reduced risk of human error
- Accelerated IT processes (often from days to minutes)
- Consistent configuration and management across a multivendor environment
- Automated deployment, configuration, and configuration life-cycle management, including rolling out policy and updating systems and firewalls across the entire network
- Rapid replication of field problems using configuration information in service catalogs
- Ability to embed Ansible automation into existing security tools and processes using representational state transfer application programming interface (RESTful API)
- Highly scalable automation solution covering access control, credentials vault, job and workflow scheduling, source control integration, and auditing with graphical inventory management, simplifying representation of all components, and providing visibility into all automation activity

Red Hat Ansible Automation includes modules and roles specifically created for integration with security vendors and security solutions, for example, Splunk (SIEM), Snort (intrusion detection and prevention), and Checkpoint (enterprise firewall).

RED HAT SATELLITE

Red Hat Satellite provides IT information about Red Hat systems in the environment, including identifying systems that are out of date and systems with known vulnerabilities. Organizations use Red Hat Satellite for subscription and content management, provisioning security-compliant hosts, configuration management, and patch management. Red Hat Ansible Automation works with Red Hat Satellite to automatically deploy and manage software configurations for end-to-end, automated management and control of systems and applications throughout their life cycle, helping maintain security, compliance, and an audit trail.

- Satellite defines and enforces a standard operating environment (SOE).
- Satellite uses Ansible Automation to deploy Red Hat Enterprise Linux system roles and install Insights for the SOE.
- Satellite identifies drift from the SOE and uses Ansible Automation to remediate drift issues.
- Satellite identifies security, performance, stability, and availability risks through Insights. Insights can then dynamically generate Ansible Playbooks for direct execution from Satellite for risk remediation.
- Systems provisioned via Satellite can perform callbacks to Ansible Tower for post-provisioning playbook execution.
- Satellite uses Ansible Automation to import and use Red Hat Enterprise Linux system roles.
- Via the dynamic inventory, Ansible Tower uses Satellite as a dynamic inventory source.
- Insights can be deployed using Ansible Automation from within Satellite.

RED HAT INSIGHTS

Red Hat Insights is included with Red Hat Satellite and can also function individually as a Red Hat Enterprise Linux add-on. Findings from Insights provide actionable predictive analytics. When integrated with Ansible Tower, Insights can be configured to automatically generate playbooks and perform remediation with the generated playbooks. Ansible Tower uses the Insights API to support jobs for site-wide remediation. You can also integrate Insights detection and remediation capabilities into external systems or scripts, giving operations teams the ability to scale guided remediation out to the entire enterprise.

Ansible Tower can be configured to connect to the Insights API and retrieve information from it. For example, Ansible Tower can pull the Ansible Playbooks used in the Customer Portal version of Red Hat Insights. That way, these Ansible Playbooks can be launched directly from Ansible Tower for automated remediation of issues found by Insights.

Because Insights is integrated within Satellite, you can directly execute remediation playbooks from Red Hat Satellite's web interface.

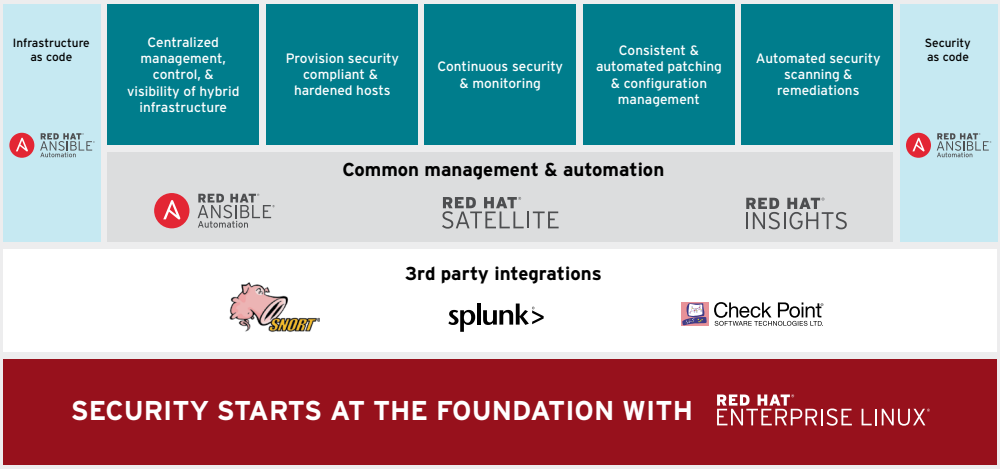


Figure 2. Automated security and compliance with Red Hat

USE CASE—AUTOMATED PATCH MANAGEMENT

Working together, Red Hat Satellite, Red Hat Insights, and Red Hat Ansible Automation seamlessly detect risks to Red Hat Satellite-managed hosts and fix many of these discovered issues using Red Hat Ansible Automation Playbooks. You can create a repeatable remediation plan, act upon that plan, and provide report information to auditors. Insights can be configured to control the type of information that is sent to Satellite, allowing you to see the data that is being sent and manage it.

1. Use Insights to identify systems that require patching.
2. Create an Insights plan for the playbooks you want to run and the systems on which to run them.
3. Schedule the execution of the Insights plan or run it manually.
4. Act on the information provided by the Insights plan. Insights learns and gets smarter with every additional piece of intelligence and data. It can automatically discover relevant insights, proactively recommend tailored next actions, and even automate tasks.
5. Provide consolidated audit trail information produced by the execution of the Insights plan, which includes who ran the plan, the start and end times, and task-level execution.

This combination of Red Hat Satellite, Red Hat Ansible Automation, and Red Hat Insights helps you find issues and fix them before they cause problems, providing a solution for continuous monitoring and automated security and compliance actions.

SUMMARY

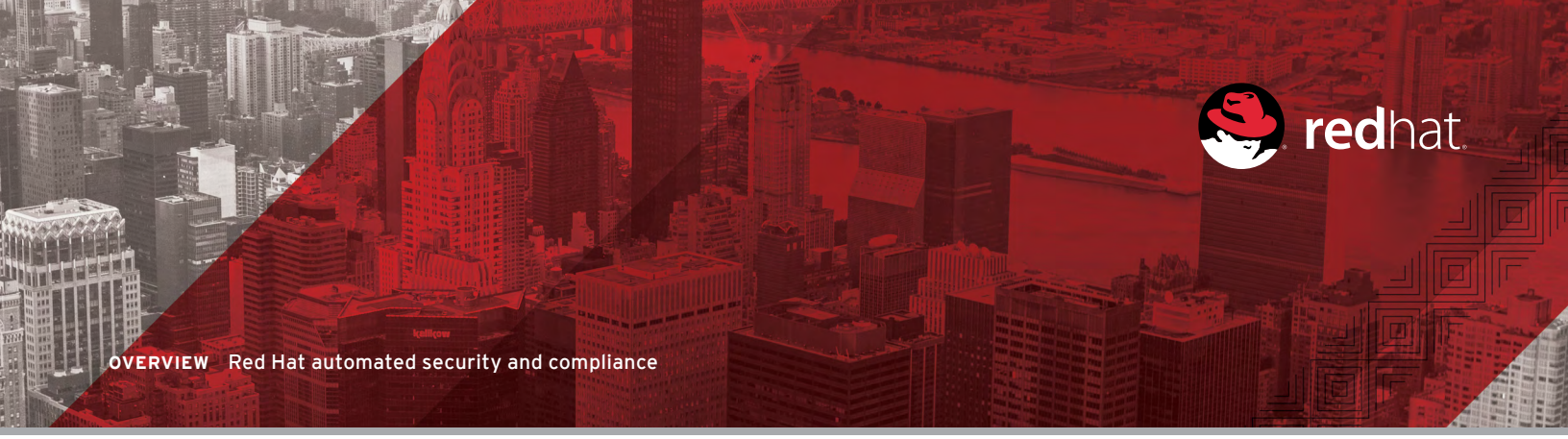
As networks evolve toward programmability, and other technologies—such as network function virtualization (NFV)—add complexity, automation is critical for managing the IT and network environment. The technologies comprising the Red Hat automation and compliance solution address service provider concerns with end-to-end automation for IT and networks.

Whether it is hooking into Red Hat Satellite to provision and configure security-compliant systems, using Red Hat Insights data to proactively resolve security issues, or using simple automation to deploy, manage, and upgrade your cloud, Red Hat Ansible Automation provides the common automation language and operational layer with exposed APIs needed for end-to-end automation across organizations with device-specific and app-specific needs for holistic security. Red Hat Ansible Automation provides automation for the entire Red Hat Enterprise Linux environment, including discovery of environment information, adherence to organizational policies, and making configuration changes based on that policy.

All Red Hat products are vendor-agnostic, supporting your IT environment without replacement of critical legacy applications and processes, providing integration and orchestration of security tasks and processes across devices, platforms, and vendors. With Red Hat, resources can focus on innovation, while Red Hat supports your critical security automation and simplifies your services management.

NEXT STEPS

- To initiate or expand security and compliance automation, a Red Hat Discovery Session helps analyze your environment for automation opportunities. Red Hat Services also offers a more comprehensive Automate Security and Reliability Workflows offering, which combines Red Hat Insights, Red Hat Satellite, and Red Hat Ansible Tower to identify existing gaps or potentially problematic configurations identified by Insights. The Automate Security and Reliability Workflows offering provides a scalable framework on which to use and customize Insights-provided playbooks, and also use and deploy customer playbooks, to remediate vulnerabilities and provide an audit trail across the IT environment.
- Preview a video of Red Hat Satellite 6.4 working with Red Hat Insights and Red Hat Ansible Automation to seamlessly detect risks to hosts managed by Red Hat Satellite and easily fix discovered issues using a Red Hat Ansible Automation Playbook available for remediation via Insights. See how you can find issues and fix them before they cause you problems.



LEARN MORE

- Red Hat Satellite, Red Hat Insights, and Red Hat Ansible Automation also provide additional security management and control across the Red Hat portfolio, for example, Red Hat OpenStack® Platform clients.
- Other Red Hat technologies, including Red Hat OpenStack Platform, provide functionality to specifically address key security and compliance concerns. Red Hat understands that end-to-end security, compliance, and auditing orchestration is needed in today's constantly changing environment and provides the platforms and tools needed for management and control.

For questions or additional information, contact your Red Hat representative.

ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

NORTH AMERICA
1 888 REDHAT1

EUROPE, MIDDLE EAST, AND AFRICA
00800 7334 2835
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
info-latam@redhat.com

redhat.com
f14713-201901