Red Hat automated security and compliance for financial services

> *"Teams are able to move faster, collaborate more efficiently across the company, and spend more time innovating. This effort helps us achieve our promise to do it right for our customers."*[1]
>
> **James Hixon**
> Senior Director,
> Cloud Automation and Engineering,
> Ally Financial

Introduction

As digital adoption grows, so does the complexity of the associated infrastructure. This scenario is especially true in the financial services sector, which has traditionally been risk averse and change resistant, bound by both technical and regulatory constraints. Financial services firms need automation capabilities to deploy applications and to ensure that distributed architectures are consistent and compliant with the required security. Inconsistent patching and configurations can be hard to manage in an environment with Windows and Linux® operating systems, virtualized infrastructure, public and private cloud infrastructures, and containers.

As this mixed environment grows, risk increases with reduced visibility and control, making manual security and compliance monitoring increasingly difficult. In addition, relationships are often strained between development, operations, and security teams—with security personnel 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 can cause trouble for organizations. Identified vulnerabilities are an additional challenge. When fixes are eventually applied, organizations then struggle with the documentation needed for what was remediated, when, and by whom. Banks, payment providers, and insurers, along with other financial service firms, must also adhere to security standards, such as Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR), which requires stringent tracking, reporting, and documentation to remain in compliance.

Automation to address security and compliance

To address security and compliance concerns, financial services providers focus 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
  - Ability to repeat, share, and verify—and assist with security and compliance audits
  - Everyone in the organization can speak the same scripting/programming language, increasing ease of use

[1] *Red Hat success story. "Ally Financial adopts cloud platform and DevOps, speeds time to market," May 2019.*

- System provisioning
  - Integration with IT service management (ITSM)
  - Storage provisioning
- Workflows
  - Simplified services management
- Continuous security and monitoring with Day 2 security operations
  - Patch management
  - Vulnerability identification and management (e.g., health checks)
  - 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 and tedious
- 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 changelog information
- Ineffective or nonexistent communication between operations and security teams

Financial products and services firms must determine where manual tasks are performed, and their frequency, to determine an automation strategy. They should focus on flexible automation technologies to accommodate future requirement changes. Selecting the right automation technologies is key for rapid implementation and expansion across network devices and services.

Intelligent security automation with Red Hat

Red Hat® technologies offer an end-to-end software stack to support your automation strategy—from a security-hardened operating system and 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 Platform, Red Hat Satellite, and Red Hat Insights is particularly powerful.

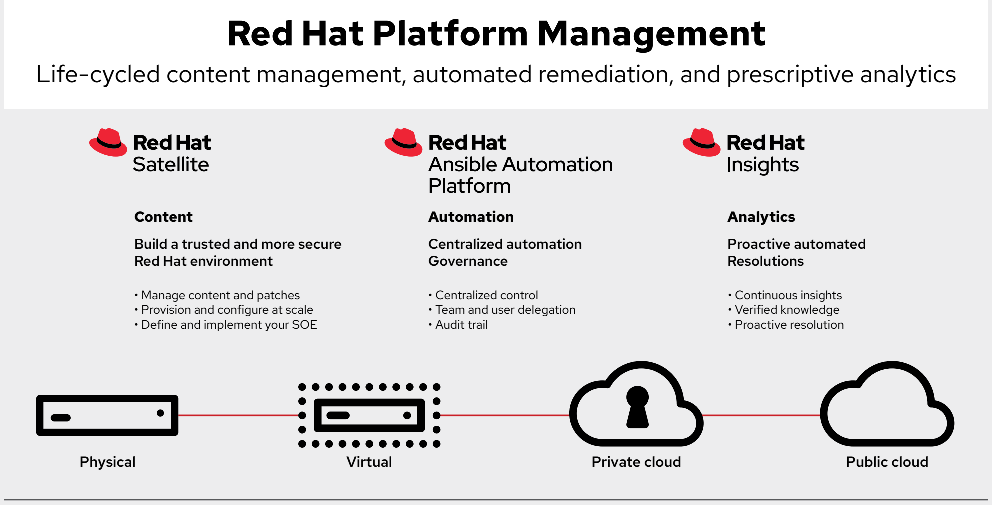
Red Hat Platform Management
Life-cycled content management, automated remediation, and prescriptive analytics
Red Hat Satellite
Content
Build a trusted and more secure Red Hat environment
• Manage content and patches
• Provision and configure at scale
• Define and implement your SOE
Red Hat Ansible Automation Platform
Automation
Centralized automation Governance
• Centralized control
• Team and user delegation
• Audit trail
Red Hat Insights
Analytics
Proactive automated Resolutions
• Continuous insights
• Verified knowledge
• Proactive resolution
Physical
Virtual
Private cloud
Public cloud

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

These Red Hat technologies work together 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.
- Defense Information Systems Agency (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 provides enhanced software security automation to mitigate risk through integration of OpenSCAP with Red Hat Ansible Automation Platform. This integration supports the application of pregenerated Red Hat 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. These can 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, utilizing 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 Security-Enhanced Linux (SELinux) system role can be used to correctly and consistently configure 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, guarding against privilege escalation bugs.

Red Hat Ansible Automation Platform

Red Hat Ansible Automation Platform, which includes Red Hat Ansible Tower, is simple, powerful, 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 tasks
- Reduced risk of downtime through a consistent infrastructure management approach
- Minimized risk of systematic errors through automated analysis, detection, and resolution
- Accelerated time to revenue by bringing technology into service faster
- 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 policy rollout 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 Platform 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

Ansible Automation Platform 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 with information about Red Hat systems in the environment, including identifying systems that are out of date and with known vulnerabilities. Organizations use Satellite for subscription and content management, provisioning security-compliant hosts, configuration management, and patch management. Ansible Automation Platform works with 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.

Red Hat Satellite:

- Defines and enforces a standard operating environment (SOE).
- Uses Ansible Automation Platform to deploy Red Hat Enterprise Linux system roles and install Red Hat Insights for the SOE.
- Identifies drift from the SOE and uses Ansible Automation Platform to remediate drift issues.
- Identifies security, performance, stability, and availability risks through Insights, which 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.
- Use of Ansible Automation Platform 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 Platform 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 and when integrated with Ansible Tower, Insights can be configured to automatically generate playbooks and perform remediation. Ansible Tower uses the Insights API to support jobs for site-wide remediation. Insights detection and remediation capabilities can be integrated 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 to retrieve information from it. For example, Ansible Tower can pull the Ansible Playbooks used in the Customer Portal version of Red Hat Insights, and these playbooks can be launched directly from Ansible Tower for automated remediation of issues.

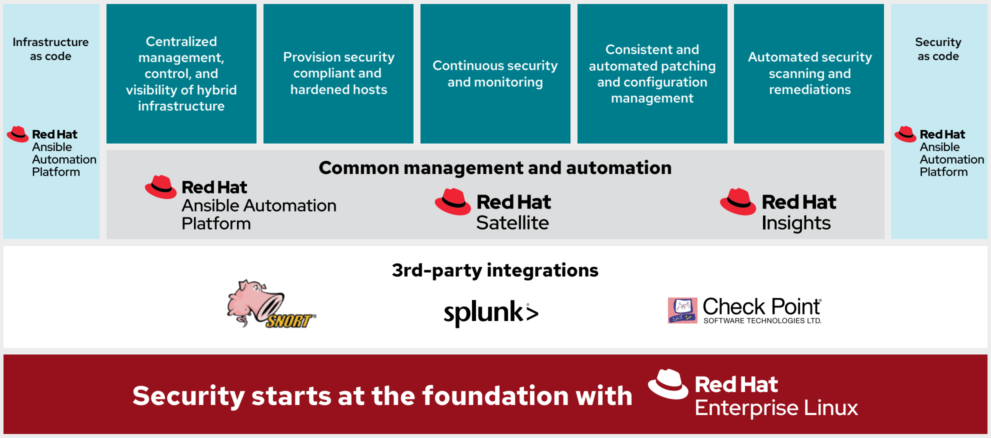
Infrastructure as code
Red Hat Ansible Automation Platform
Centralized management, control, and visibility of hybrid infrastructure
Provision security compliant and hardened hosts
Continuous security and monitoring
Consistent and automated patching and configuration management
Automated security scanning and remediations
Security as code
Red Hat Ansible Automation Platform
Common management and automation
Red Hat Ansible Automation Platform
Red Hat Satellite
Red Hat Insights
3rd-party integrations
SNORT
splunk>
Check Point SOFTWARE TECHNOLOGIES LTD.
Security starts at the foundation with Red Hat Enterprise Linux

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 Platform seamlessly detect risks to Red Hat Satellite-managed hosts and fix many of these discovered issues using Red Hat Ansible Automation Platform 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 transmitted data 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.

Summary

As financial networks evolve toward programmability, and applications add complexity, automation is critical for managing the IT and network environment. The Red Hat automation and compliance solution addresses financial service provider concerns with end-to-end automation for IT and networks.

Whether enabling 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 Platform provides the common automation language and operational layer with the exposed APIs needed for end-to-end automation. This approach is especially applicable across organizations with device-specific and app-specific needs for holistic security. Red Hat Ansible Automation Platform provides automation for the entire Red Hat Enterprise Linux environment, including discovering environment information, adhering to organizational policies, and enacting configuration changes based on that policy.

All Red Hat products are vendor-agnostic, and can support your IT environment without replacing critical legacy applications and processes, providing integration and orchestration of security tasks and processes across devices, platforms, and vendors. Internal 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 analyzes your environment for automation opportunities. Red Hat Services also offers a more comprehensive offering for automating security and reliability workflows, combining Red Hat Insights, Red Hat Satellite, and Red Hat Ansible Tower to identify existing gaps or potentially problematic configurations identified by Insights. The 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.

- Attend the security and compliance for financial institutions webinar to learn more about how Red Hat security management technology can help reduce infrastructure risk in your financial organization.

Learn more about Red Hat solutions

Red Hat Satellite, Red Hat Insights, and Red Hat Ansible Automation Platform provide additional security management and control across the Red Hat portfolio, for example, Red Hat OpenShift® clients.

Other Red Hat technologies 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 or read more about financial services automation.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

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

North America
1 888 REDHAT1
www.redhat.com

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