Red Hat

Automate security to align enterprise IT

How to unify security operations across SecOps, ITOps, and DevOps

Contents

Introduction

IT cybersecurity and compliance is a top concern

Security is an ongoing focus for most organizations, and many executives share a growing concern about cyberthreats. At the same time, compliance mandates continue to evolve and grow.

When a threat such as a breach or missing compliance mandate happens, the effects can be detrimental to revenue, business valuations, and stakeholder trust. As a result, organizations are reframing their view of cybersecurity as a business driver.

Safeguarding against threats

Protecting your organization is a critical, but often daunting task. Security teams must assemble, maintain, and adapt toolsets to monitor complex environments so they can meet the latest internal and external security policies.

Technical sprawl means that there are additional areas to protect while the volume of attacks continues to grow in sophistication and type.

For SecOps teams, it's imperative to proactively protect this evolving enterprise operation. Yet, there is often a missing link between what security experts observe and the ability to implement the needed changes across the IT operation. ITOps and DevOps teams are also pressured to stay resilient, yet innovate quickly.

The primary challenges with safeguarding against threats include:

Increased attack sophistication

Cyberattacks are becoming more advanced and adaptive, making it difficult for teams to detect and mitigate threats using traditional tools.

More attack surfaces

As organizations expand across cloud, on-premise, and edge environments, every new endpoint, application, and integration increases exposure.

Slow resolution speed

When a threat is identified, every second counts. Delays can lead to outages, data loss, or service disruption.

Disconnected technology stacks

Many organizations rely on a patchwork of tools that don't communicate or share data effectively, creating blind spots.

More compliance

Growing regulatory demands require continuous evidence of security, privacy, and operational controls across systems and services.

Cybersecurity is critical for business growth

According to Gartner®, Cybersecurity is no longer just about protection; it's a critical driver for business growth. With 85% of CEOs recognizing its importance, security leaders have a unique opportunity to demonstrate the value of cybersecurity investments not only in safeguarding assets but also in enabling strategic business objectives."[1]

This perspective signals that security has become strategic because it helps protect revenue, safeguard trust, and accelerate innovation without disruption.

To keep pace with rising risk and complexity, businesses must evolve through automation to help:

Protect revenue and stock prices

Security breaches and downtime can have immediate financial consequences. By automating protection, detection, and response workflows, organizations can contain threats more quickly and sustain confidence.

Safeguard stakeholder trust

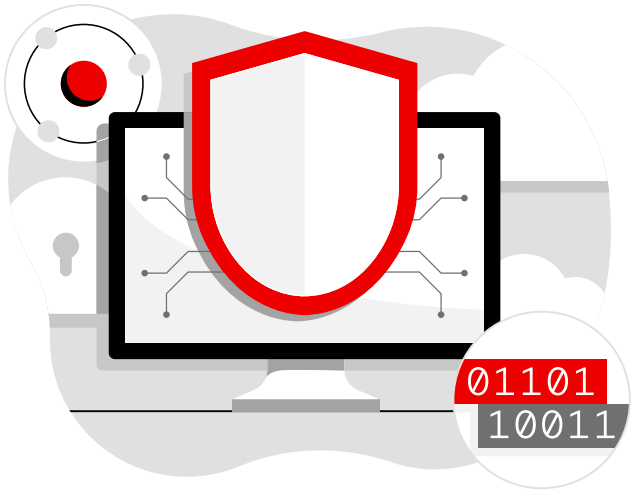
Automation can help implement policies and compliance standards the same way, every time, demonstrating sound governance and strengthening confidence among stakeholders.

Keep digital business moving

Automating monitoring and event-driven responses keeps systems resilient by identifying, isolating, and resolving issues before they cascade into larger disruptions.

Reduce audit time

Generating real-time, audit-ready reports and proof of compliance using automation allows teams to spend less time on documentation and more time on higher-value work.



A single, flexible automation platform that is capable of applying security and compliance measures helps reduce automation complexity across the enterprise. For example, a change in one area may effect another, and this is where tooling that can orchestrate an automated workflow and implement the changes at scale is needed.

This e-book explores how security automation can be infused across the entire operation, how businesses can accelerate threat response, and how best practices can be implemented for compliance, reporting, and governance.

[1] Gartner Press Release. "Gartner Survey Finds 85% of CEOs Say Cybersecurity is Critical for Business Growth." April 22, 2025.
GARTNER is a trademark of Gartner, Inc. and/or its affiliates.

Chapter 1

Security automation is foundational for cybersecurity and compliance

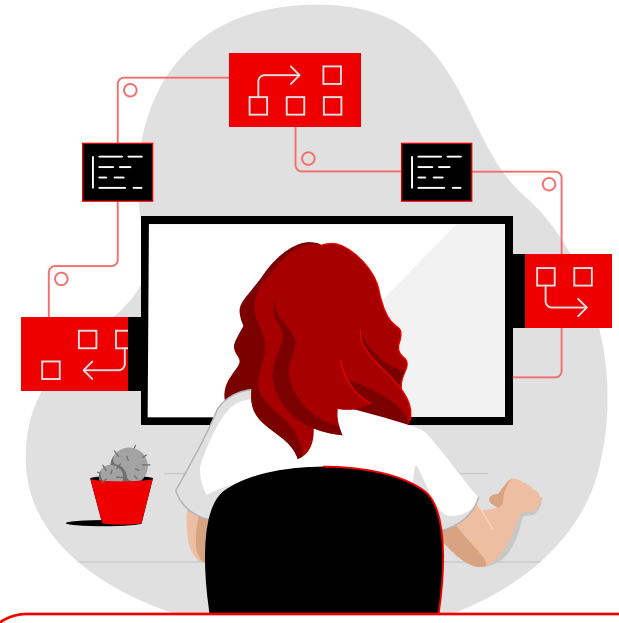
Once seen as an efficiency gain, automation is quickly becoming a foundational approach to modern cybersecurity.

This shift is redefining how teams safeguard systems, respond to incidents, and build resilience at scale.

What is security automation?

Security automation helps organizations scale their ability to enforce security policies, maintain compliance, reduce operational risk, and efficiently respond to security challenges across hybrid IT environments.

This involves automating the manual tasks associated with managing the security posture of your business. It consists of multiple practices, which can be divided into 5 general categories:



1 Automate security into operational workflows

Automating security into operational workflows makes sure every system, service, and environment is built with protection in place from the start.

Instead of relying on teams to manually apply checks, enroll tools, or validate baselines, automation embeds these steps directly into the workflows that power day-to-day operations.

It begins with defining an automated workflow that consistently performs essential security actions. These may include:

- Applying specific configurations.
- Validating baseline settings.
- Registering systems with monitoring or endpoint tools.
- Installing agents that automatically enroll new servers into security platforms.

Security automation also supports teams by making sure that security baselines are enforced continuously and uniformly. Whether validating system hardening requirements or making sure that required controls are in place, automation makes these checks consistent and repeatable.

When security automation is considered from the start, compliance requirements can also be integrated into the workflow. Through automation that embodies the relevant internal and external security and compliance policies, you can help make sure that systems operate within defined frameworks, such as Federal Information Processing Standards (FIPS) and other compliance standards without the additional burden of manual verification.

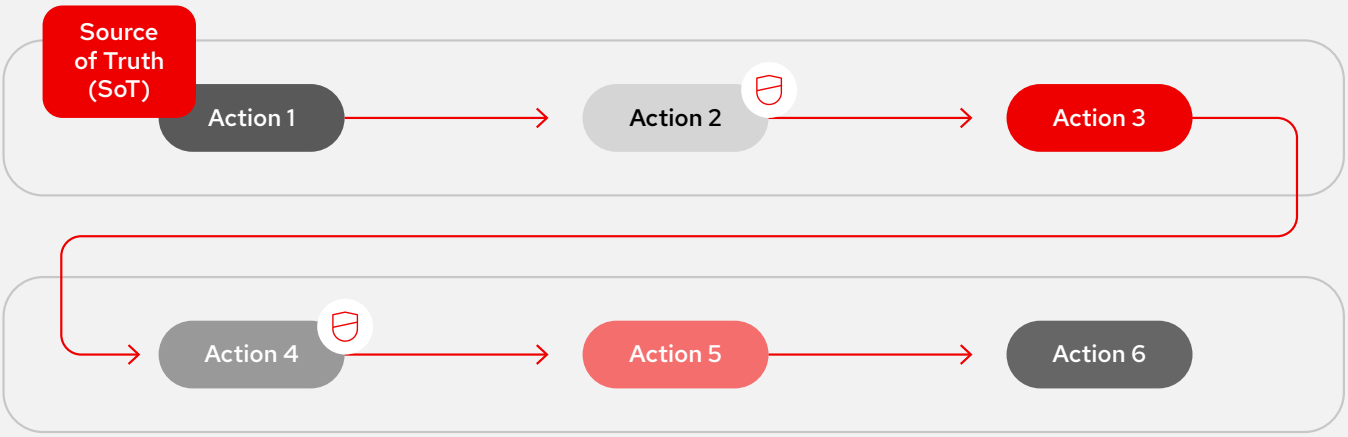


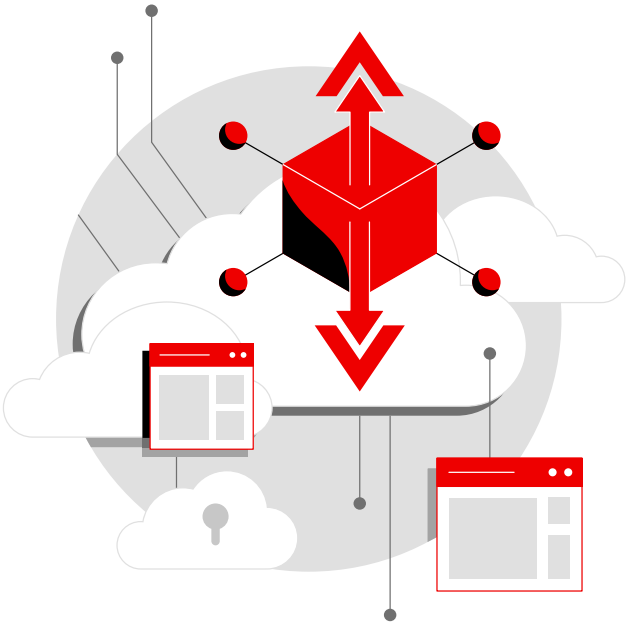
Figure 1: *Automated workflows can incorporate security and compliance steps into ITOps.*

2 Address vulnerabilities at scale

Every unpatched system is a potential vulnerability. In modern hybrid environments, even a single missed vulnerability can expose an organization to unnecessary risk.

Security automation helps eliminate that risk by integrating with vulnerability scanners or management systems such as Red Hat® Lightspeed, formerly Red Hat Insights. Dynamic inventories automatically generate and filter host lists, drawn from across your operation, to create a granular and current set of targets for automated action. This allows the organization to synchronize across changing infrastructure so that you can deploy patching and configuration management no matter where target resources such as applications, servers, networks, virtual machines (VMs), or cloud instances are located.

Instead of manually gathering lists or relying on out-of-date configuration management database (CMDB) entries, automation continuously identifies assets and keeps inventories current. This means teams can act with confidence, knowing they're comprehensively addressing affected systems, not just the ones that surfaced through manual checks. The result is more accurate updating with fewer gaps that can potentially create risks.



Automation enhances the full patching lifecycle

By combining dynamic inventory with automation designed around sources of truth that embody your security and compliance policies and baselines, organizations can patch consistently, validate compliance quickly, and remediate vulnerabilities at scale. This reduces exposure, speeds up response, and frees teams to focus on higher-value initiatives—from new innovations to more advanced security capabilities to better resilience.

Automation workflows are flexible and you can design the end-to-end automated process that meets your needs.

Here is an example of how you can structure an automated workflow to apply a patch at scale:

Before patching

Using automation playbooks at this stage, you can capture snapshots or backups to reduce the risk of unintended disruption. Red Hat Ansible® Automation Platform can gather facts and create prepatch infrastructure visibility reports for your teams to view compliance status and patching levels. These reports provide valuable information to help build the right playbooks to address concerns at scale.

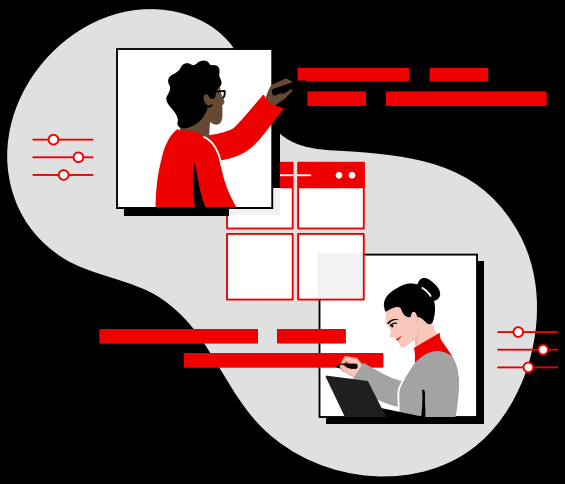
Applying a patch

By using dynamic inventories or creating an inventory of affected systems programmatically, you have a comprehensive list of systems or resources that require patching.

An automation playbook can target this inventory to apply the patch and thus you can complete patching in less time and at scale.

After patching

Automated reports can also validate that patches were successfully applied, update the CMDB or IT service management (ITSM) system, generate compliance or audit reports, and automatically close tickets—all without manual intervention.

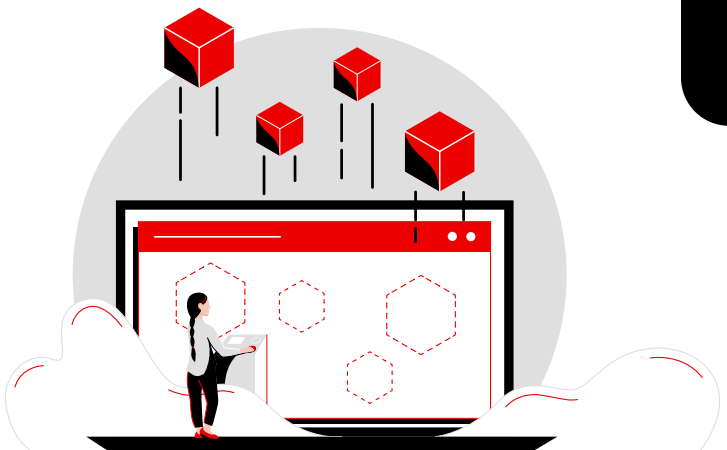


How a stock exchange reduced trading time to seconds

Bolsas y Mercados Argentinos (BYMA), an Argentine Stock Exchange, offers security-focused and transparent access to various investments for institutions, companies, and the general public. To safeguard against emerging threats and vulnerabilities, BYMA set out to reduce operating system (OS) configuration time, improve user access and administration, and automate vulnerability remediation.

Using Ansible Automation Platform, BYMA reduced key administration tasks from minutes to seconds and improved both Log4j vulnerability remediation and its overall security posture.

Read the BYMA case study



3 Automate security into application development

To safeguard modern applications, security must be built into the application development process before it reaches production. Security automation streamlines the process by embedding protection into every stage of the development lifecycle—from creating code to testing to deploying it at scale, as demonstrated in figure 2.

Automated workflows can provision compliant development and test environments. They can also enforce configuration baselines, apply patches, and orchestrate security testing, including static application security testing (SAST) directly within continuous integration and continuous delivery (CI/CD) pipelines.

Secrets management further strengthens this process by protecting sensitive data and allowing certificate rotation at scale, without exposing keys, passwords, or credentials.

Policy enforcement can be used to control what automation does, such as to prevent a mismatch of resources from being used, for example automation intended for development inventory that is attempting to run on production inventory.

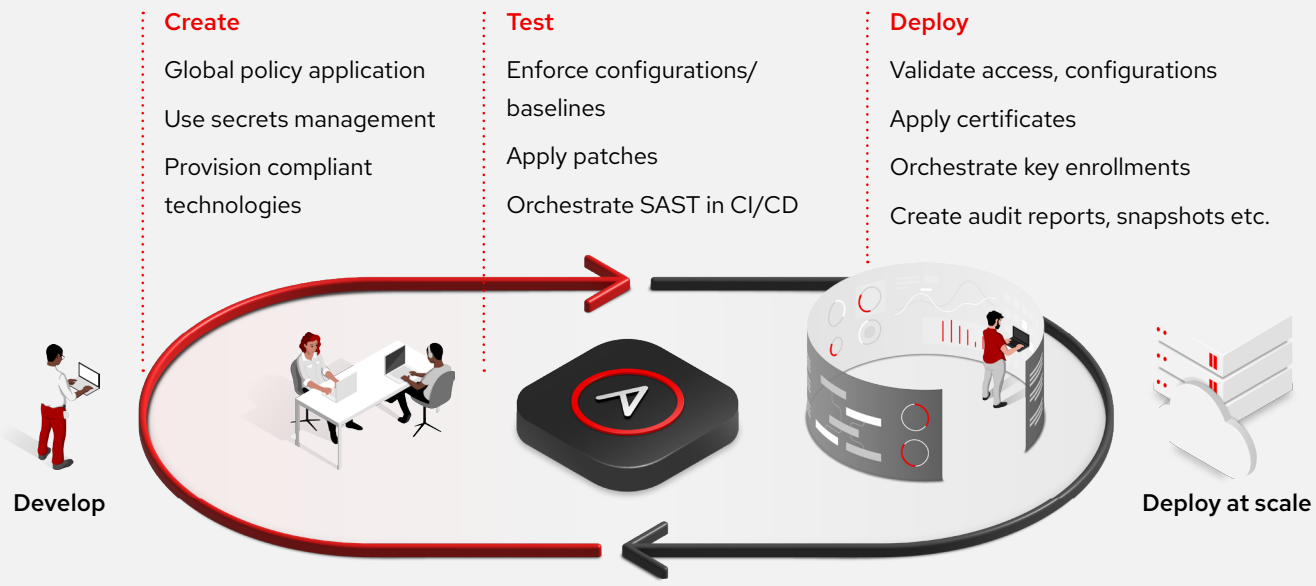
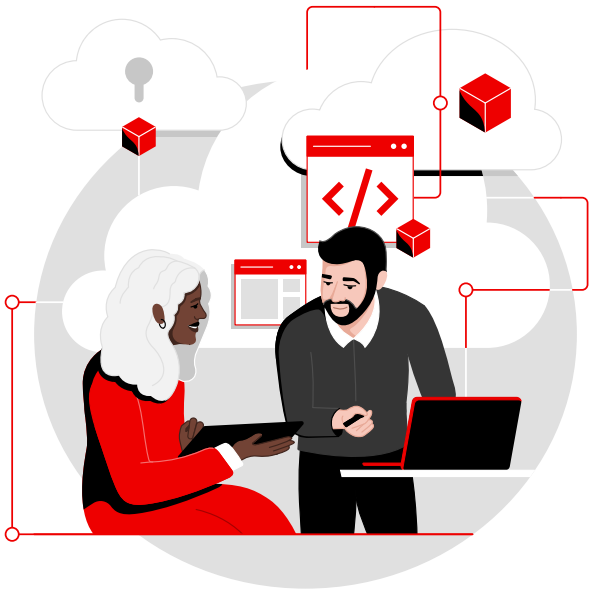


Figure 2: Build security and compliance into application development throughout the process, from development to test to production.



4 Provide benefits for already busy IT teams

By embedding security tasks directly into operational workflows, protection becomes standardized and consistent.

For security teams, this instills greater confidence in the organization's overall security posture.

For IT teams, automation makes it easier to implement security requirements without slowing down delivery or adding procedural overhead.

Event-driven automation takes this a step further. When drift occurs, automated workflows can trigger immediate action or create notifications, reapply source-of-truth configurations, and/or update a CMDB. You define which events matter and how the system should respond.

The result is a consistent, resilient, and efficient security posture delivered without adding more work to already over extended teams.

5 Start small, think big

Security automation doesn't require a massive overhaul on Day 1. The most successful teams begin with a single playbook—automating 1 repeatable task, 1 security check, or 1 compliance step. Over time, these individual playbooks can be stitched together into larger, end-to-end workflows that automate entire security processes.

This incremental approach helps teams scale automation at the pace that fits their needs and maturity, while still advancing toward their long-term vision.

Adopt a zero-trust approach

Zero trust is an approach to designing security architectures based on the premise that every interaction begins in an untrusted state. Instead of security focusing on fortifying the perimeter, a zero-trust approach incorporates security measures at all levels across the organizations while adhering to a **never trust, always verify** approach.

Automation helps when you are adopting zero trust by applying security controls to any part of your operation. You can apply policies, open and close access points, enroll required monitoring tooling for key resources and create audit trails and reports.

Red Hat Ansible Automation Platform modes of operation

Ansible Automation Platform offers multiple ways to run automation, giving teams the flexibility to address both predictable operational needs and fast-moving, real-time events as they occur. Whether you're executing planned changes at scale or responding instantly to shifts in your environment, Ansible Automation Platform provides a consistent, reliable foundation for response.

Planned automation

Using standard playbooks designed for expected or scheduled work, playbook-driven automation lets teams roll out changes at scale with precision. From provisioning and configuration to patching, updates, and compliance enforcement, teams gain a foundation for predictable, repeatable operations which can be scheduled as desired.

Event-driven response

As a part of an Ansible Automation Platform subscription, Event-Driven Ansible provides the event-handling capability needed to automate response to changing conditions in any IT domain.

Event-Driven Ansible automatically reacts to changing conditions as identified by external event sources such as observability tools, allowing for rapid, rule-driven decisions. Its flexible architecture supports webhooks, Event Streams, and Kafka, making it easier to connect with monitoring and observability systems, security tools, and custom event sources to trigger the right automation at the right moment.

Event-Driven Ansible receives an alert, completes a rules-based decisioning process and takes the desired action. You select the alerts and specify every aspect of the response including the rules and the action to be taken when the conditions in the rules are met.

Ansible Automation Platform helps teams coordinate tasks across teams and solutions to build a more efficient approach to security operations.

Chapter 2

Accelerate threat response

Modern teams need to outpace threats and must neutralize or remediate these threats as quickly as possible. What if you could respond to alerts automatically?

Ansible Automation Platform helps make this possible through its included Event-Driven Ansible capability, combined with the full breadth of automation features of the platform. It gives teams the power to apply patches, enforce baselines, and update controls consistently across thousands of systems. By working with event-driven automation, Ansible Automation Platform helps IT and security teams respond in real time by accelerating fact gathering without manual steps, and allowing for consistent, automated actions across known and unknown threat scenarios.

For known threats, site-reliability engineers (SREs) can design rulebooks that act in the desired way, whether it's renewing certificates, disabling suspicious activity, or enhancing tickets by gathering facts automatically to accelerate resolution.

For unknown threats, IT teams can proactively scan for risks such as untagged cloud resources or excessive privileges. You can design automation to handle the discovery, ticket creation, and corrective steps, making resolution scalable yet less complex.

Threat response for IT teams

For IT teams, delays often come from gathering facts and routing alerts. You can use Event-Driven Ansible to remove this challenge by automatically collecting system data the moment an alert appears–without delay–then include the facts in a service ticket for accelerated resolution.

Organizations that pair SRE and security team collaboration with automated response show 54% faster MTTR and more consistent remediation outcomes.[2]

[2] Splunk research. "State of Observability 2025." 2025.

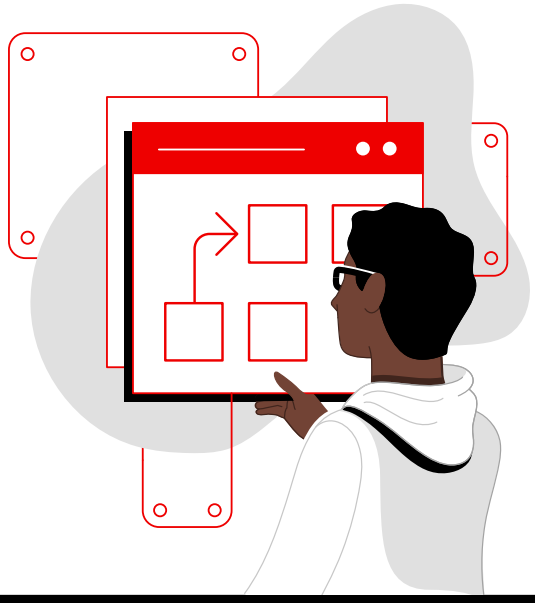
Threat response for security teams

When it comes to risks, security teams depend on fast visibility and coordinated response. Event-Driven Ansible can be integrated with existing security and observability tools to initiate automated forensics, validate root causes, and, when necessary, quarantine processes or traffic in real time in any domain or across domains.

For known threats, speed is essential. With Event-Driven Ansible, alerts immediately trigger fact gathering and predefined responses, reducing mean time to resolution (MTTR). Teams can also use AIOps capabilities to assist in resolving the issue—further accelerating response while reducing manual lift.

For unknown threats, proactive action is a prudent step. Using automation, teams can continuously scan for exposures such as misconfigurations, privilege escalations, or unsecured cloud resources. Event-Driven Ansible triggers investigations based on events, while Ansible Automation Platform performs targeted scans and applies remediations across large, dynamic inventories.

For example, security teams may receive an alert of escalated privileges and automate an event-driven response to both gather facts, redirect system logging to a SIEM for investigation and disable the service or user. Should the root cause be a configuration error, Ansible can apply the Source of Truth configuration at scale to resolve all affected hosts.



By automating everything from detection to corrective action, organizations can close vulnerabilities early, before they escalate into incidents or disruptions that affect business.

Chapter 3

Implement and maintain compliance

As compliance requirements expand rapidly, keeping up with them across hybrid, multicloud, and distributed environments can be overwhelming for any team.

Security automation helps organizations consistently meet these obligations by enforcing baselines, detecting technology drift, and remediating issues before they become audit concerns.

A single source of truth

Ansible Automation Platform allows organizations to define single-source of truth (SoT) configurations and security baselines that represent the controls, standards, and regulatory requirements that matter most. These baselines can be applied during provisioning, used for continuous drift detection, and reused across environments, making sure that systems remain compliant with internal and external policies with less manual effort.

Dynamic inventory

Compliance management is further strengthened via dynamic inventory. By continuously identifying and updating all systems in your environment—including cloud instances, VMs, servers, network devices, applications, and edge endpoints—you always know exactly which resources are affected by a compliance update. This eliminates missed targets and positions teams to enter audits with confidence and complete visibility.

Event-Driven Ansible automation

Event-Driven Ansible adds another layer of protection by working with your event sources to notify teams when a compliance issue occurs, such as an expired certificate or the need for additional compliance checks. Teams can respond with certificate rotation, run compliance scans and more. It gives you both speed and control.

Hardening

A key component of compliance is hardening, which refers to configuring systems, VMs, applications, cloud services, and networks and edge devices to reduce the attack surface.

Automation streamlines these tasks by validating patches, detecting unauthorized APIs, checking access controls, encrypting sensitive data, and orchestrating secrets or applying identity-management requirements.

For example, an out of compliance network configuration that could potentially create an opening for a threat to occur. This can be managed with a fully-automated response that reapplies the source of truth configuration.

Compliance reporting

Audit and compliance reporting is another area where automation delivers value. Ansible Automation Platform generates both full audit trails of automated actions taken and provides accelerated, flexible reporting across systems and domains.

Using playbooks, teams can create the reports they need, from configuration drift reports to patch status reports to OpenSCAP compliance scans to change histories or targeted gap assessments, without disrupting operations or manually gathering data.

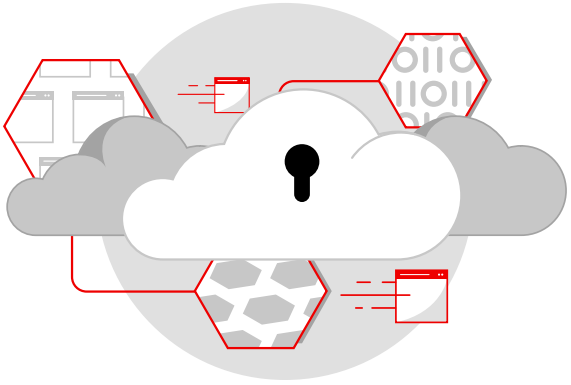
Security automation in national defense

The Defense Information Systems Agency (DISA) has transformed DODNet operations by introducing enhanced network management and increased automation. Using Ansible Automation Platform for intelligent automation playbooks, DISA has streamlined provisioning, configuration management, and patching to support mission-critical communications and stringent defense compliance requirements.[3]

Laying the groundwork for the future

Security automation lays the groundwork for AIOps and automated management of AI infrastructure. Without consistent governance, orchestrated workflows, and reliable data, AI has the potential to amplify a threat and automation keeps it aligned.

IT automation is therefore critical, not just for today's compliance and risk management needs, but for preparing organizations to adopt AI effectively in the next wave of transformation.



[3] Ferris, Michelle. "DISA transforms DODNet operations to drive efficiency." United States Government News, 11 Jun. 2025.

Chapter 4

Security and compliance across the organization

Implementing automation in any area of your organization does not happen instantly, and it's not an all-or-nothing proposition.

Security automation is a journey. Each organization will start and stop at different points according to their needs. Those needs will also dictate the path that each organization takes. No matter where you are in your journey, even small security automation efforts can deliver benefits.

How Red Hat can help advance your journey

Ansible Automation Platform can serve as an integration layer between your security and IT teams, tools, and processes to extend your security automation capabilities.

A flexible, interoperable platform helps organizations:

- Connect security teams, ITOps, and DevOps with systems, processes, and tools.
- Automate team actions by building in security from the start.
- Integrate toolchains on both the security and operational sides.
- Take automated event-driven actions, by integrating with event sources such as observability and monitoring tools.
- Collect information from systems and direct it to predefined systems and locations efficiently and without manual intervention.
- Change and propagate configurations with ease from centralized interfaces.

Advanced communications and collaboration

Using a consistent automation platform and common language across the organization can also improve communication and collaboration. When using a single language and automation tool, teams can better collaborate to perform required security and compliance actions in a fraction of the time, while making sure there is consistency and accuracy so you can enhance your overall security posture.

- Privileged access management (PAM)
- Intrusion detection and prevention systems (IDPS)
- Secure web gateways
- Enterprise firewalls
- Endpoint protection platforms
- Security information and event management (SIEM)
- Threat intelligence platforms
- Secure email gateways

Figure 3. An automation platform can connect your security systems, tools, and teams.

An automation platform for the whole organization

There are many automation solutions available, but not all include the capabilities needed for effective security automation. Look for automation platforms that offer:

A universal, accessible automation language

A language that is easier to understand and write allows you to document and share information between security team members with different domain expertise.

A modular and extensible design

A modular platform allows organizations to deploy automation in steps. Extensibility helps to accommodate additional and future security tools as needed.

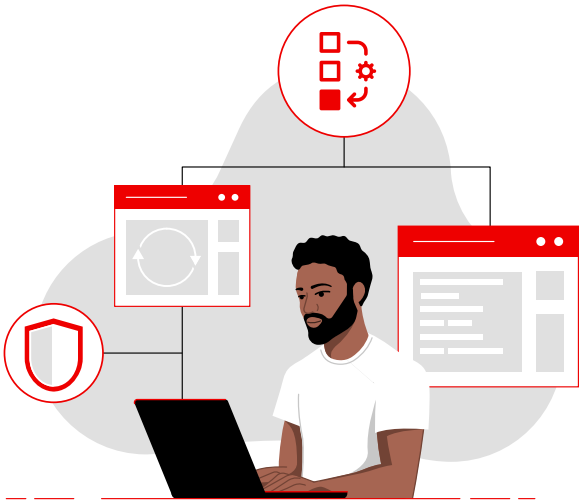
Move your security organization forward with Ansible Automation Platform

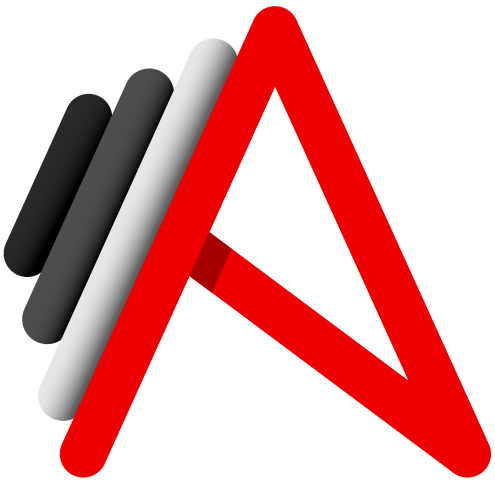
A foundation for building and operating automation services at scale, Ansible Automation Platform delivers all the tools and features you need to implement security automation. It combines a straightforward, readable automation language with a trusted, composable execution environment and security-focused sharing and collaboration capabilities.

Its open foundation allows organizations to connect and automate almost anything you need across your IT infrastructure and security operation, creating a common platform for participation and sharing across the entire organization.

Equipped with a set of security-focused Ansible automation content to coordinate the activity of multiple types of security solutions for a more unified response to cyberthreats and security operations.

Ansible Automation Platform also includes tools and capabilities to help organizations optimize automation. This includes both the automation dashboard and automation analytics, which together provide insight into how automation is used across an organization as well as return of investment (ROI) and benefits from automation.





Ansible automation hub lets team members access certified automation content through a centralized repository. A rich set of content collections are available to help customers jumpstart automation projects for the multivendor technologies in their environment. Customers can also create custom content that supports digital signing to establish chain of custody and confirm no unauthorized changes have occurred. Policy enforcement further allows control over what automation can do, for example who can run automation on which inventory. Together, all of this means you can operate automation with more confidence.

And the included Ansible Content Collections streamline the management, distribution, and consumption of automation assets. These are Red Hat certified or validated, signed and delivered in a convenient format. To streamline content creation and extend capabilities further, Ansible Automation Platform now includes AI-assisted support through Ansible Lightspeed. This AI service helps users create high-quality automation efficiently by offering intelligent code recommendations based on natural language prompts and can also provide knowledge to support ongoing IT operations.

Reports provide essential information. Automation reduces the time and effort required to create and distribute key data and insights. Together, security teams can operate with the information they need rather than the information they can get—drastically improving security posture.

Ansible Automation Platform delivers business value

A more efficient, streamlined way to automate your security operations helps organizations uncover business value. See figure 4.

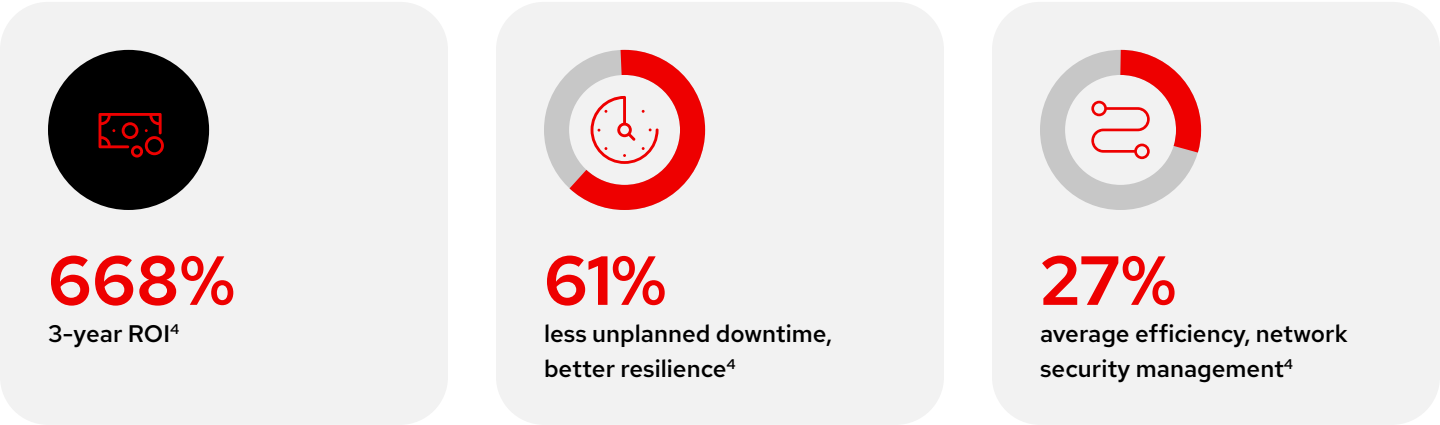


Figure 4: Insights from The business value of Red Hat Ansible Automation Platform report.[4]

An automation platform can support an organization's core business priorities, including:

Reduced enterprise risk
Automate configuration hardening and continuous policy enforcement across hybrid cloud environments.

Unified security and ITOps teams
Automate across security and IT teams with a common automation framework for a coordinated defense.

Accelerated threat response
Automation alert processing, data enrichment, and critical remediation actions.

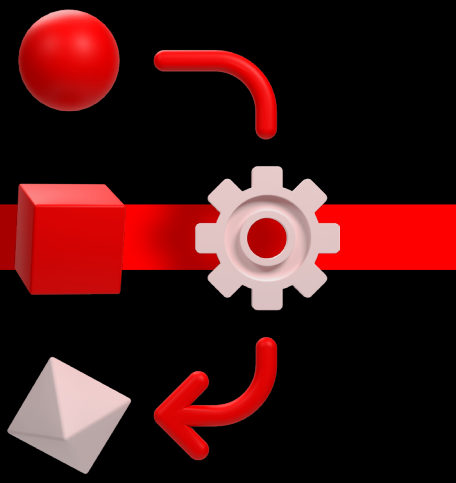
Improved security and compliance
Automate continually for evidence gathering and posture assessments against security benchmarks.

> **We chose Red Hat Ansible Automation Platform because we can achieve efficiency and productivity through better controls, fewer mistakes, and the scaling and automation.**[4]
>
> Red Hat telecommunications customer

[4] IDC White Paper, sponsored by Red Hat. "The business value of Red Hat Ansible Automation Platform." Document #US51839824, Mar. 2024.

Learn more

Get started with security and compliance for ITOps



Security automation can help identify and respond to growing security threats more quickly and at scale.

Red Hat helps safeguard the organization by connecting security teams, tools, and processes with a consistent, collaborative automation platform.

Discover how Ansible Automation Platform connects the entire organization in The automated enterprise e-book.

Learn how to automate security with Red Hat Ansible Automation Platform.

Explore security for your hybrid cloud. Read the Boost hybrid cloud security e-book.

Read the use case, Security automation with Red Hat Ansible Automation Platform.

Speak with a Red Hatter about taking the next step in your security automation journey.