

/Keep your options open



# **Simplify** your security operations center

Prioritize efficiency and security with a unified automation platform

# See what's inside

Page 1

IT security is a top concern

Page 2

What is security automation?

Page 3

Automation integrates your security tools, systems, and processes

Page 4

Security automation is a journey

Page 5

Use cases and integrations: Define your path to security automation

Page 7

Simplify your security operations center with Red Hat Ansible Automation Platform

Page 9

Automation in action: Red Hat Ansible Automation Platform delivers proven business value

Page 10

Ready to simplify your security operations center?



# IT security is a top concern



Security is a leading issue for most organizations, and many CEOs are concerned about cyber threats. This apprehension is not unfounded: 70% of organizations that have experienced a security breach report a significant or very significant disruption to business as a result.<sup>1</sup>

Protecting your organization is a critical—but frequently daunting—task. Security teams must assemble, maintain, manage, and adapt complex environments using multiple tools and services from a variety of often-competing vendors. The quantity of offerings increases each year, so teams must continually research, assess, and integrate new products as the security landscape changes.

Additionally, the severity and cost of security breaches continue to grow. Costs from lost business and post-breach response in 2024 rose nearly 11% over the previous year.<sup>1</sup> And the average cost of a data breach jumped to US\$4.88 million in 2024, up from US\$4.45 million in 2023.<sup>1</sup>

Security-related tasks can be time-consuming, tedious, and error-prone when human intervention is required. Security teams are overwhelmed and understaffed, with the number of organizations facing a critical lack of skilled security workers rising to 53% in 2024, compared to 42% in 2023.<sup>1</sup> The average cost of breaches associated with a high-level shortage of security skills jumped to US\$5.74 million in 2024 from US\$5.36 million in 2023, a 7.1% increase.<sup>1</sup>

However, implementation of automation and AI-based solutions is on the rise. The number of organizations that use security AI and automation extensively grew to 31% in 2024.<sup>1</sup> Wherever AI and automation are applied, they accelerate the work of identifying and containing breaches. Extensive use of AI and automation in key security areas—prevention, detection, investigation, and response—reduced the average time to identify and contain data breaches by 33% for response and 43% for prevention in 2024.<sup>1</sup> Extensive automation and AI usage are also shown to dramatically lower average breach costs when compared to organizations that don't use these technologies in key security areas.<sup>1</sup>



## Impacts of ineffective security

The number, severity, and cost of security breaches continue to grow.

**US\$4.88 million**

The global average cost of a data breach in 2024<sup>1</sup>

**26.2%**

Growth of the cyber skills shortage<sup>1</sup>

**1 in 3**

Share of breaches involving shadow data<sup>1</sup>

**292**

Days to identify and contain breaches involving stolen credentials<sup>1</sup>

**46%**

Share of breaches involving customer personal data<sup>1</sup>

**US\$4.99 million**

Average cost of a malicious insider attack<sup>1</sup>

<sup>1</sup>"Cost of a Data Breach Report 2024," IBM, accessed 31 July 2024.

# What is **security automation?**

Security automation involves automating the manual tasks associated with maintaining the security posture of your business. It consists of multiple practices, which can be divided into 4 general categories:



## Response and remediation

Event-driven activities that involve security analyst participation, guidance, or both.



## Security operations

Day-to-day process- and policy-driven activities performed on your security infrastructure by technology teams.



## Security compliance

Activities to ensure infrastructure is compliant with security policies and regulations.



## Hardening

Activities to apply custom security policies to infrastructure with the targeted intent and goals.

This e-book focuses on automating response and remediation activities and security operations.

## Benefits of AI and automation for security operations, response, and remediation activities



### Boost speed and efficiency

Automation streamlines tasks and removes the need for manual intervention, accelerating security operations and allowing staff to refocus on high-value initiatives. Organizations extensively using security AI and automation identified and contained data breaches nearly 100 days faster on average than organizations that didn't use these technologies at all.<sup>1</sup>



### Increase security at scale

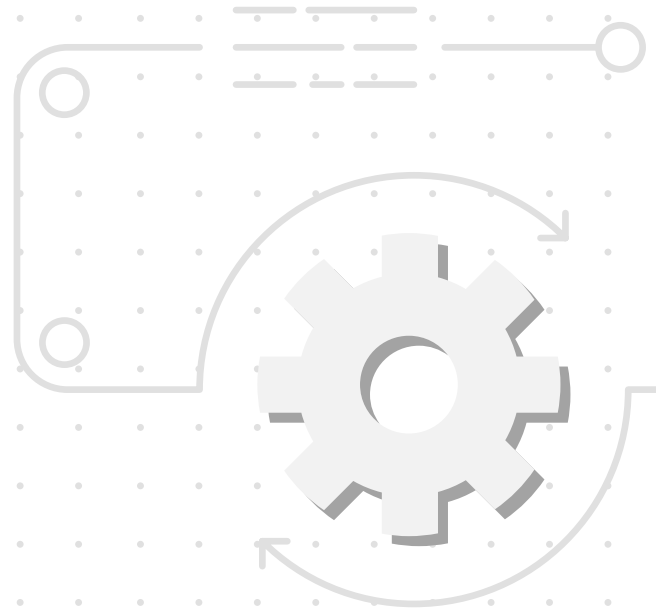
Applying automation across your security infrastructure increases consistency and allows you to take a more holistic approach to security. Each staff member can manage more tools, devices, and systems, so you can operate at scale. Automation also reduces the risk of human errors, improving accuracy.



### Reduce the risk and cost of breaches

Organizations not using AI and automation had average costs of US\$5.72 million, while those making extensive use of AI and automation had average costs of US\$3.84 million, a savings of US\$1.88 million.<sup>1</sup> Correspondingly, the use of AI and automation is on the rise: The number of organizations that used security AI and automation grew to 31% in this year's study from 28% in 2023.

<sup>1</sup>"[Cost of a Data Breach Report 2024](#)," IBM, accessed 31 July 2024.



## Learn more about security compliance and hardening

Discover how automation can help security compliance and hardening by reading these resources:

- [Boost hybrid cloud security e-book](#)
- [Enhance security with automation: A Red Hat customer success series](#)
- [Use case: Security automation with Red Hat Ansible Automation Platform](#)

# Automation integrates your security tools, systems, and processes

## Unite people, processes, and tools with a consistent, flexible platform

An automation platform can serve as an integration layer between your security teams, tools, and processes. A flexible, interoperable platform lets you:

- Connect your security systems, tools, and teams.
- 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.
- Create, maintain, and access custom automation content related to your security tools and processes.
- Trigger automated actions across multiple security tools when a threat is detected.

Using a consistent automation platform and language across your organization can also improve communication and collaboration. When every solution in a security portfolio is automated through the same language, both analysts and operators can perform a series of actions across products in a fraction of the time, maximizing the overall efficiency of the security team. And a common framework and language lets security and IT teams share designs, processes, and ideas more easily, both internally and across your organization.

## Automation success = people + processes + platform

Maximizing the value of automation requires more than just a tool—you also need to consider your people, processes, and platform.

- **People** are at the core of any business initiative. Participation within and across teams lets staff share ideas and collaborate more effectively.
- **Processes** move projects within your organization from start to finish. Clear, documented processes are essential for effective automation.
- An automation **platform** provides the capabilities for building, running, and managing your automation assets. In contrast to simple automation tools, an automation platform gives your organization a unified foundation for creating, deploying, and sharing consistent automation content and knowledge at scale.

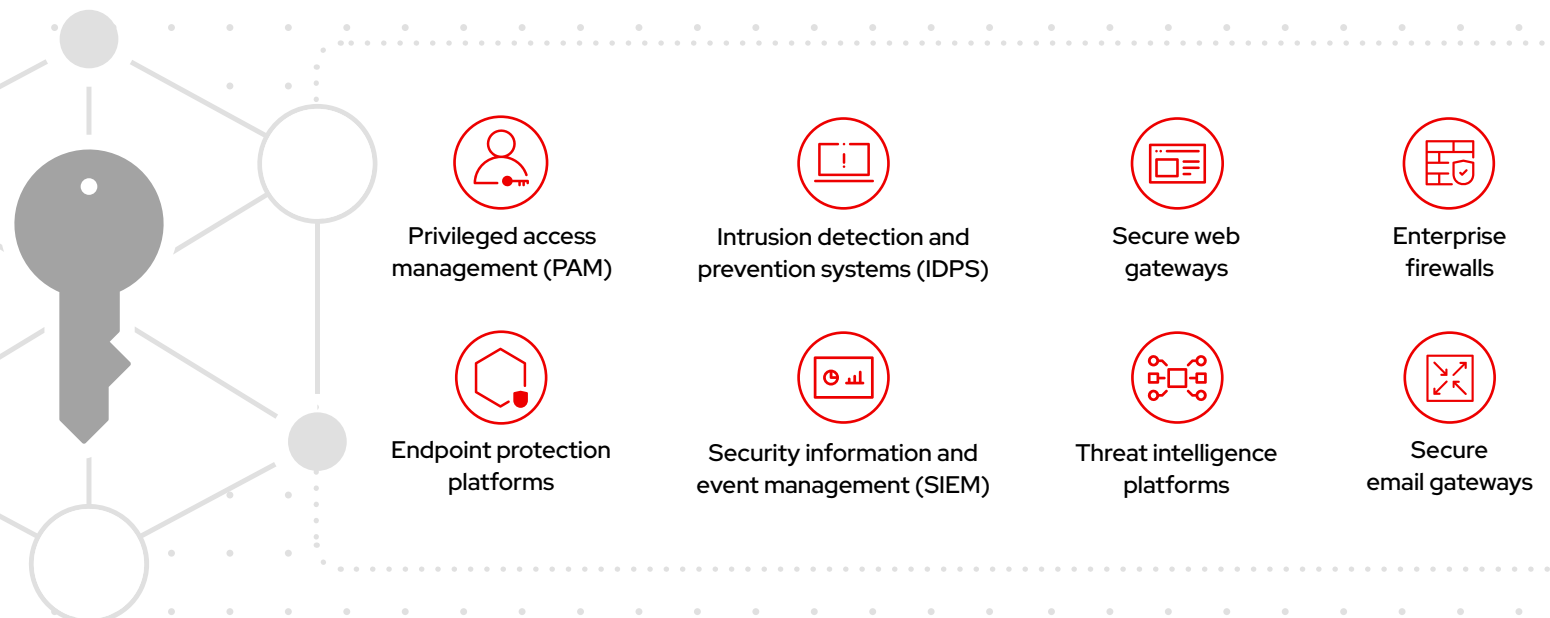


Figure 1. An automation platform can connect your security systems, tools, and teams.

# Security automation is a journey

Implementing automation in any area of your organization does not happen instantly, and it is 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. Even so, no matter where you are in your journey, even small security automation efforts can deliver benefits.

## Assess your security automation maturity level

Most organizations fall into one of 3 main stages of security automation maturity. Determining your organization's current stage will help you adopt the right tools and processes at the right time to make your automation journey more successful.

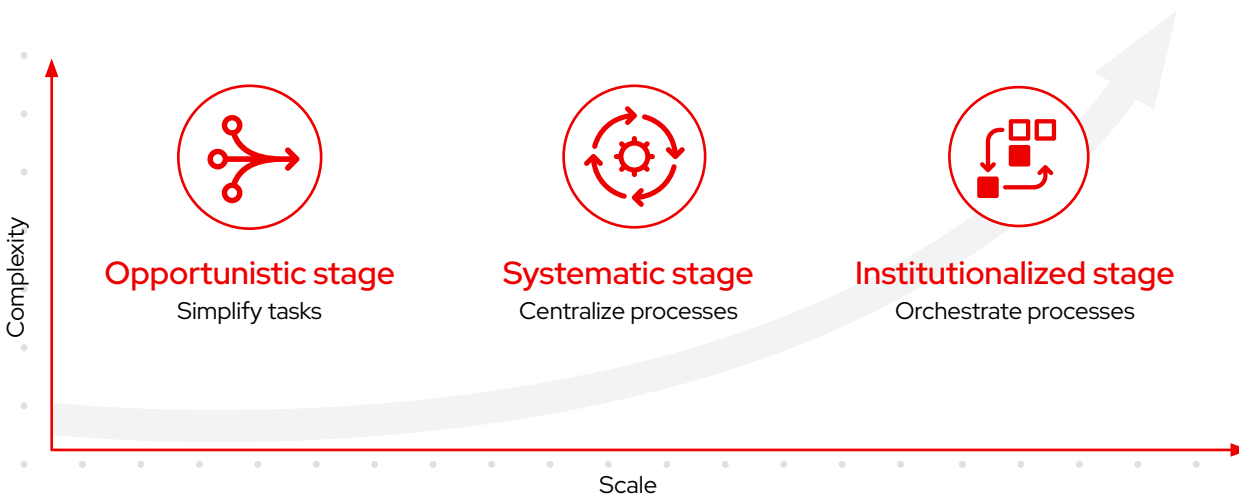


Figure 2. Stages of security automation maturity



## Stage 1: Opportunistic

This stage focuses on saving time by automating security operations. Common goals include standardizing security actions across similar devices and technologies and streamlining manual tasks performed across products from different vendors.



## Stage 2: Systematic

This stage focuses on improving processes and efficiency by adopting a cohesive set of security operations tools and services. Common goals include building security processes into higher-level workflows and centralizing security response processes.



## Stage 3: Institutionalized

This stage focuses on boosting collaboration and integrating security across your organization. Common goals include creating automated, programmatic workflows that span all aspects of security and integrating your security and IT technologies.

# Define your path to security automation

## Common, high-level use cases for security automation

Each of these use cases can serve as a starting point for your security automation journey. The key is to start small and simple, and build over time.

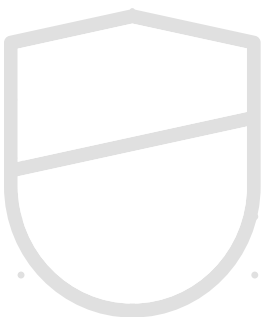


### Investigation enrichment

Investigating security alerts and incidents involves collecting information from a variety of security systems to assess whether a legitimate event has occurred. Information is typically gathered through a series of user interfaces, emails, and phone calls. This inefficient process can delay action against threats, leaving your business vulnerable and increasing the potential costs associated with a breach. Automation allows you to programmatically assemble information across your security systems, supporting on-demand enrichment of triage activities performed through security information and event management (SIEM) systems. As a result, you can assess—and respond to—alerts and incidents more efficiently.

### Threat hunting

Threat hunting involves identifying and investigating potential threats to security in a proactive fashion. As with incident investigation, staff manually gather and send information between many systems. Using automation, you can customize and streamline alerts, correlation searches, and signature manipulation to swiftly examine potential threats. You can also automatically create and update SIEM correlation queries and intrusion detection system (IDS) rules to improve detection. Consequently, you can update your organization's security defenses more frequently and efficiently to better protect your business.



### Incident response

Incident response involves taking action to stop a breach from continuing. Once a breach is discovered, security staff must respond quickly and at scale to contain it. However, response actions often include multiple manual tasks, slowing remediation time and leaving your organization vulnerable for longer. Automation helps you react faster by codifying actions into repeatable, preapproved playbooks. You can speed tasks like blocking attacking IP addresses or domains, allowing non-threatening traffic, freezing compromised credentials, and isolating suspicious workloads for further investigation to minimize the damage associated with the incident.

## Integration is essential

Unified automation approaches require integration between your automation platform and your security technologies. Essential integrations include:



**Firewalls** control traffic flow between networks, protecting internet-exposed applications. Automation can speed policy and log configuration changes.



**Intrusion detection and prevention systems (IDPS)** monitor network traffic for suspicious activity, issue threat alerts, and block attacks. Automation can simplify rule and log management.



**Security information and event management systems** collect and analyze security events to help detect and respond to threats. Automation can provide programmatic access to data sources.



**Privileged access management (PAM) tools** monitor and manage privileged accounts and access. Automation streamlines credential management.



**Endpoint protection systems** monitor and manage devices to improve their security. Automation can simplify common endpoint management tasks.



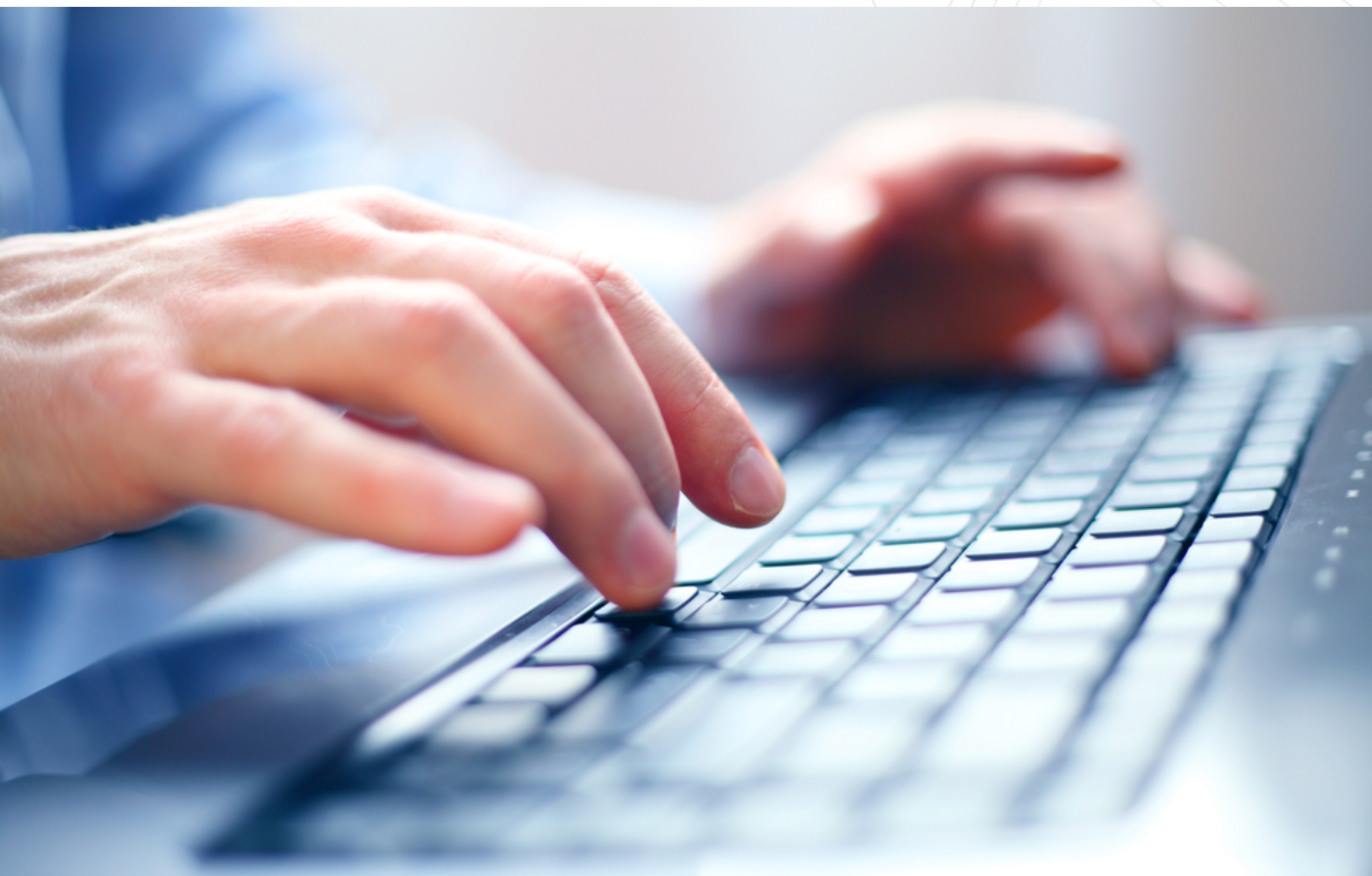
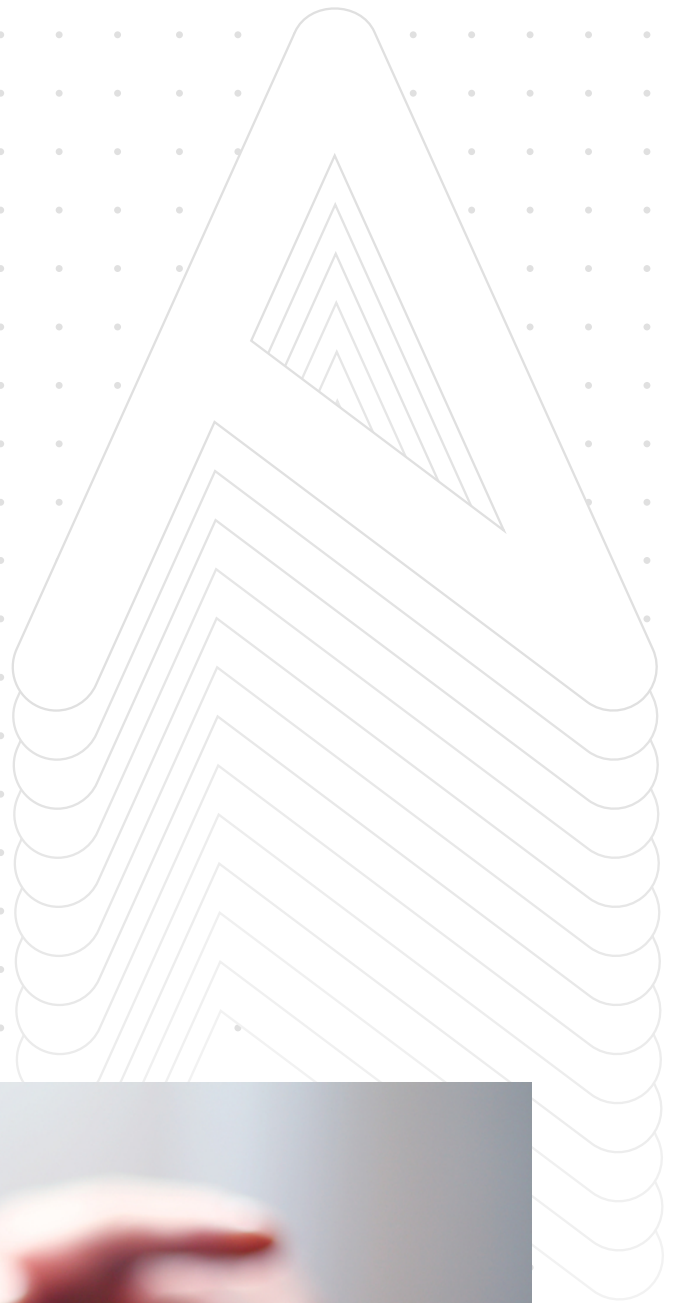


Simplify your security operations center

# with **Red Hat Ansible Automation Platform**

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 easy to understand and to write allows you to document and share information between security team members with different domain expertise.
- **An open and unbiased approach.**  
To be effective, your automation platform must interoperate with your entire security infrastructure and vendor ecosystem.
- **A modular and extensible design.**  
A modular platform allows you to deploy automation in steps. Extensibility helps you accommodate additional and future security tools from other vendors as needed.



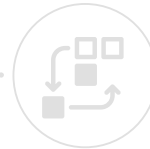
## Move your security organization forward with Red Hat

A foundation for building and operating automation services at scale, **Red Hat® Ansible® Automation Platform** delivers all the tools and features you need to implement security automation. It combines a simple, easy-to-read automation language with a trusted, composable execution environment and security-focused sharing and collaboration capabilities. An open foundation allows you to connect and automate almost everything in your security and IT infrastructure, creating a common platform for participation and sharing across your entire organization. Red Hat Ansible Automation Platform has also delivered proven outcomes in other areas, including IT and network operations and DevOps.

A supported set of **security-focused Ansible collections**—including modules, roles, and playbooks—is included with the platform. These assets coordinate the activity of multiple classes of security solutions for a more unified response to cyber threats and security operations:

- Chain workflows and playbooks for modular reusability.
- Consolidate and centralize logs.
- Support local directory services and access controls.
- Integrate external apps using RESTful application programming interfaces (APIs).

Red Hat Ansible Automation Platform also includes tools and capabilities to help you optimize your automation. **Automation Analytics** provides insight into how your organization uses automation. **Automation Hub** lets team members access certified automation content through a centralized repository. And **Content Collections** streamline the management, distribution, and consumption of automation assets.




### Get help from the experts

Red Hat can help you successfully deploy automation faster.

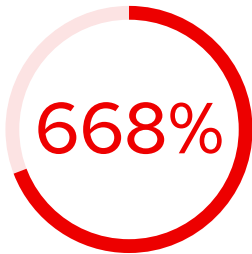
- **Red Hat Services Program: Automation Adoption** provides a framework for managing an organization-wide automation adoption journey.
- **Red Hat Training and Certification** offers hands-on training and practical certification to help you use automation more effectively.
- **Red Hat Support** works with you to ensure success on your IT journey. [Award-winning web support](#) gives you access to best practices, documentation, updates, and security alerts and patches. You can also connect with a support engineer or technical account manager to resolve issues and obtain specialized guidance.
- **Certified partner content collections** allow you to readily automate hardware and software from a broad selection of vendors. This trusted, prebuilt automation content is available through Ansible automation hub and is supported by both the partner and Red Hat.

Automation in action

# Red Hat Ansible Automation Platform delivers proven business value



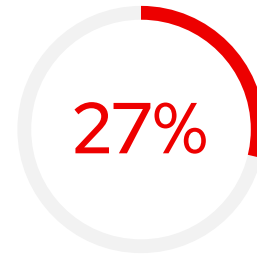
Red Hat Ansible Automation Platform provides a more efficient, streamlined way to automate your security operations center. Analyst studies of organizations that use Red Hat Ansible Automation Platform demonstrate measurable business value. In fact, IDC interviewed multiple decision makers about their experiences with Red Hat Ansible Automation Platform and found that study participants gained efficiencies for their IT teams, and enhanced agility and performance led to improved development and business results.





3-year ROI<sup>2</sup>



less unplanned downtime,  
better resilience<sup>2</sup>



average efficiency,  
network security  
management<sup>2</sup>

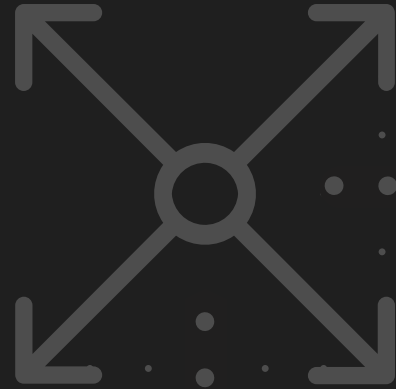


"We chose Red Hat Ansible Automation Platform because we can achieve efficiency and productivity through better controls, fewer mistakes, and the scaling and automation."<sup>2</sup>

<sup>2</sup> IDC White Paper, sponsored by Red Hat. "[The Business Value of Red Hat Ansible Automation Platform](#)." Document #US51839824, March 2024.

# Ready to simplify your security operations center ?

Automation can help you identify and respond to growing security threats faster and at scale. Red Hat helps you protect your business by connecting your security teams, tools, and processes with a consistent, collaborative automation platform.



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

[red.ht/automate-security](https://red.ht/automate-security)