Red Hat

Enhance security with automation

A Red Hat customer success series

Contents

Intro-duction

Automation is evolving security

The challenge to integrate IT security teams and solutions in a fast-paced environment is a requirement that every organization must solve for. And, while each approach to security is different, there are strategies that can be learned and adapted to help protect your valuable data, applications, IT systems, networks, and devices from malicious or unintended activities.

To help share these strategies, this e-book highlights 5 success stories from Red Hat® Ansible® Automation Platform customers that use automation to integrate and scale their security solutions to investigate and respond to threats across their organization in a coordinated and unified way.

How does automation enhance security?

Most organizations have a security team that knows what needs to be done, but configuring systems and applications manually, especially thousands of them, to protect against attackers takes more time and more skilled resources than is practical.

Automation can close this skills and resource gap by applying and enforcing security standards that adapt to meet internal and external security guidelines. The result is drastically reduced response times and decreased vulnerability.

> ***Organizations with fully deployed security AI and automation were able to detect and contain a breach much more quickly than organizations with no security AI and automation deployed.***
>
> IBM. "Cost of a Data Breach Report 2022." July 2022.

Ansible Automation Platform helps teams automate and integrate security solutions that can investigate and respond to threats across the enterprise in a coordinated and unified way using a curated collection of modules, roles, and playbooks.

What does a unified security approach include?

Security solutions are constantly evolving to stay one step ahead of security threats. Some key aspects to consider include:

Investigation enrichment

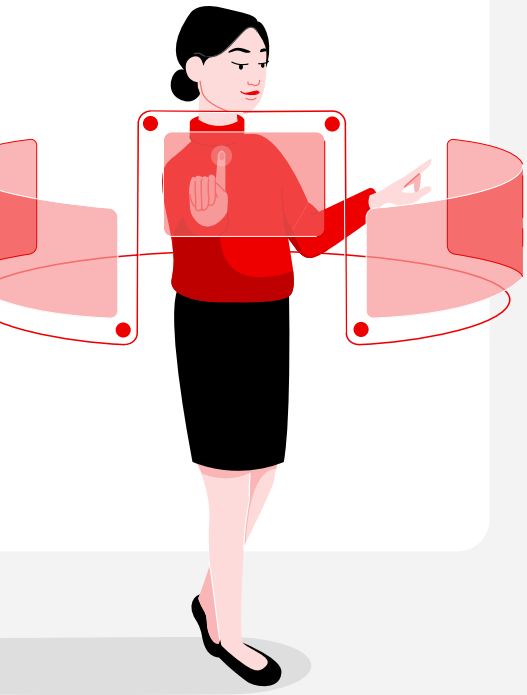
Collecting logs across firewalls, intrusion detection systems (IDS), and other security systems programmatically enable on-demand enrichment of triage activities performed through security information and event management systems (SIEMs).

Threat hunting

Automatically tune the level of logging and create new IDS rules and new firewall policies facilitating the detection of more threats in less time.

Incident response

Remediate faster-automating actions like blacklisting IP addresses or domains, whitelisting non-threatening traffic, or isolating suspicious workloads for further investigation.



Why choose Ansible for security automation?

Security is everybody's responsibility. Ansible is a powerful, agentless tool that makes automation accessible across the organization, from IT operations to development to network engineers to security teams because it delivers automation in a human-readable language. This allows organizations to do more with automation, including:

- Increase productivity. Ansible uses a simple human readable language so there's no need for specialized skills to code or manage to ensure tasks are executed in the proper order.
- Manage all IT infrastructure. Gain the ability to gather and audit information and stay on top of configuration management and workflow orchestration.
- Boost efficiency and security. An agentless architecture lets you deploy solutions more quickly without the vulnerability of agents to exploit or update.

The following success stories illustrate the power and scalability of automation for security, and how a unified automation platform, such as Ansible Automation Platform, helps organizations enhance their security posture.

1

EMORY UNIVERSITY

Emory University mitigates sudo threat with Red Hat Ansible Automation Platform

> *People didn't think we could patch Linux servers every 30 days, but with Red Hat Ansible Automation Platform it's possible and it's necessary.*
>
> Steve Siegelman, Manager of Systems Engineering, Office of Information Technology, Emory University

Emory University in Atlanta, Georgia is home to more than 15,000 students at its metro Atlanta campuses. With research ties to institutions around the globe and as the operator of Georgia's largest healthcare system, it's no surprise that the institution is a target for cyberattackers looking to exploit and gain access to confidential information through its digital footprint.

Once there's an entry through a vulnerability, the concern is the attacker would surreptitiously move throughout the network taking intellectual property and slipping away undetected. The school's Office of Information Technology (OIT) is tasked with maintaining systems for students, staff, faculty, researchers, and other stakeholders to ensure that networks and data are protected from unauthorized access and potential security breach. This is why there was such an alarm in January 2021 when the Red Hat team alerted OIT to a vulnerability within Emory's Red Hat Enterprise Linux® systems affecting the operating system's sudo utility.

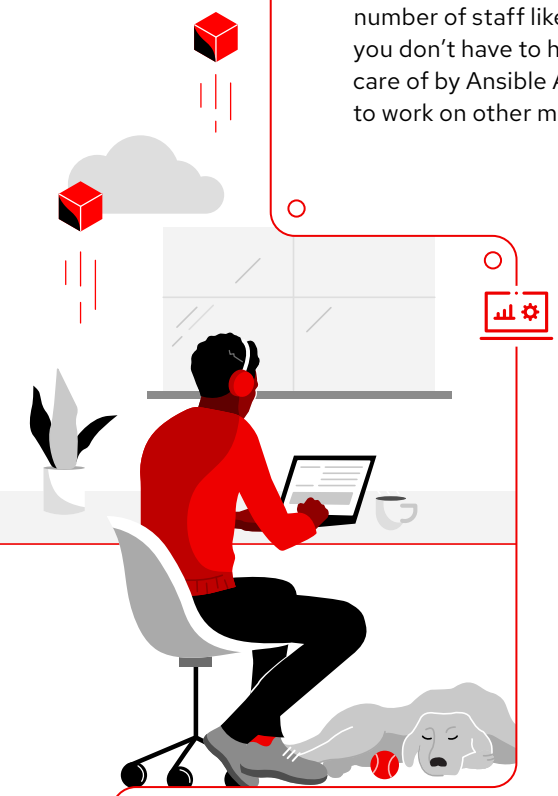
Ansible automation accelerates security risk remediation

Patched updates in hours not weeks

With more than 500 servers using Red Hat Enterprise Linux under their charge, the OIT knew they had a difficult road ahead if they had to install the patch manually, which would have put the university's infrastructure in danger. The solution was to use an Ansible Playbook to apply the patches automatically to each server. What would have taken up to two weeks to remediate across all servers took collectively four hours.

Freed valuable resources to focus on higher-value projects

Ansible Automation Platform was first used for Emory's financial systems before it was rolled out to the student and Human Resources systems. "We're pressed to do more with the same number of staff like many other organizations. And when you don't have to handle repetitive tasks that could be taken care of by Ansible Automation Platform, that frees people to work on other more critical projects," said Siegelman.



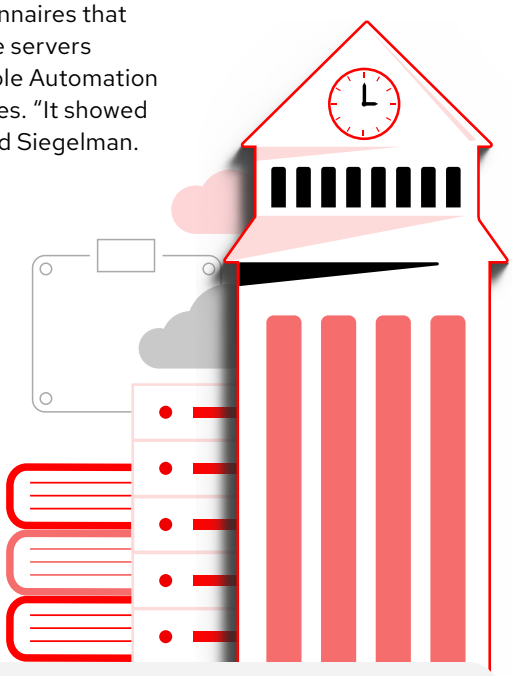
IT staff freed to focus on adapting to COVID-19 challenges

Another example of the Ansible Automation Platform's flexibility was in March 2020 when Emory, like nearly every school and organization, was forced to close its buildings and send students and staff to work from home.

OIT needed database servers to be quickly deployed in order to handle tracking essential employees for on-campus clearance. The selected staff filled out questionnaires that were fed into the system. Setting this up on the servers manually would have taken days, but with Ansible Automation Platform it was completed in a matter of minutes. "It showed what automation on the backend could do," said Siegelman.

Security innovation beyond the campus with automation

The need for automation is critical to Emory's plans moving forward, especially as it transitions to the cloud. "We have some legacy systems that are a mix of old and new builds, and we're putting a great deal of effort into our AWS platform," said Siegelman. "With these different systems, Ansible Automation Platform allows us to have repeatable processes that are standardized. No matter if the platform is in the cloud or on premises, everything looks in place."



Download
the Emory University success story

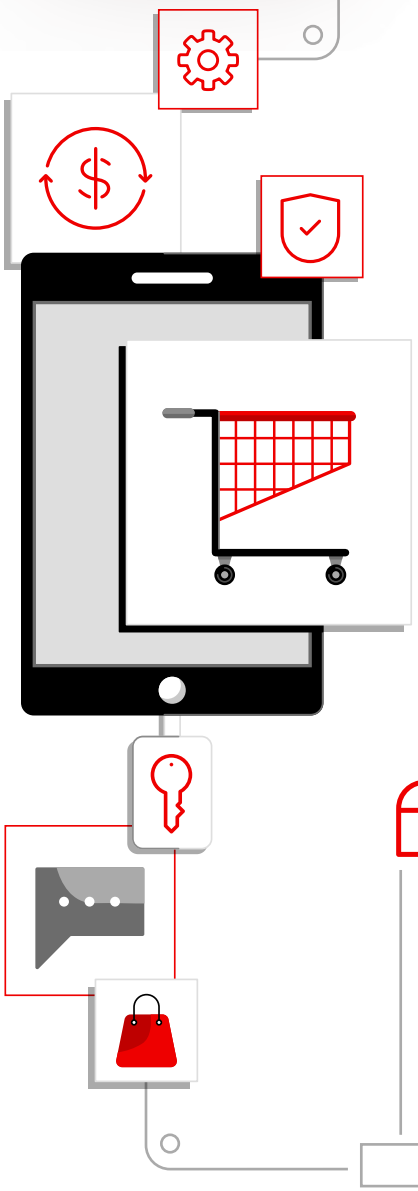
2

SCHWARZ

Retailer Schwarz Group automates IT with Red Hat Ansible Automation Platform

The Schwarz Group is the fourth-largest retailer in the world. The German retailer operates more than 12,500 stores in 33 countries. Schwarz is rapidly growing its international presence, and to succeed, the group must balance consistent store management with the flexibility to adapt to local demands and the agility to open new stores quickly, particularly in new markets–all while mitigating risk.

To manage these stores consistently while flexibly adapting to local demand, the group migrated from existing Puppet management to Red Hat Ansible Automation Platform. With a consistent operational foundation, the group can use self-service capabilities to quickly deploy innovative digital services and stay competitive while maintaining a strong security posture.



Consistency is the key to security across thousands of retail stores worldwide

Schwarz IT employs more than 3,500 engineers to support more than 1,000 SAP systems and 28PB of datacenter-hosted storage. Each Schwarz store operates a Storeserver, a central operational system installed by the company's local IT team that controls a range of store functions, from checkout kiosk systems and closed-captioning security (CCTV) to recycling and reward programs.

To improve user management and authorization, Schwarz IT sought to introduce controlled, efficient self-service capabilities to speed deployment processes. To achieve this, Schwarz IT implemented Ansible Automation Platform.

> *Due to complex and time-intensive processes, the community version did not work to our satisfaction. Automation is a critical component of our business operations, and enterprise support was a key reason we decided to use Red Hat's solution.*
>
> Felix Kuehner, Head of Storeserver, Core Infrastructure Services, Schwarz IT.

During a two-day workshop, Schwarz IT's teams worked with Red Hat's technical experts to review the architecture and establish best practices for the new automation solution.

The group now runs more than 5,000 Ansible Automation Platform jobs each day to manage its store servers.

Improved risk management with role-based system access

Using Ansible Automation Platform, Schwarz IT can more effectively balance controlling system access by authorized application and development with desired self-service capabilities. Role-based access control means application teams can automate deployments as regular users without requiring root access to critical core business systems. "This feature provides high-level consistency while letting individuals be proactive in working on new and existing projects," said Kuehner.

After its initial success with Ansible Automation Platform, Schwarz IT plans to continue exploring ways to help The Schwarz Group achieve consistent yet responsive store operations.

> ***We've valued working with Red Hat and hope to continue using Ansible to find new ways to make our business more modern and efficient.***
>
> Felix Kuehner, Head of Storeserver, Core Infrastrastructure Services, Schwarz IT

Download
the Schwarz success story

Agile Defense enhances security compliance with Red Hat Ansible Automation Platform

3

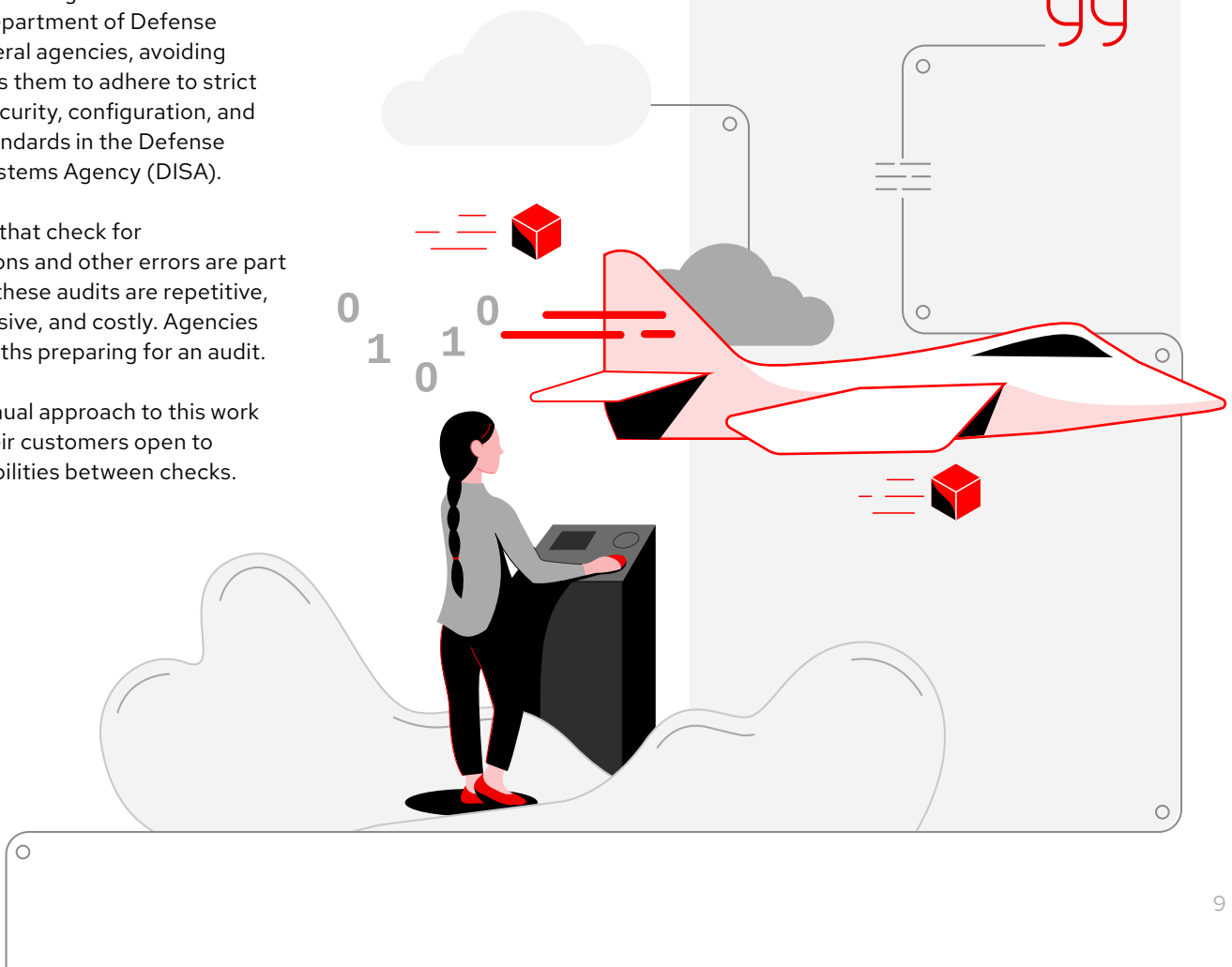
Agile Defense is a leading information technology services business based in Reston, Virginia. With many U.S. Government clients, including several U.S. civil agencies and various branches within the U.S. Department of Defense, IT security is a top priority.

Preventing cybercriminals from gaining unauthorized access to their systems and infrastructure has never been more pertinent. Many breaches that occur are the result of configuration errors. For the U.S. Department of Defense (DoD) and federal agencies, avoiding threats requires them to adhere to strict information, security, configuration, and compliance standards in the Defense Information Systems Agency (DISA).

Regular audits that check for misconfigurations and other errors are part of the job, but these audits are repetitive, resource-intensive, and costly. Agencies can spend months preparing for an audit.

A reactive, manual approach to this work was leaving their customers open to known vulnerabilities between checks.

> ***Our customers' production tasks would grind to a halt ahead of an inspection while they got all their documentation in line.***
>
> Shawn Draper, Solutions Engineer at Agile Defense



Using automation to mitigate the impact of audits

Misconfigurations and audits are a pervasive pain point for many of Agile Defense's government customers. The leading IT services business, which prides itself on innovation through information technology, partnered with Red Hat to create a Security Technical Implementation Guide (STIG) configuration, reporting, and remediation tool. The STIG automation solution performs ad hoc systems audits, optionally remediates misconfigurations, and reports on the current state of devices. Otherwise known as Agile Defense's Compliance as a Service (CPaaS), the STIG automation solution uses Red Hat Ansible Automation Platform because of its flexible and scalable automation capabilities.

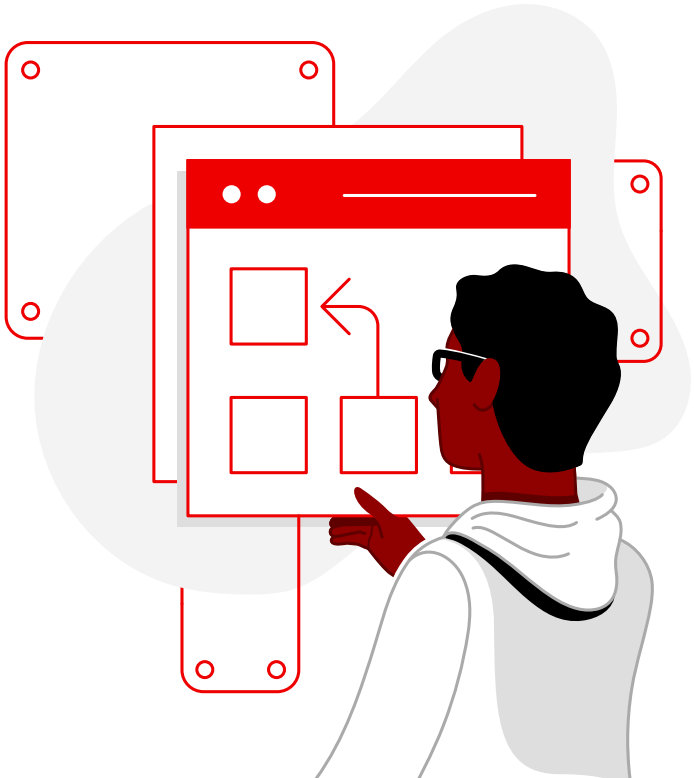
Additionally, Red Hat collaborated with DISA on a STIG for Red Hat Enterprise Linux and understands the importance of creating standards for every device, operating system, and software version.

> ***We chose Red Hat Ansible Automation Platform to tackle this problem because it can communicate with everything.***
>
> Shawn Draper, Solutions Engineer at Agile Defense

The security advantage of Ansible Playbooks

CPaaS uses Red Hat Ansible Automation Platform configuration management automation capabilities to audit for open vulnerabilities. "Red Hat Ansible Automation Platform connects to devices and executes commands specified in an Ansible Playbook," said Draper.

Having identified misconfigurations automatically, CPaaS can also automatically remediate them by following commands in a bespoke Ansible Playbook. Agile Defense has built a variety of playbooks, each designed to test a different type of device. These include playbooks for Red Hat platforms, Windows devices, VMware hypervisors, Cisco routers and switches, and firewalls.



Customers' time spent on audits reduced by

CPaaS helps with all of the paperwork by automatically producing all necessary documentation. Specifically, CPaaS uses Ansible Automation Platform to write an XML check file (viewable in DISA's STIG Viewer) for every device on the network and vulnerability identified to present to the auditor. These artifacts can show current-state information and demonstrate that particular security configurations have been implemented. Ansible Automation Platform also allows customers to extend the capabilities of CPaaS to manage workflows and inventory, schedule audits, and introduce role-based access control. CPaaS also ensures consistency across devices.

> ***One of the great things about automation is that it does the same thing every time.***
>
> Shawn Draper

The proactive monitoring of an agency's security posture that CPaaS provides is critical to maintaining readiness in the face of cyberthreats. Historically, this monitoring has been resource-intensive and required additional software on endpoint devices. By using Ansible Automation Platform to scan for open vulnerabilities, Agile Defense's CPaaS saves its government customers 98% of time spent on audits.

Download the Agile Defense success story

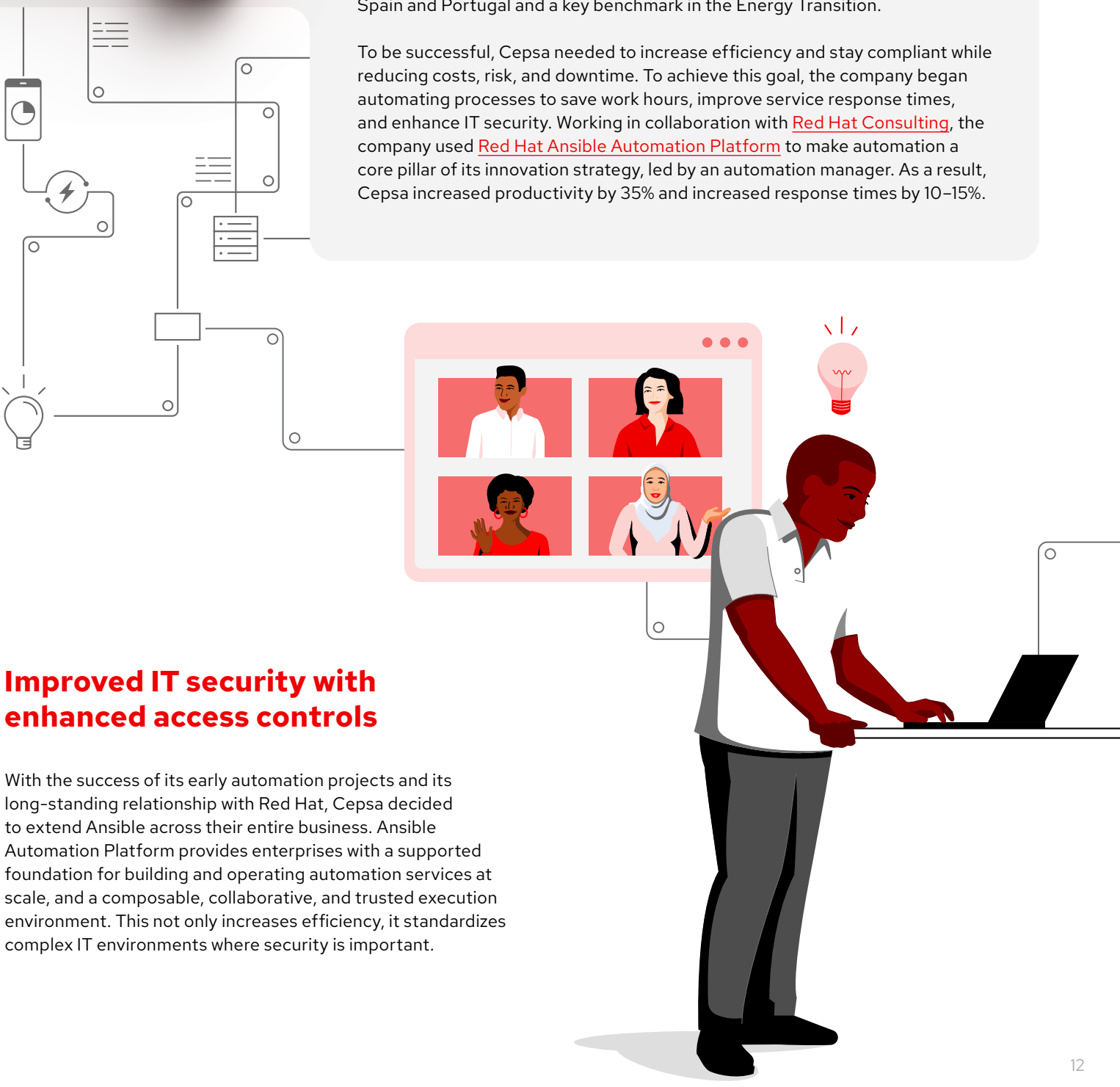
4

CEPSA

Cepsa boosts efficiency with Red Hat Ansible Automation Platform

Global energy and chemical company Cepsa is on a mission toward carbon reduction around the globe. In 2022, the company presented its strategy to be a leader in sustainable mobility, biofuels, and green hydrogen with a focus on Spain and Portugal and a key benchmark in the Energy Transition.

To be successful, Cepsa needed to increase efficiency and stay compliant while reducing costs, risk, and downtime. To achieve this goal, the company began automating processes to save work hours, improve service response times, and enhance IT security. Working in collaboration with Red Hat Consulting, the company used Red Hat Ansible Automation Platform to make automation a core pillar of its innovation strategy, led by an automation manager. As a result, Cepsa increased productivity by 35% and increased response times by 10–15%.



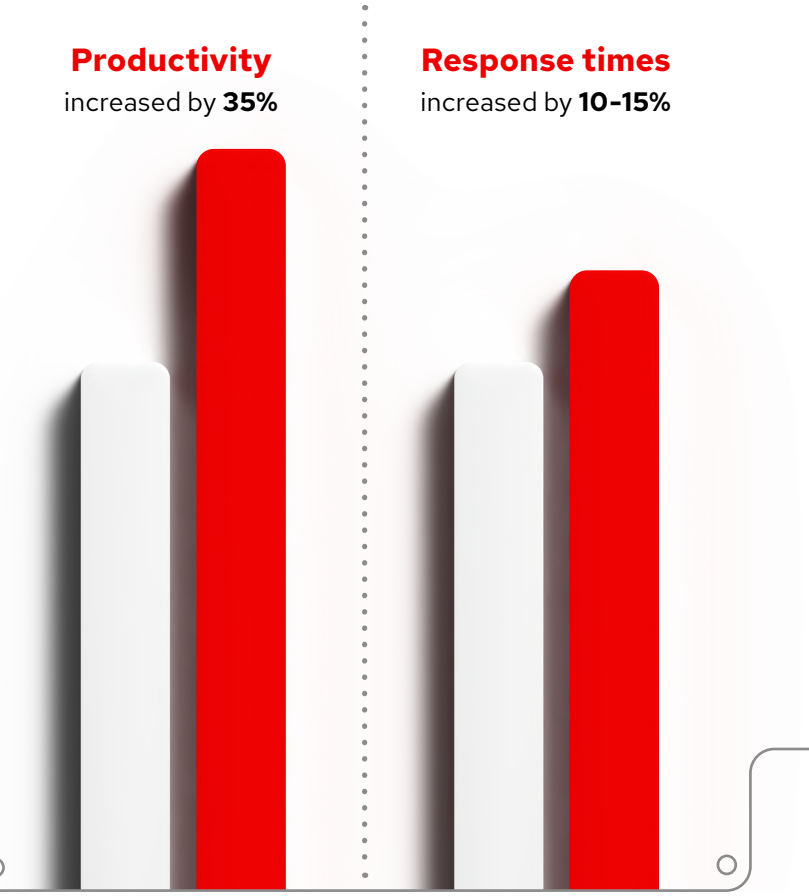
Improved IT security with enhanced access controls

With the success of its early automation projects and its long-standing relationship with Red Hat, Cepsa decided to extend Ansible across their entire business. Ansible Automation Platform provides enterprises with a supported foundation for building and operating automation services at scale, and a composable, collaborative, and trusted execution environment. This not only increases efficiency, it standardizes complex IT environments where security is important.

Ansible's easily understood Playbook syntax allowed Cepsa to define security parameters for any part of their system, whether it's setting firewall rules, locking down users and groups, or applying custom security policies. Standardizing processes has helped Cepsa reduce the number of additional security administration permissions in its systems, mitigating risk. It now groups users by job role and department to ensure the correct permission levels are granted without overextending access.

As a result, Cepsa increased productivity by 35% and increased response times by 10–15%.

A technician can now access Ansible Automation Platform and can restart the service without credentials, giving them the assurance that the process will be executed the same way it is outlined in the predetermined code.



Automation helped support a positive cultural shift, resulting in better collaboration between teams. Red Hat is collaborating with us to implement best practices and learn from their expertise across our entire organization.

Francisco José Martín, Automation Manager,
Department of Exploitation and Operation, Cepsa

Shifting to a security-focused culture with expert automation guidance

Red Hat Consulting helped Cepsa implement the changes needed to maximize the value of their new automation technology and approach. Working alongside the Cepsa team, Red Hat experts helped show the value of an agile work approach and ongoing quality improvements through a continuous integration and continuous delivery (CI/CD) approach.

Download
the Cepsa success story

5

SIEMENS

Siemens improves communication security wth Red Hat Ansible Automation Platform

Headquartered in Munich, Germany, Siemens is the largest engineering company in Europe. The international technology group focuses on electrification–from power generation, transmission, and distribution to smart grid solutions and the efficient application of electrical energy.

Due to the sensitive nature of its business, Siemens is committed to staying at the forefront of security technology. In order to reliably protect access to confidential information, Siemens' 295,000 employees and 100,000 employees from its business partners use public key infrastructures (PKIs), checking the certificates and identity of public keys. A growing use of this technology is to secure Internet-of-Things (IoT) communication and now maintains two PKI environments for different application use cases.

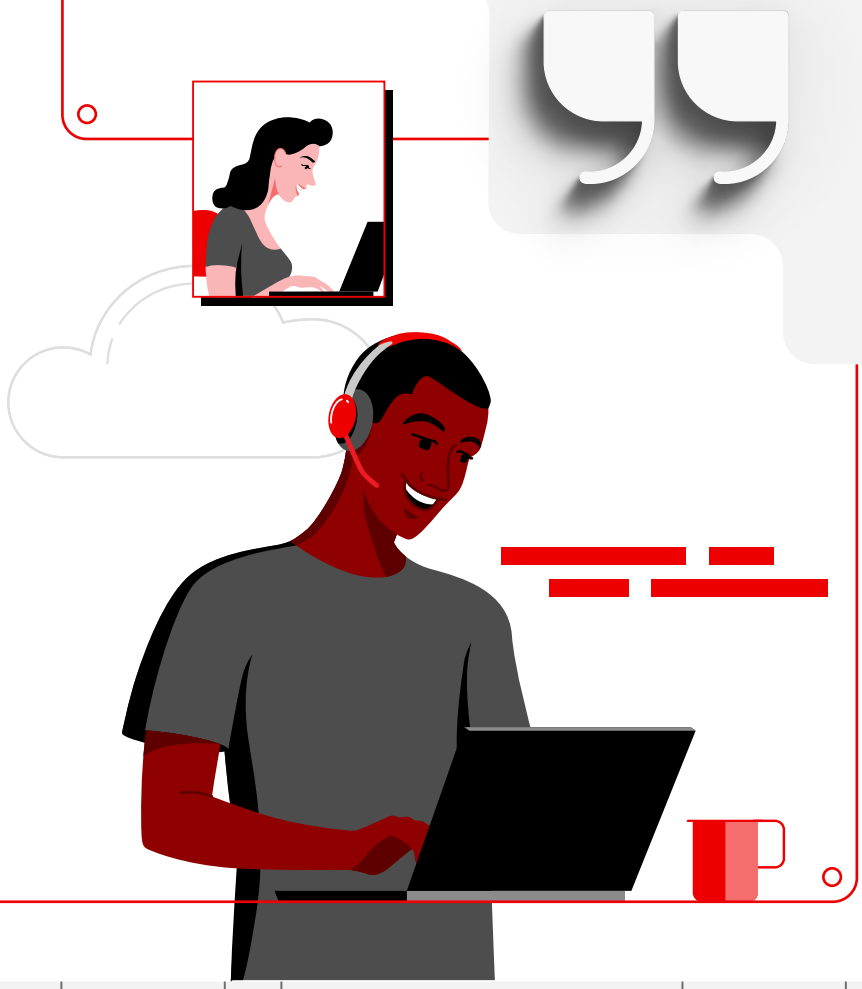
> ***This is especially important since infrastructure-as-code with Red Hat Ansible Automation Platform is more than the introduction of a new tool–it requires a fundamental change in the mindset of system administrators.***
>
> Rufus Buschart, head of public key infrastructure (PKI), Siemens

Whenever we need Red Hat, they're there for us, and our vision is to work together to develop a best practice platform for automation to optimize efficiency and innovation of our organization.

Rufus Buschart

As communications between service teams across the organization expands, configuration complexity is also increasing for Siemens' PKI team. To support this demand, Siemens replaced its legacy automation solution with Ansible Automation Platform.

Using Ansible Automation Platform, Siemens is now able to automate administrative tasks, help increase configuration quality, and help improve communication security throughout the company. Furthermore, Siemens has benefitted from Red Hat expertise and plans to work with Red Hat to explore automating testing processes, with the goal to establish a common blueprint for continuous deployment.



Download the Siemens success story

Con-clusion

Ansible Automation Platform helps organizations manage automated security systems to stay ahead of malicious attacks. With access to hundreds of modules that help security teams to automate all aspects of their IT environment and IT processes, Ansible can integrate many teams to protect complex security perimeters, unifying your security approach and strengthening your security posture.

Ansible Automation helps security teams:

Chain workflows and playbooks for modular reusability.

Security teams can configure a sequence of jobs that share inventory, playbooks, or permissions to fully automate investigations or remediations.

Consolidate and centralize logs.

Integration with third-party external log aggregation services helps security teams identify trends, analyze infrastructure events, monitor anomalies, and correlate disparate events.

Support local directory services and access controls.

Pairing user directory services with infrastructure allows security teams to centralize job access and execution, assign operation subsets to specific roles, and share tasks with other groups.

Integrate external apps using RESTful APIs.

Security teams can use Red Hat Ansible Automation Platform to manage other enterprise applications—like security orchestration and automated response (SOAR) solutions.

Enhance your security posture using automation.

Learn more about Red Hat Ansible Automation Platform.

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com