

Achieve a strong, steady IT security posture with automation

“Our clients are in the midst of significant modernization and digital transformation projects—and they’re doing it on compressed timelines. Automation is the key to realizing new levels of efficiency, agility, and resilience.”

Kurt Sand
General Manager,
DevSecOps,
CyberArk

Overview:

Discover how automation can enhance overall IT security and improve operational efficiency without impeding DevOps, SecOps, or ITOps.

Ensuring security across modern IT environments

Organizations are deploying open source applications, automated IT infrastructures, and DevOps methodologies to speed development and innovation. Across these environments, every application, script, automation tool, and other non-human identity relies on some form of privileged credential to access tools, applications, and data.

To protect the IT landscape from security issues and counter potential cyberattacks, organizations need to embed security into existing day-to-day operation processes and development pipelines.

As a result, organizations are turning to automation to manage privileged access to critical systems and data, in order to enhance overall IT security and improve operational efficiency without impeding DevOps, SecOps, or ITOps.

By integrating comprehensive IT automation with a full life cycle solution for managing the most privileged accounts and keys, organizations can confidently automate end-to-end processes, including IT itself and the identities using these services.

Managing consistent, security-focused credentials with automation

CyberArk’s integration with Red Hat® Ansible® Automation Platform strengthens security to protect data, infrastructure, and assets across the enterprise, in a cloud, and throughout the DevOps pipeline, through the automation of secrets and privileged access management.

Together, Red Hat Ansible Automation Platform and CyberArk Privileged Access Manager (PAM), a platform used to manage privilege access across IT environments, streamline the rotation and management of privileged credentials and automate the prevention and remediation of high-risk activities.

A balance between automation agility and security best practices

By automating CyberArk PAM configurations, Red Hat Certified Content Collection significantly enhances the security posture, streamlines operational processes, and ensures compliance with regulatory requirements.

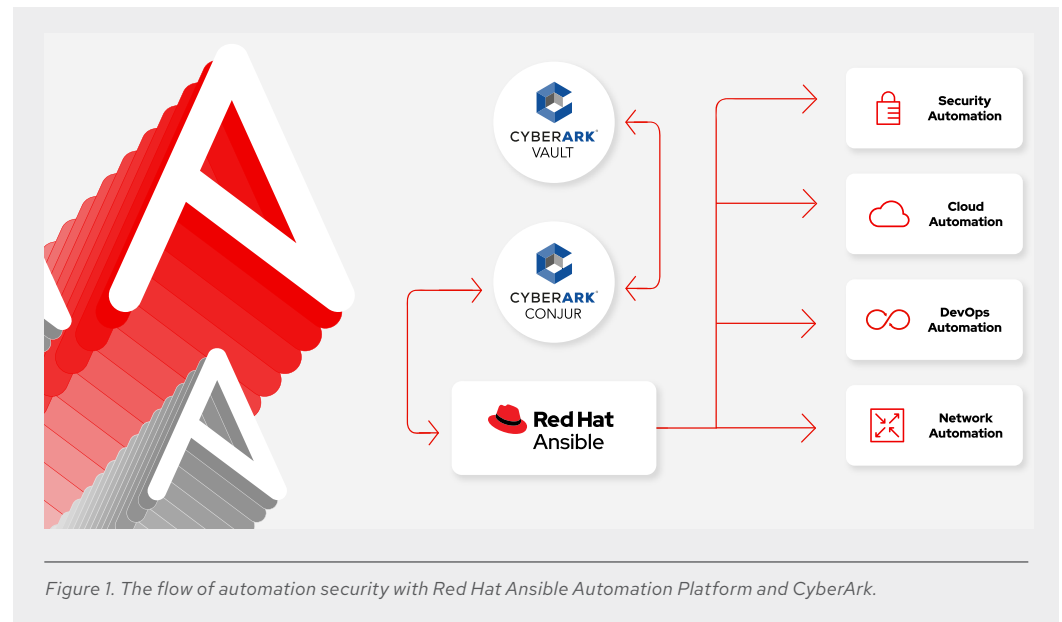
Both the Software-as-a-Service (SaaS) and on-premise versions of CyberArk PAM integrate with Red Hat Ansible Automation Platform application programming interfaces (APIs) to act as the secrets provider for the automation of endpoints.

The integrations allow you to automate the remediation and onboarding of new users or groups in CyberArk PAM and make changes as needed in a declarative and infrastructure-as-code (IaC) approach.

Red Hat Automation Platform works with CyberArk Conjur and CyberArk Vault to safeguard access to secrets needed to perform automation with sensitive information, such as passwords to access protected data or keys used to connect to cloud services. You can also create temporary credentials for access to secrets using Red Hat Ansible Automation Platform to further reduce the security risk of your automation.

This integration helps organizations enhance the security of their automation processes, ensure controlled access to privileged information, and maintain a strong security posture in line with CyberArk PAM principles.

In addition, the certified Ansible Content Collections from CyberArk allow for straightforward management of CyberArk PAM. The collections include modules and roles that facilitate the automation of tasks related to the remediation of users and groups, adjustments to privileges, and other common administrative activities within CyberArks PAM.



About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with [award-winning](#) support, training, and consulting services.

North America

1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa

00800 7334 2835
europe-latam@redhat.com

Asia Pacific

+65 6490 4200
apac@redhat.com

Latin America

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

f facebook.com/redhatinc

t @RedHat

in linkedin.com/company/red-hat

redhat.com
#693383_0124

Gain a consistent security posture with automation

With CyberArk and Red Hat Ansible Automation Platform, you can safeguard your enterprise environment through automation and maintain a consistent security posture across your network, DevOps, cloud, and security settings. Together, the solutions allow you to:

- ▶ Simplify operations by automating complex and security sensitive tasks, credential management, and rotation, and common CyberArk administrative tasks.
- ▶ Strengthen security, reduce risk, and improve compliance across the IT environment.
- ▶ Minimize the security burden on development organizations and improve the organization's security posture without affecting velocity.

Strengthen security across your IT environment

Learn more about how Red Hat Ansible Automation Platform and CyberArk Privileged Access Manager can help you automate your organization safely without impeding DevOps, SecOps, or ITOP:

- ▶ [Watch the developing an approach to centralize and automate secrets-management video.](#)
- ▶ [Watch the trusted automation series demonstration.](#)
- ▶ [Find out about the Red Hat and CyberArk partnership.](#)