CYBERARK

SOLUTION BRIEF

CYBERARK APPLICATION IDENTITY MANAGER™ SECURES ANSIBLE AUTOMATION IMPLEMENTATIONS

Key Features and Benefits

- Consistently secure and manage passwords and other secrets used by Ansible
- Keep secrets out of playbooks to reduce vulnerabilities
- Automatically rotate credentials to improve security posture
- Avoid duplicating secrets management functionality across multiple platforms
- Meet audit and compliance requirements

ANSIBLE by Red Hat®

CyberArk Application Identity Manager helps Ansible by Red Hat customers mitigate risks by protecting secrets and privileged account credentials used by applications, scripts, and throughout automated environments.

CyberArk Application Identity Manager lets developers and security teams proactively secure and manage secrets and privileged account credentials based on administratively defined policies. The comprehensive application identity management solution protects secrets used by Ansible, keeping credentials out of playbooks. In conjunction with other CyberArk Privileged Access Security solutions, CyberArk Application Identity Manager centralizes and automates secrets management, reducing security vulnerabilities and minimizing attack surfaces, while streamlining operations.

Challenges with Embedded Credentials

In today's complex IT environments, automation scripts, applications, and other services are continuously created, executed, and disabled. Automation tools like Ansible require privileged account access to execute scripted operations. In a typical Ansible environment privileged account credentials and secrets are scattered across physical and virtual machines, and hard-coded into automation scripts, making them nearly impossible to track and manage.

Worse still, credentials are often issued by build team members, independently of the security organization. Secrets often remain unchanged for months or even years after release. Former employees, contractors and development partners often maintain access to critical applications and systems long after termination, exposing the business to security breaches, malicious attacks and confidential data theft.

Secure and Manage Credentials and Secrets used by Ansible

The CyberArk Privileged Access Security Solution is the industry's most complete solution for protecting and managing privileged accounts across on-premises and cloud infrastructure and development environments. The CyberArk solution helps organizations efficiently administer secrets and privileged account credentials, proactively monitor and control privileged account activity, and quickly respond to threats.

CyberArk Application Identity Manager, an integrated component of the CyberArk Privileged Access Security Solution, reduces security vulnerabilities by enabling organizations to remove hard-coded and unmanaged credentials from Ansible playbooks, introduce role-based access controls, and safeguard credential exchanges. Secrets are securely stored in the CyberArk Digital Vault—out of repositories, out of source code, and off of developer laptops and user-accessible storage systems—for centralized control and manageability. Passwords, SSH keys, and other credentials can be automatically rotated based on policy for robust protection.

Partner Products

- Red Hat Ansible Automation (Commercial Solutions)
- Ansible (Open Source Solution)

CyberArk Products:

- CyberArk Application Identity Manager
- CyberArk Core Privileged Access Security Solution

Note: CyberArk Application Identity Manager plug-in bundled with Ansible v2.4 or greater

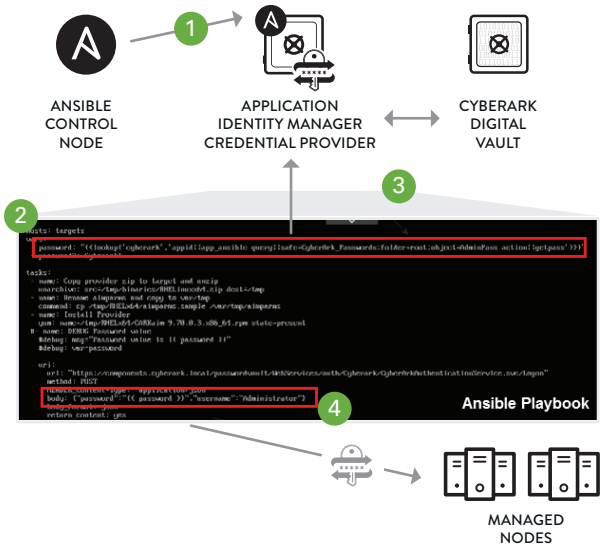
Joint Solution Provides Seamless Integration

CyberArk Application Identity Manager integrates seamlessly with Ansible, helping IT teams, development staff and security professionals centralize and simplify the management of security credentials across the application lifecycle. The CyberArk Application Identity Manager plug-in for Ansible was approved by the Ansible community and is bundled with Ansible.

The integrated solution automatically secures and manages credentials used by Ansible playbooks, helping organizations:

- Eliminate hard-coded passwords to reduce vulnerabilities
- Cache credentials locally to optimize performance and availability
- Audit privileged account activity for regulatory compliance
- Safely store and rotate credentials to strengthen security
- Avoid duplicating secrets management functionality across multiple platforms to simplify operations

The diagram below describes the integrated solution components and workflows.



Workflow

1. Application Identity Manager Credential Provider plug-in installed on Ansible Control Node.

Whenever Ansible Requires Privileged Credentials

2. Standard python 'lookup' executed from within Ansible Playbook
3. Lookup uses Application Identity Manager CLIPasswordSDK call to retrieve credentials from Credential Provider
4. Credentials stored in variables and used throughout playbook to access assets, APIs, configure systems, install applications, etc.

About CyberArk

CyberArk is the only security company that proactively stops the most advanced cyber threats – those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to protect against cyber threats before attacks can escalate and do irreparable business damage.

About Red Hat

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

ANSIBLE
by Red Hat