LEADING INSURANCE COMPANY

CASE STUDY

CYBERARK®

Company: North American Insurance Company

Leading insurance company uses CyberArk to safeguard mission-critical applications running on Red Hat® Openshift®

Insurer accelerates and secures their digital transformation

Industry: Insurance

Annual Revenue: > $25B

Employees: > 25,000

CyberArk Product & Services:
Secrets Manager/Conjur Secrets Manager Enterprise

"We liked how easy it was to manage secrets on Red Hat OpenShift using CyberArk's secrets management platform."

Large North American Insurance Company

Red Hat OpenShift

servicenow

A major North American insurance company secures mission-critical applications running on Red Hat OpenShift using CyberArk Secrets Manager.

The insurance company uses the secrets management solution to reduce the attack surface, mitigate risk, and accelerate their digital transformation. The solution provides a centralized approach for managing secrets and privileged credentials across the entire application spectrum—from the organization's hybrid applications to containerized applications running in the cloud.

To make it easier for application development teams to securely provide containerized applications with the secrets and credentials needed to access databases and other sensitive resources, the insurer integrated ServiceNow® with CyberArk Secrets Manager. This provides developers with a self-service solution which has helped the company accelerate their digital transformation while strengthening security.

THE CHALLENGE

The insurance company wanted to use DevOps methodologies and containerize thousands of applications to increase business agility, eliminate inefficiencies, and accelerate the pace of innovation. Containerized applications use secrets such as passwords, tokens and SSH keys to gain access to sensitive enterprise resources such as databases, web applications, compute, storage and networking services. The security team recognized that in some other organizations, out of expediency, developers have hardcoded secrets, access keys and other sensitive credentials into applications. Hard coded credential are not only challenging to rotate, but also potentially expose the business to data theft and malicious attacks. The insurer's information security organization wanted to ensure credentials were removed from code to reduce potential vulnerabilities, such as inadvertently exposing secrets in the code stored on repositories. A key priority was to ensure applications can securely access data bases and other sensitive resources without impairing developer productivity or hindering application delivery.

CHALLENGE

- Migrate thousands of applications to containerized environments by leveraging DevOps tools, container platforms, cloud and hybrid environments
- Reduce time to market for new services for both external customers and internal users
- Address new security concerns with the adoption of DevOps tools and processes
- Maintain a single point of control across the enterprise regardless of the underlying technology platforms and compute environments

KEY BENEFITS

- Accelerated the business's digital transformation by centrally managing secrets for applications migrated from on-premise, to containerized and cloud environments
- Reduced development cycle by simplifying how developers enable applications to securely access databases and other sensitive resources
- Improved security by natively authenticating and then providing containerized applications with the secrets they require to access databases and other resources.
- Eliminated secret zero. Automatically rotate secrets based on policy. Simplified removing hard-coded credentials from code.
- Achieved migration plan of securely providing applications with 1+ million secrets per day using Secrets Manager.

SOLUTION

The insurance company selected Conjur Secrets Manager Enterprise to secure its Red Hat OpenShift based applications and CI/CD tools. Conjur Enterprise is specifically architected for containerized and DevOps environments, and lets the company efficiently secure, rotate, audit and manage secrets and other credentials at scale, based on policy.

A long-time CyberArk customer, the insurance company was well versed in the advantages of CyberArk Secrets Manager. By deploying Secrets Manager the company also extends their previous CyberArk investments with the establishment of a common digital vault and single point of control for credentials used by traditional and containerized applications, developers, test engineers, system admins and other personnel.

The company implemented a self-service framework using the ServiceNow IT Service Management platform as a front-end.

THE RESULTS

Secrets Manager helps the company take advantage of the benefits of Red Hat OpenShift containers without compromising security or agility. The solution helps the insurer accelerate time-to-market, reduce risk, and free up development resources to focus on core functionality. With Secrets Manager, containerized applications gain secure access to Oracle, DB2, and MS SQL Server databases, under the policies and guidelines established by the corporate security organization.

ABOUT CYBERARK

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust Cyberark to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com.

For DevOps solutions visit www.cyberark.com/devops and for developer focused blogs, discussion forums, technical content and CyberArk's open source secrets management solution visit www.conjur.org.