ROCKWELL AUTOMATION

CASE STUDY

CYBERARK®

Rockwell Automation

Company: Rockwell Automation, Milkwaukee, WI
www.rockwellautomation.com

Rockwell Automation Deploys CyberArk for Proactive Privileged Access Management, Provisioning, and Control

Annual Revenue: $6.66 billion USD (2018)
Employees: 23,000
CyberArk Product & Services:
Privileged Access Manager Solution
Platforms:
Windows servers, Unix/Linux, Oracle, VMware, desktops and service accounts

"CyberArk has delivered excellent product features, which are streamlined to scale throughout the organization. CyberArk's solutions have proved much faster to deploy than other security tools, giving us good quality insight within a short time period."

Jayne Little, Information Security Engineer (Privileged Access), Rockwell Automation

Innovative global industrial automation provider utilizes the CyberArk Privileged Access Manager Solution to manage, standardize and control privileged access without sacrificing productivity.

Rockwell Automation delivers business process control and information platforms, software applications and automation components to customers around the globe. With over twenty thousand global employees and multiple privileged accounts across diverse computing environments and servers, the company required a solution to simplify management across the privileged account lifecycle.

In addition, in line with the company's commitment to product excellence and innovation, Rockwell sought an agile solution that could be managed across multiple teams, without sacrificing productivity or the quality of their work.

THE CHALLENGE: SECURE PRIVILEGED ACCOUNTS, AUTOMATE PASSWORD MANAGEMENT AND PROVIDE METRICS FOR SUCCESS

One of Rockwell Automation's most important IT priorities was to proactively identify the privileged access risk while ensuring that all accounts complied with regular but flexible password policies. With multiple employees, servers, privileged accounts and password policies established across their platforms, standardization and control would be imperative to ensuring that Rockwell identified and mitigated the risks associated with unmanaged privileged accounts. The company sought a solution to enforce and automate role-based privileged access control and policies in order to secure accounts, mitigate password vulnerabilities and support audit and compliance requirements such as those defined within Cobit's DS5.4 User Account Management.

Moreover, reflective of Rockwell's process- oriented business, the company required detailed access to metrics that demonstrated the extent of privilege access vulnerabilities, including any risks associated with unmanaged accounts and administrative rights.

IMPLEMENTING SECURITY BEST PRACTICES: ACHIEVING BUSINESS CONTINUITY BY AUTOMATING PRIVILEGED ACCESS MANAGEMENT

For Rockwell Automation, the only solution considered was the CyberArk Privileged Access Manager Solution. After analyzing the product, Rockwell immediately recognized that the CyberArk solution enables a proactive and automated approach to privileged access management—ensuring security best practices across multiple IT teams and both Windows and Unix environments. Moreover, further supporting best practices and business continuity, Rockwell was able to integrate the CyberArk solution with existing security tools, including vulnerability management for deeper, authenticated scans and collection of privileged activity within their Security Information and Event Management (SIEM).

Challenge

- Secure, provision and control privileged accounts, automate privileged access management and provide metrics for success

Environment

- Windows, Unix

Results & Key Benefits:

- Standardization and automated password management for reduced risk around privileged accounts
- Enforcement of role-based privileged access control while creating smoother work processes
- Proactive management of privileged access, accounts and activity—enabling audit

"We view our relationship with CyberArk as a partnership. Their technical expertise enables our team to look at our security problems in new and different ways—essentially providing us with quality insight in short time periods to ensure security best practices."

Jayne Little, Information Security Engineer (Privileged Access), Rockwell Automation

In just two months, thanks in part to CyberArk's technical resources, the company was able to fully implement the solution. With solid role definitions integrated with SailPoint's IIQ suite, Rockwell was able to reduce operational costs by improving the onboarding process and streamlining privileged access through CyberArk's Privileged Access Manager Solution.

"CyberArk has delivered excellent product features, which are streamlined to scale throughout the organization," commented Jayne Little, Information Security Engineer (Privileged Access) at Rockwell Automation. "CyberArk's solutions have proved much faster to deploy than other security tools, giving us good quality insight within a short time period."

RISK IDENTIFICATION AND ASSESSMENT: CYBERARK'S AUTO-DISCOVERY TOOLS ENABLE A HOLISTIC UNDERSTANDING OF ROCKWELL'S "PRIVILEGED" RISK

Another important component of Rockwell's deployment involved the company's focus on organizational risk identification and assessment. With the CyberArk solution, Rockwell can proactively identify and assess security vulnerabilities and risks in near

real-time. This functionality also includes, of course, the ability to identify and automatically provision privileged accounts through CyberArk's auto-discovery capabilities. With the CyberArk Privileged Access Manager Solution, the company can also establish and meet metrics by identifying, managing, securing and provisioning all privileged accounts in a regular and controlled fashion, while also guaranteeing that privileged credentials adhere to defined security policies to better manage and assess risks associated with privileged accounts.

The company also plans to deploy CyberArk's Discovery & Audit (CyberArk DNA™) solution to complement the Privileged Access Manager Solution and scan and analyze privileged accounts across their networks to develop a more complete understanding of the security risks that privileged accounts present to their IT environment.

RESULTS: STANDARDIZATION, CONTROL AND COLLABORATION—A UNIQUE AND PRODUCTIVE USER EXPERIENCE

Most importantly, since implementation Rockwell has met their primary goals: standardization, control and cross-team collaboration. CyberArk creates a unified accountability and control point over all privileged accounts. In addition, Rockwell has established security best practices across their computing environments, including a renewed focus on regular inventory "clean up," as well as automated password change policies based on pre-defined rules. In terms of collaboration, the CyberArk solution has satisfied Rockwell's requirement of an agile solution that can be deployed and accessed across multiple teams.

"We view our relationship with CyberArk as a partnership. Their technical expertise enables our team to look at our security problems in new and different ways—essentially providing us with quality insight in short time periods to ensure security best practices," added Jayne Little.

Rockwell continues to achieve business continuity by automating this password management process and providing IT admins with personalized workflows for quicker access, improved usability and greater operational efficiency.

Finally, it is important to convey that CyberArk's solution provides Rockwell with an unprecedented level of visibility into their security risks. No matter the function of the employee—risk, compliance, security and/or IT—Rockwell's team continues to engage with the product to identify new problem areas, risks and potential solutions. This usability continues to increase demand for CyberArk's solutions across their organization.

©CyberArk Software Ltd. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 05.21 Doc. 216056692

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.