Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation

Summary

There are many server settings that customer infrastructure teams can select to harden servers against growing cyber threats. But how can they find and use Dell's security configuration settings best-practices? And how can they efficiently and continuously check if the settings are incorrectly configured or have changed? The answer is the cybersecurity feature in the CloudIQ for PowerEdge AIOps solution. It compares the configuration of deployed PowerEdge servers to a security related configuration policy. When CloudIQ identifies a deviation between the actual settings and the recommended configuration settings, it notifies the administrator and recommends remediation steps to correct the issue(s).

This Direct from Development (DfD) tech note details the time savings that customers can achieve by using the CloudIQ automated cybersecurity policy engine versus manually examining compliance.

Authors

Mark Maclean
Technical Marketing Engineering

Kyle Shannon
Product Management

Introduction

In today's always-on, always-connected environment, all organizations constantly need to enhance their cybersecurity strategy to mitigate the increasing threat of attack. Using the built-in cybersecurity feature of Dell CloudIQ, customers can easily build security policies to protect PowerEdge servers. A policy consists of ready-to-use tests that customers can enable simply by selecting a checkbox. The tests consist of infrastructure security settings that are based on Dell best practices and the American NIST (National Institute of Standards and Technology) cybersecurity framework. Dell CloudIQ Cybersecurity for PowerEdge both enables the easy creation of a policy and automates the policy policing—making it simple, efficient, and predicable.

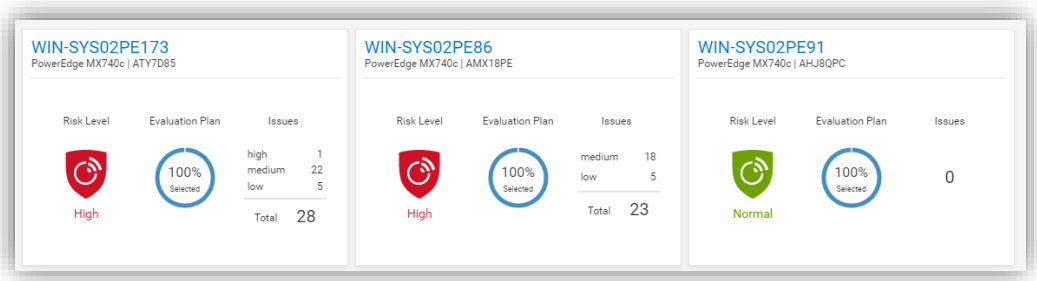


Figure 1. **CloudIQ Cybersecurity Dashboard**

CloudIQ is the AIOPs proactive monitoring and analytics application that delivers system health insights and recommendations for Dell infrastructure solutions, including storage, data protection, networking, and of course, PowerEdge servers.

The cybersecurity policy engine built into CloudIQ has over 30 security configuration rules for PowerEdge that can be implemented simply. Because CloudIQ is cloud based, it can integrate with any number of OpenManage Enterprise (OME) instances across multiple datacenters, through the OME CloudIQ Plugin. This means that CloudIQ can apply the same policy to multiple OME managed servers, regardless of their location. This feature is delivered by CloudIQ without any additional configuration at the iDRAC or OME level. When a policy is established, CloudIQ continuously checks the desired state of PowerEdge security configuration settings against the current "as is" configuration. If a server is found to be out of policy compliance, it is highlighted. The results are scored by CloudIQ, with the most vulnerable servers being given a "high" risk level. Individual problems can be viewed with recommended remediation. These recommended security configuration corrections can then be executed one-to-one per server using the iDRAC GUI. If multiple hosts are found to be non-compliant, then OME can be used to deliver a configuration update template file or execute a RACADM script to correct the security configurations for multiple servers.

The Benefits Of Automation

To understand the profound impact of the automation of this process, we have tested it against a manual process for 1, 10, 100*, and 1,000* servers. Based on the testing of the CloudIQ Cybersecurity approach for a customer with 1000* servers, we found the following:

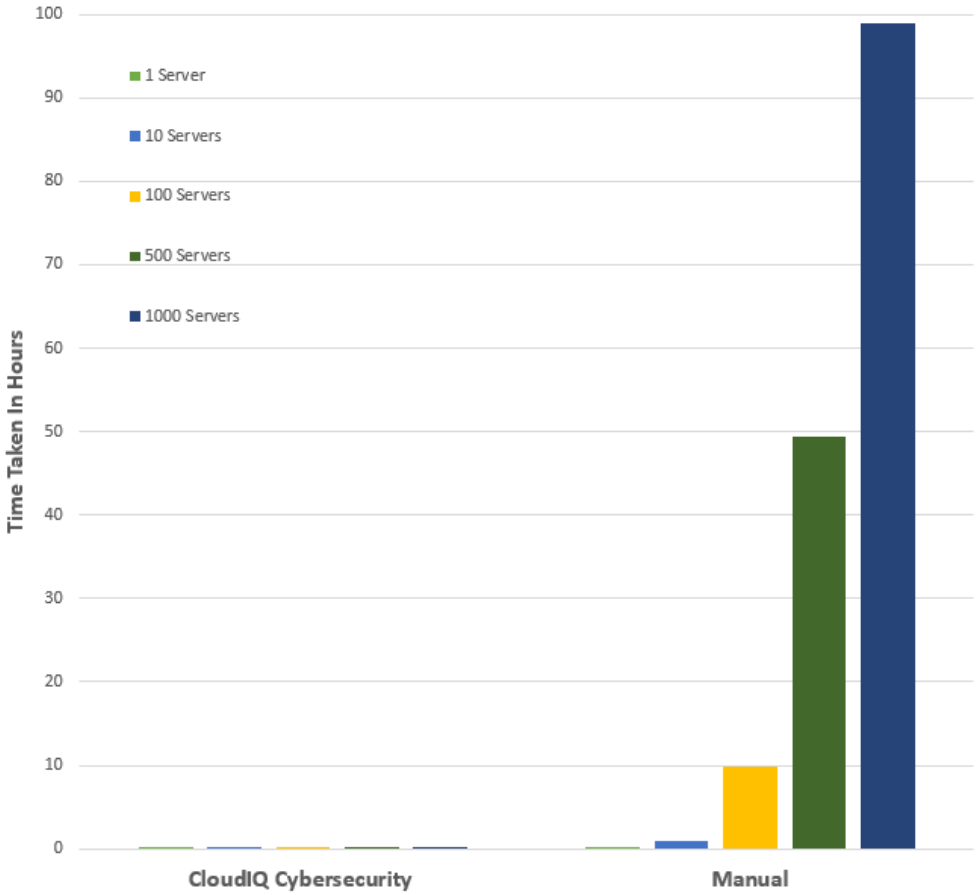
- The CloudIQ task completed 99% quicker than a manual review.*
- CloudIQ reduced the time by 98 hours to complete the task once.*
- Using CloudIQ Cybersecurity automation saves over a week of effort immediately versus manual.*
- Once enabled, CloudIQ monitors of all these key security configuration settings continuously.

*Projected outcomes based on analysis of results, results may vary.

In the lab testing, we found that manually checking 15 settings on the iDRAC GUI took 5 minutes 56 seconds. By contrast, creating a CloudIQ cybersecurity policy consisting of 15 active test items and selecting target server(s) only took 2 minutes 58 seconds. In addition, whether creating the policy for 1, 10, 100, or 1000 servers, this task took the same amount of time. However, using the manual process, each additional server added an additional 5 minutes 56 seconds to complete the checks. Also, after the policy is set, CloudIQ continues to check the servers' as-is settings for compliance.

Results Summary

The following graph highlights the differences between automation and the manual process, showing the time saving advantages.



See Table 1 near the end of this document for full results.

Testing Overview

To demonstrate the ease of use and the impact of automation, we tested two different approaches: manual versus automation. To use this Cybersecurity feature of CloudIQ:

- OpenManage Enterprise 3.9 “OME” or higher must be installed, with the CloudIQ Plugin 1.1 or higher enabled
- the PowerEdge server(s) must be covered by Dell Pro Support
- the target servers for the policy must already be discovered by OME

To build the policy, the user must have the CyberSec admin rights assigned in CloudIQ. Some of the configuration rules used in the test security policy are the iDRAC default values. However, any of these values can be changed on an individual iDRAC by administrators with the correct rights, opening a security weakness.

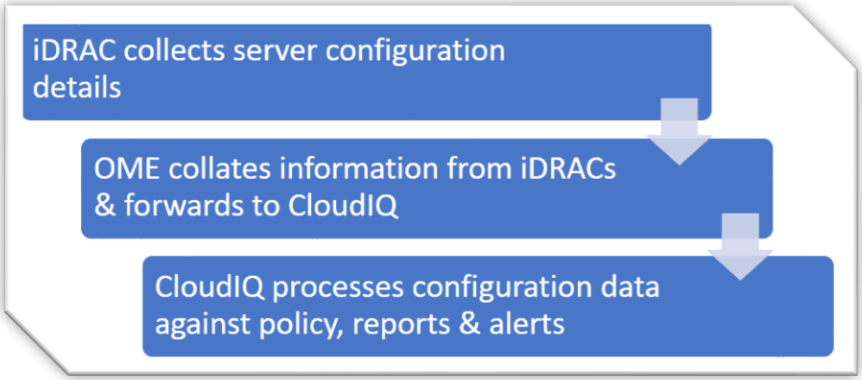


Figure 2. **Configuration Data Flow**

Testing Procedure

To ensure an accurate comparison of the test approaches, we rigidly tested and documented our testing. We selected 15 common settings, a mixture of BIOS and iDRAC configuration values, and enabled 15 tests in the trial policy.

Tests were conducted in-house on July 6, 2022, at Dell Technologies in Austin TX, in the technical marketing lab facility and online using Dell’s CloudIQ offering.

I. USB ports: Disabled

II. iDRAC active NIC: Dedicated

III. System lock down: Enabled

IV. iDRAC config from host: Disabled

V. IPMI over LAN: Disabled

VI. Secure boot: Enabled

VII. Password policy: Strong

VIII. VNC: Disabled

IX. SNMP version 3: Enabled

X. SSH: Disabled

XI. Syslog: Enabled

XII. Active directory authentication: Enabled

XIII. IP blocking: Enabled

XIV. Virtual media encrypted: Enabled

XV. NTP time synchronization: Enabled

Steps for an automated approach: using CloudIQ PowerEdge Cybersecurity policy

Starting from the CloudIQ “sign in page” https://cloudiq.emc.com:

1. Sign into CloudIQ.
2. From the menu down at the left-hand side of the screen. select Cybersecurity.
3. Select Policy.
4. Select the templates tab.
5. Select add template.
6. Name template.
7. Select PowerEdge from product drop down menu, then click next.
8. In the template evaluation plan, configure the following:
9. Access Control – select: IP blocking is enabled/SSH is disabled/The SNMP configured for V3/Active directory authentication is enable / VNC disabled
10. Audit and Accountability – select: NTP time synchronization enabled / Remote Syslog enabled
11. Configuration Management – select: configure iDRAC from Post/System lockdown enabled/USB ports disabled
12. Identification and Authentication – select: Password has minimum strength score of strong
13. System and Coms Protection – select: IPMI over lan disabled / virtual media encryption enabled / dedicated nic
14. System and information – secure boot enabled
15. Select finish.
16. Select the systems tab.
17. Select the required hosts from the list of hosts (in our test we selected a list of 1 or 10 or 100 or 1000).
18. Click assign.
19. Select the required template from the drop down template list menu.
20. From the menu down at the left-hand side of screen, select system risk to view results.

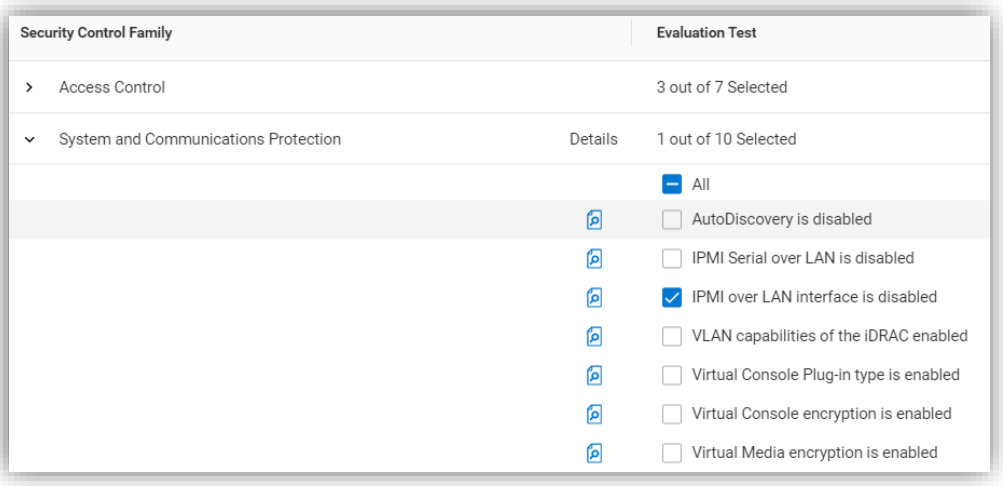


Figure 3. **Select rules to build a policy**

Steps for the manual approach: checking configuration values in iDRAC GUI

From a browser displaying the iDRAC login screen:

1. Login
2. USB – Configuration/BIOS settings/integrated devices/user accessible USB ports: all ports off
3. Secure boot – Configuration/BIOS settings/TPM advanced /secure boot: enabled
4. VNC – Configuration/Virtual console/VNC server/Enable VNC server: Disabled
5. SNMPv3 – Configuration/System setting/Alert config/SNMP trap/SNMP setting/SNMP Trap format: SNMP v3
6. Syslog – Configuration/System settings/Alert configuration/Remote syslog settings/Remote syslog: Enabled
7. Virtual Media encryption – Configuration/Virtual media/Attached media/Virtual Media encryption: Enabled
8. Dedicated port – iDRAC settings: Active NIC interface: dedicated
9. Local iDRAC Config – iDRAC settings/services/local config/disable iDRAC local configuration: enabled
10. IPMI – iDRAC settings/connectivity/network/IPMI settings/Enable IPMI over lan: disabled
11. Password Policy – iDRAC settings/users/global users settings/Password setting/Policy/Score: Strong[1]
12. AD authentication – iDRAC settings/Users/Directory services/Microsoft AD: Enabled
13. SSH – iDRAC settings/services/SSH/Enabled: Disabled
14. IP blocking – iDRAC settings/Connectivity/Network/Advanced networking setting/IP blocking/Blocking: Enabled
15. NTP time synchronization – iDRAC settings/settings/Time zone/NTP server/Enable NTP: Enabled
16. Lockdown – check padlock icon on top right of screen is displaying locked mode

These steps were tested using Dell PowerEdge R540 BIOS 2.12.2 and iDRAC9 firmware: 5.10.00.00.

[1] Enforcing the strong password policy manually ensures new password compliance with the password policy, however pre-existing accounts could still have weak passwords waist cloudIQ flags any iDRAC with weak password.

Results

Number of servers	CloudIQ Cybersecurity Policy	Manual Checking
1	2 Min 58 Sec	5 mins 56 secs
10	2 Min 58 Sec	59 min
100	2 Min 58 Sec	9 hours 53 mins
500	2 Min 58 Sec	49 hours 26 mins
1000	2 Min 58 Sec	98 hours 53 min

Table 1. Results of Testing

Summary

Our testing showed that automation using the Dell CloudIQ for PowerEdge cybersecurity policy engine brought major benefits in time efficiency, repeatability, predictability, and of course, peace of mind. The benefits also dramatically increased as we extrapolated the number of servers in the testing data.

References

CloudIQ on Dell.com - for data sheets and demo videos

Take Control of Server Cybersecurity with Intelligent Cloud-Based Monitoring Blog

Building and Tracking Dell CloudIQ Cyber Security Policies for PowerEdge Servers Video

Technical Knowledge Page For OpenManage Enterprise CloudIQ Plugin

Additional Cybersecurity Related Solutions from Dell