## DCLTechnologies

# Build a fortified cybersecurity foundation with **CloudIQ AIOps**

# Security misconfigurations are the 5th greatest cybersecurity risk<sup>1</sup>

As your IT environment scales and gets more distibributed across core, edge and cloud, manually checking all your systems' security settings is impractical.

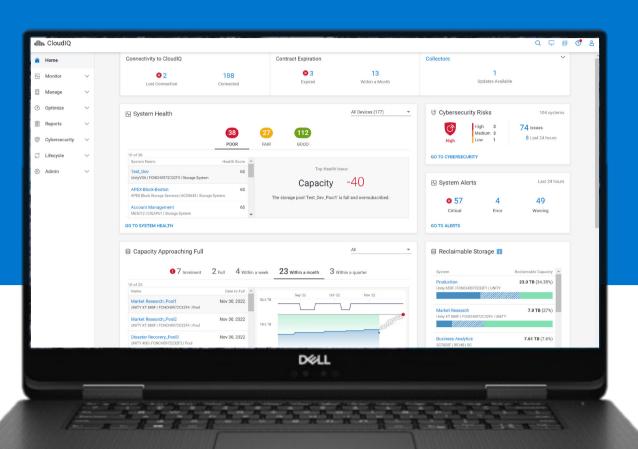
When security misconfigurations go unnoticed, you leave your organization vulnerable.

The solution is intelligent software that automates checking, keeps you continuously aware of risks and recommends remediation.

#### AlOps for Intelligent Infrastructure Insights

1,000s

#5

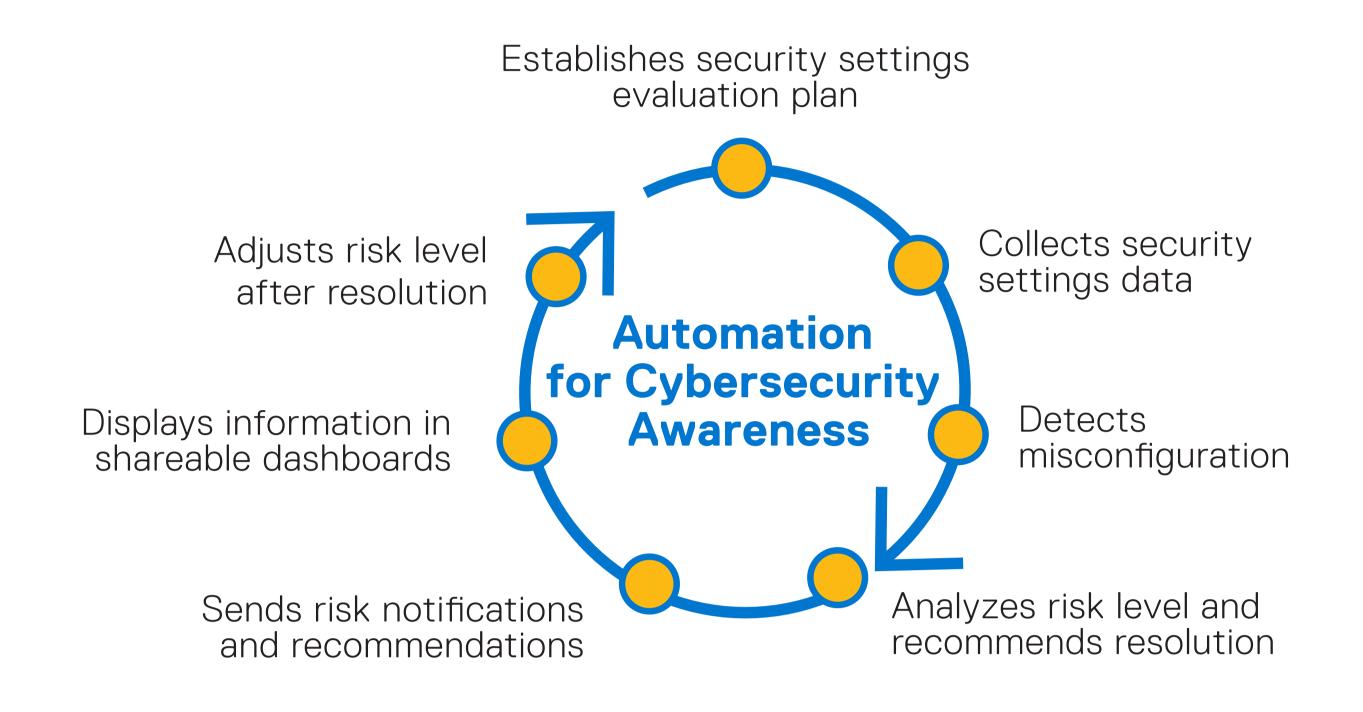


of organizations and IT administrators worldwide rely on CloudIQ AlOps for Dell infrastructure proactive monitoring, analytics and recommendations to lower IT risk, plan ahead and improve productivity

> **CloudIQ** — cloud-based AlOps application included with Dell ProSupport and ProSupport Plus contracts

## Fortify with CloudIQ Cybersecurity

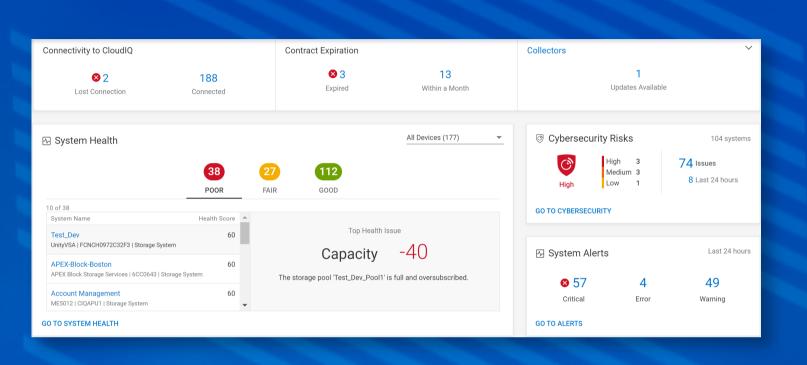
Close the IT administration-cybersecurity gap by automating the process of infrastructure security monitoring



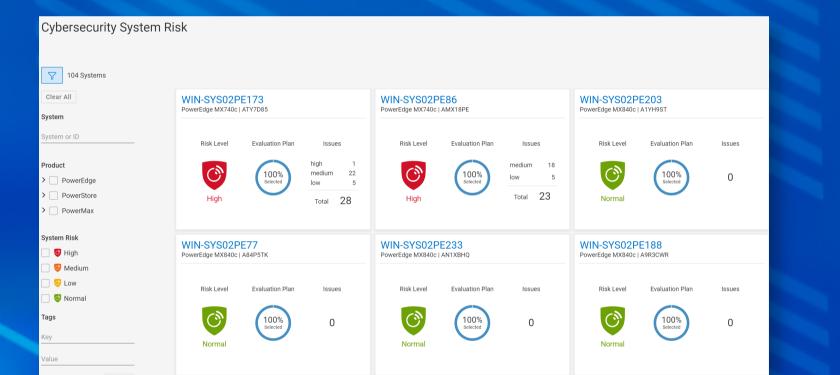
### **Reduce Risk**

#### Keep continuously aware of infrastructure security misconfigurations with:

- A summary of the number of systems with security misconfigurations and their risk levels
- Consolidated view of systems filterable by risk level, system type, location, business unit, application environment, etc.
- Clear description of the risk and recommendations for correcting security misconfigurations and lowering risk



CloudIQ overview dashboard with cybersecurity summary



 Smart Security Advisories tailored to system type and version that provide a remediation path to eliminate vulnerabilities

Enterprise-wide systems cybersecurity view

	ath 1	OJ					🗄 Manuf	acturing_Pr	Od PowerStore	1000X   RV429L62		Z LAUNCH ELEMENT MANAGER
lities							🖓 Health	Inventory	Capacity	III Performance	Cybersecurity	
							SECURITY A	SSESSMENT	SECURITY ADVISO	ORIES		
							s	ystem Risk Level		С	Cybersecurity Issues	Evaluation Plan
								Medium		5 Total 1 Last 2	<b>1</b> Jaw 1	86% 8 of 10 tests Selected
							CYBERS	ECURITY ISSUES	EVALUATION	PLAN		
							5 issues					
							Severity		Is	sue		Creation Time
							> 🚯 N	Лedium	N	ITP time synchronization is	s not configured	1 hour ago
ecurity Adviso	ries						> <b>(</b> ) N	Aedium	N	ITP time synchronization is		1 hour ago 20 hours ago
Security Adviso	ries					Туре	> <b>(</b> )	Vledium	Ν			
	ries ▲ 2 <sub>High</sub>		◆ 1 Medium	1 Low		Туре	> $ o$ M Storage	Aedium	N 4 Hypervisor		use	
Impact 4 Critical	▲ 2	Synopsis			Publist	Туре DSA-2021-134	4	<i>Medium</i>	4		Cyberse	20 hours ago
Impact 4 Critical	A 2 High	Synopsis VMware ESX	Medium	Low	Publist 07	262.00403	4	Medium	4	∍ in (	Cyberse	20 hours ago
Impact • 4 Critical Details Advisory ID	A 2 High	a terrer a	Medium Type	Low Impacted Syst	07 -	DSA-2021-134 DETAILS Advisory ID	4 Storage SYSTEMS DSA-2021-134		4 Hypervisor	> in (	Cyberse	20 hours ago
Impact  Advisory ID  Control  Mathematical  Advisory ID  Mathematical  VMSA-2021	A 2 High Impact A High Critical	VMware ESX	Medium Type Hypervisor	Low Impacted Syst	07 * 05	DSA-2021-134 DETAILS	4 Storage SYSTEMS DSA-2021-134 Dell EMC Unisphere for Pro EMC Solutions Enabler Vi	owerMax, Dell EMC Uniss tual Appliance, and Dell	4 Hypervisor phere for PowerMax Virtu EMC PowerMax Embedd	s in t xal Appliance, Dell led Management	Cyberse	20 hours ago
Impact 0 4 Critical Details Advisory ID @ VMSA-2021 @ VMSA-2021	▲ 2 High Impact ▲ High Critical	VMware ESX VMware vCe	Medium Type Hypervisor Hypervisor	Low Impacted Syst 1 1	07 <b>*</b> 05 07	DSA-2021-134 DETAILS Advisory ID Synopsis	4 Storage SYSTEMS DSA-2021-134 Dell EMC Unisphere for PC EMC Solutions Enabler Vir remediation is available for users to compromise the	owerMax, Dell EMC Unisy trual Appliance, and Dell	4 Hypervisor phere for PowerMax Virtu EMC PowerMax Embedd	s in t xal Appliance, Dell led Management	Cyberse	20 hours ago
Impact d 4 Critical Details Advisory ID @ VMSA-2021 @ VMSA-2021 @ DSA-2021-13	A 2 High Impact A High Critical A High A High Critical	VMware ESX VMware vCe Dell EMC Uni	Medium Type Hypervisor Hypervisor Storage	Low Impacted Syst 1 1 1	07	DSA-2021-134 DETAILS Advisory ID Synopsis CVSSv3 Range Impact	4 Storage SYSTEMS DSA-2021-134 Dell EMC Unisphere for PC EMC Solutions Enabler Vir remediation is available for users to compromise the 5.9 - 2.7 High	owerMax, Dell EMC Unisy trual Appliance, and Dell	4 Hypervisor phere for PowerMax Virtu EMC PowerMax Embedd	s in t xal Appliance, Dell led Management	Cyberse	20 hours ago
•••• 4 Critical           Details         Advisory ID           @          VMSA-2021           @          VMSA-2021           @          DSA-2021-13           @          DSA-2021-13	Lange Contract Contra	VMware ESX VMware vCe Dell EMC Uni Dell EMC Uni	Medium Type Hypervisor Hypervisor Storage Storage	Low Impacted Syst 1 1 1 1 1	07	DSA-2021-134 DETAILS Advisory ID Synopsis	4 Storage SYSTEMS DSA-2021-134 Dell EMC Unisphere for Po EMC Solutions Enabler Vir remediation is available for users to compromise the 5.9 - 2.7	owerMax, Dell EMC Unisy trual Appliance, and Dell	4 Hypervisor phere for PowerMax Virtu EMC PowerMax Embedd	s in t xal Appliance, Dell led Management	Cyberse	20 hours ago
Impact         4           Impact         Impact           Impact	A 2 High Impact A High O Critical Critical O Critical O Critical	VMware ESX VMware vCe Dell EMC Uni Dell EMC Uni VMware ESX	Medium Type Hypervisor Hypervisor Storage Storage Hypervisor	Low Impacted Syst 1 1 1 1 1 1	07 06 07 05 12 06	DSA-2021-134 DETAILS Advisory ID Synopsis CVSSv3 Range Impact Published	4 Storage SYSTEMS DSA-2021-134 Dell EMC Unisphere for PC EMC Solutions Enabler Vir remediation is available for users to compromise the 5.9 - 2.7 High 07-22-2021	owerMax, Dell EMC Unisş tual Appliance, and Dell or multiple security vulne affected system. 1-3156, CVE-2021-23841	4 Hypervisor phere for PowerMax Virtu EMC PowerMax Embedd rabilities that may be exp , CVE-2021-3450, CVE-20	Jai Appliance, Dell Jai Appliance, Dell Jed Management ploited by malicious	Cyberse	20 hours ago

Smart security advisories

#### Manage Policy

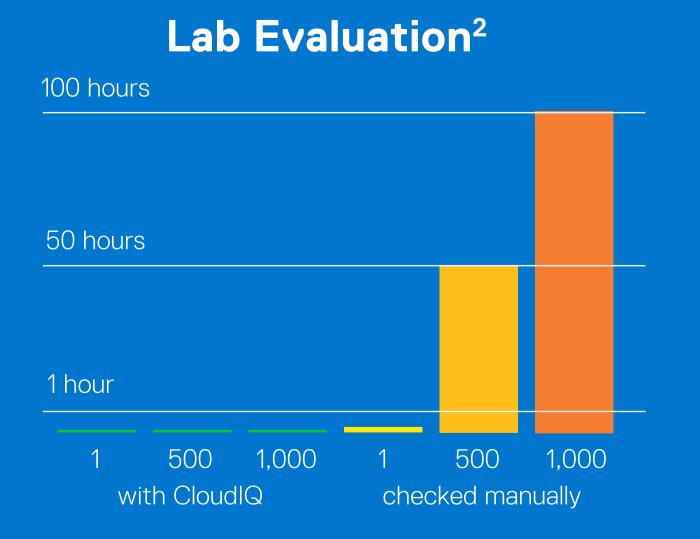
Health 🗎 Inventory 🕕 Performance	Cybersecurity	
RITY ASSESSMENT		
System Risk Level 👔	Cybersecurity Issues	Evaluation Plan
C	Ο	100% 31 of 31 tests
Normal	U	Selected
Norma		
CYBERSECURITY ISSUES EVALUATION PLAN	Ν	
aluation tests		
luation Tests	Status	Last Detected Details
Access Control	Enable 26 out of 31 Evaluation Test Selected	
Audit and Accountability	Security Control Family	Evaluation Test
Configuration Management	✓ Access Control	Details 7 out of 7 Selected
	✓ Access Control	
Identification and Authentication	✓ Access Control	
<ul> <li>Identification and Authentication</li> <li>System and Communications Protection</li> </ul>	Access Control	<ul> <li>All</li> <li>IP Blocking is enabled</li> </ul>
<ul> <li>&gt; Identification and Authentication</li> <li>&gt; System and Communications Protection</li> </ul>	✓ Access Control	<ul> <li>All</li> <li>IP Blocking is enabled</li> <li>Quick Sync Read Authentication to the server is enabled</li> <li>SSH is disabled</li> <li>The SNMP agent is configured for SNMPv3</li> </ul>
<ul> <li>&gt; Identification and Authentication</li> <li>&gt; System and Communications Protection</li> <li>&gt; System and Information Integrity</li> </ul>	Access Control	<ul> <li>All</li> <li>IP Blocking is enabled</li> <li>Quick Sync Read Authentication to the server is enabled</li> <li>SSH is disabled</li> <li>SSH is disabled</li> <li>The SNMP agent is configured for SNMPv3</li> <li>User Active Directory authentication on iDRAC is enabled</li> </ul>
Identification and Authentication System and Communications Protection System and Information Integrity	Access Control	<ul> <li>All</li> <li>IP Blocking is enabled</li> <li>Quick Sync Read Authentication to the server is enabled</li> <li>SSH is disabled</li> <li>SSH is disabled</li> <li>The SNMP agent is configured for SNMPv3</li> <li>User Active Directory authentication on iDRAC is enabled</li> <li>User Generic LDAP authentication on iDRAC is enabled</li> </ul>
<ul> <li>Identification and Authentication</li> <li>System and Communications Protection</li> <li>System and Information Integrity</li> <li>bersecurity</li> </ul>	Access Control      A	<ul> <li>All</li> <li>IP Blocking is enabled</li> <li>Quick Sync Read Authentication to the server is enabled</li> <li>SSH is disabled</li> <li>SSH is disabled</li> <li>The SNMP agent is configured for SNMPv3</li> <li>User Active Directory authentication on iDRAC is enabled</li> </ul>
<ul> <li>Identification and Authentication</li> <li>System and Communications Protection</li> <li>System and Information Integrity</li> </ul>		<ul> <li>All</li> <li>IP Blocking is enabled</li> <li>Quick Sync Read Authentication to the server is enabled</li> <li>SSH is disabled</li> <li>SSH is disabled</li> <li>The SNMP agent is configured for SNMPv3</li> <li>User Active Directory authentication on iDRAC is enabled</li> <li>User Generic LDAP authentication on iDRAC is enabled</li> <li>VNC server Disabled</li> </ul>
<ul> <li>&gt; Identification and Authentication</li> <li>&gt; System and Communications Protection</li> <li>&gt; System and Information Integrity</li> <li>&gt; bersecurity</li> </ul>	Audit and Accountability	<ul> <li>All</li> <li>IP Blocking is enabled</li> <li>Quick Sync Read Authentication to the server is enabled</li> <li>SSH is disabled</li> <li>SSH is disabled</li> <li>The SNMP agent is configured for SNMPv3</li> <li>User Active Directory authentication on iDRAC is enabled</li> <li>User Generic LDAP authentication on iDRAC is enabled</li> <li>VNC server Disabled</li> <li>3 out of 3 Selected</li> </ul>
> System and Communications Protection	Audit and Accountability         Configuration Management	<ul> <li>All</li> <li>IP Blocking is enabled</li> <li>Quick Sync Read Authentication to the server is enabled</li> <li>SSH is disabled</li> <li>SSH is disabled</li> <li>The SNMP agent is configured for SNMPv3</li> <li>User Active Directory authentication on iDRAC is enabled</li> <li>User Generic LDAP authentication on iDRAC is enabled</li> <li>VNC server Disabled</li> <li>Sout of 3 Selected</li> <li>4 out of 4 Selected</li> </ul>

CloudIQ gives you a simple way to set up automated infrastructure security configuration assessment policy:

- A template-driven tool to select security configurations that CloudIQ will compare to your systems' actual configurations
- Choice of security configurations based on the NIST 800-53 r5 standard as well as Dell Technologies best practices for each specific infrastructure system

#### Improve Productivity

Improve overall IT productivity by maintaining the health, performance, capacity and cybersecurity of infrastructure



With CloudIQ, spend only 3 minutes to set policy and automate security configuration checking for up to 1,000 systems vs. 6 minutes to manually check every system

#### Lab Test Results<sup>2</sup>



to set policy and automate security configuration checking for up to 1,000 systems

Click <u>here</u> to see a short CloudIQ Cybersecurity demo. For more demos, data sheets and white papers visit:

www.DellTechnologies.com/CloudlQ

<sup>1</sup>OWASP Top Ten-2021, Open Web Application Security Project Foundation, 2021.

<sup>2</sup>Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation," a Dell Technologies Direct from Development White Paper, 2022. Actual results may vary.

© 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies is a trademarks of Dell Inc. or its subsidiaries. Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice.