How AIOps Expands Zero Trust Assurance Across the Server Landscape

Observability and intelligent advisories eliminate cybersecurity drudgery.

By Ira Miga, Cybersecurity Product Manager

Using the power of AI to advance organizations' cybersecurity, Dell Technologies has extended its CloudIQ AIOps application's cybersecurity capabilities for Dell PowerEdge servers. CloudIQ simplifies cybersecurity processes by eliminating manual checking for infrastructure security configuration risks, making organizations aware of newly discovered vulnerabilities faster and providing recommendations for remediating those issues.

CloudIQ is web-based software-as-a-service that comes with Dell ProSupport and ProSupport Plus contracts. It provides IT operations teams with a single productivity-enhancing, enterprise-wide view of the health, cybersecurity and environmental sustainability of Dell's modern data infrastructure portfolio. And that includes servers, storage, data protection, hyperconverged and network systems and a growing set of Dell APEX multicloud services.

Expanded Risk Observability

CloudIQ cybersecurity configuration risk observability now extends beyond its previous support of Dell PowerEdge rackmount and tower servers to include PowerEdge Modular Infrastructure. CloudIQ also provides this capability for Dell PowerStore and PowerMax primary storage systems.

Strong cybersecurity configuration settings that help prevent unwanted access to infrastructure are essential building blocks of a Zero Trust security foundation. Systems have multiple security settings (e.g., for different subcomponents and functions), and they can be easily misconfigured or inadvertently left open after legitimate system administration tasks are performed. With so many systems in a typical IT environment, and so many security configurations per system, it is impractical to manually check every system even once a day.

CloudIQ AIOps continuously assesses infrastructure for misconfigurations, displays risk levels of discovered misconfigurations, notifies system administrators or security staff and recommends actions to reestablish security. Lab testing shows that it can take six minutes to check just half of a single system's settings once[1], while CloudIQ continuously assesses thousands of systems hands-free and recommends the right security settings according to your predefined policy. This eliminates manual checking while keeping you fully aware of risks and how to eliminate them.

Intelligent Security Advisories

CloudIQ intelligent security advisories now extend beyond their previous support for primary storage systems to include PowerEdge servers.

Security advisories inform organizations about newly discovered IT infrastructure vulnerabilities, which criminals can exploit, and recommends actions, such as applying security patches to eliminate the vulnerabilities. Traditional IT equipment vendor-supplied advisories are email-based and require users to manually verify their systems' hardware, firmware and software versions to validate which systems are vulnerable. This can take hours and sometimes days of work before you're even ready to apply a recommended security patch.

Fortunately, CloudIQ AIOps is fully aware of each system's details, pinpointing which systems are impacted by each advisory and recommending actions. This relieves staff of manual drudgery and accelerates remediation.

Integration for Automating ITSM, SIEM and SOAR

CloudIQ Webhook was launched last year as a mechanism to integrate CloudIQ infrastructure health issue notifications with applications such as ServiceNow for ticketing, PagerDuty for incident management and Microsoft Teams and Slack for collaboration.

CloudIQ Webhook will integrate cybersecurity risk notifications with third-party IT management software to automate IT service management (ITSM), security information and event management (SIEM) and security orchestration, automation and response (SOAR) processes for speeding cybersecurity remediation.

The CloudIQ Webhook expansion will send cybersecurity risk notifications to third-party applications such as ELK Stack, Splunk and Rapid7 for security information and event management, as well as Palo Alto Networks Cortex XSOAR, IBM QRadar and Splunk for security orchestration automation and response.

Dell provides users with documentation for directing CloudIQ Webhook to push its system health and cybersecurity notifications to their chosen applications. This saves users days to weeks of programming from scratch to automate IT and cybersecurity processes.

See the CloudIQ see the CloudIQ cybersecurity demo, cybersecurity configuration and advisory infographics and more on our CloudIQ AIOps homepage.

Cybersecurity configuration risk observability and intelligent security advisories are available now for Dell primary storage (PowerStore, PowerMax) and servers (PowerEdge). Webhook support for cybersecurity risk notifications are planned for December 2023.

About the Author

Ira Miga, Cybersecurity Product Manager

At Dell Technologies, Ira works closely with engineering, design, and quality assurance to define product requirements and to prioritize and guide the development process for CloudIQ cybersecurity features. She also monitors product performance, gathers customer feedback and plans releases and enhancements. With 20 years' experience, Ira previously held engineering positions at cybersecurity vendor Imperva, ISP Bezeq International and the Israeli Navy. She is multi-lingual and earned an MBA in Business Consulting at Coller School of Management, Tel Aviv University.

[1]Dell CloudIQ Cybersecurity for PowerEdge: The Benefits of Automation," a Dell Technologies Direct from Development White Paper, 2022. Actual results may vary.

.