DELL Technologies

Product Brief

APEX AIOps for Infrastructure Cybersecurity

Keep infrastructure safe with continuous cybersecurity risk observability and recommended actions.

Up to 10x faster
to resolve issues.[1]

Save 1 workday
per week on average.[1]

<3 minutes to automate
security checks for 1,000 systems.[2]

Reduce known risks
Intelligent, automated security for servers and storage keeps you aware of risks 24/7 and recommends actions to resolve them.

Proactively address vulnerabilities
Intelligent security advisories pinpoint servers and storage with common vulnerabilities and exposures, and recommend corrective actions.

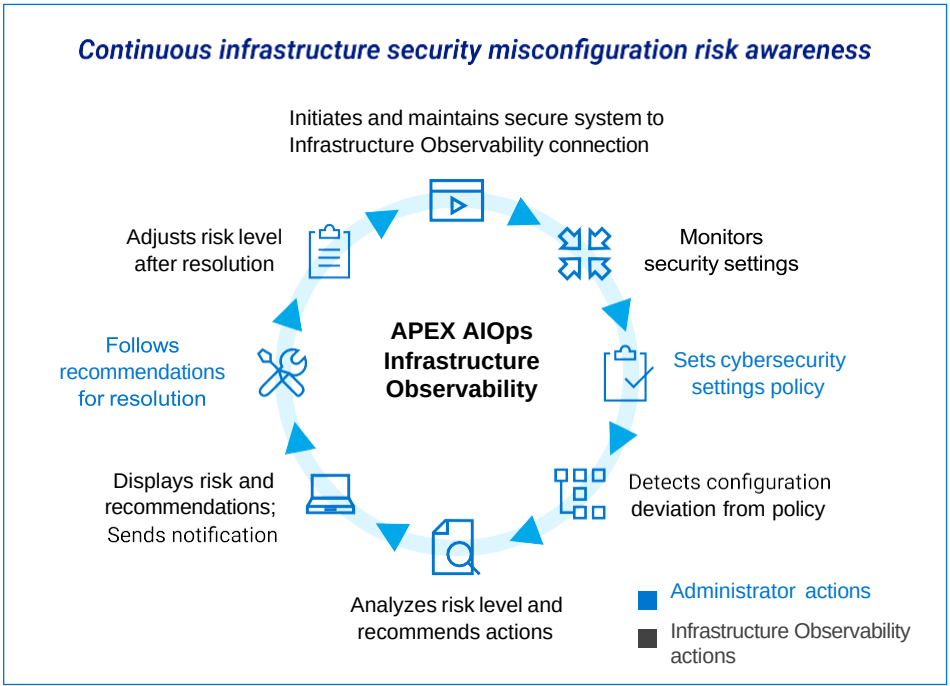
Stop ransomware attacks
Intelligent, automated data storage analysis detects ransomware attacks as they unfold so you act fast to mitigate the attack and minimize damage.

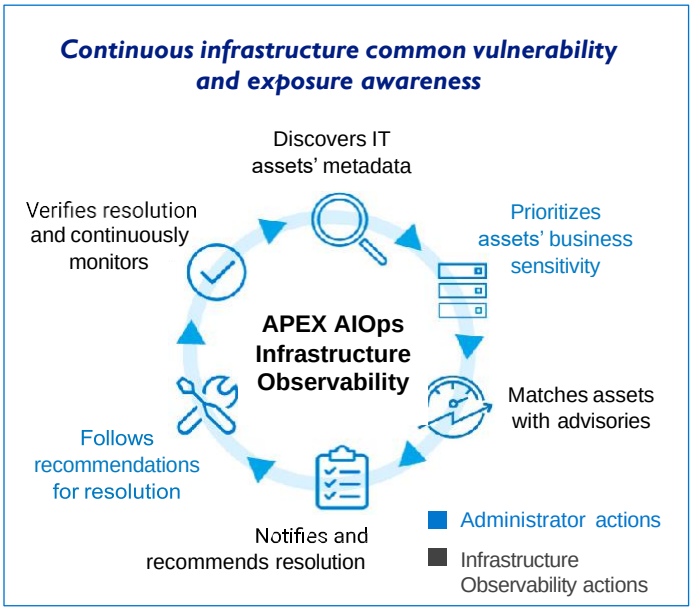
IT operations and security teams face significant challenges in managing security settings, researching new vulnerabilities, and responding to ransomware attacks. APEX AIOps Infrastructure Observability (Infrastructure Observability), a software-as-a-service solution for Dell on-premises infrastructure and Dell APEX multicloud services, can handle these tasks for you.

Infrastructure Observability is a web-based, highly secure platform trusted by thousands of organizations worldwide to ensure the health, cybersecurity, and sustainability of their Dell infrastructure. This service is included at no additional cost with Dell ProSupport service contracts.

Reduce risk with automated cybersecurity assessments
Strong cybersecurity configuration settings are crucial for preventing unauthorized access and form the foundation of a Zero Trust security model. However, systems often have multiple security settings that can be easily misconfigured or unintentionally left open after legitimate administrative tasks.

With Infrastructure Observability, you can specify your desired security settings. The platform will continuously monitor your infrastructure for any misconfigurations, alert your team, and recommend corrective actions to restore security. It also displays each system's risk level based on its misconfigurations, allowing you to prioritize and address the most critical risks first.





Address vulnerabilities faster with intelligent security advisories
Security advisories alert you to newly discovered common vulnerabilities and exposures that could be exploited by criminals. Traditional IT equipment vendors' security advisories are email-based and require hours, even days, to manually review and then verify against your systems.

Infrastructure Observability continuously monitors your Dell systems, identifies their exact versions, and matches them with relevant Dell Security Advisories. It then recommends actions, such as applying security patches, to eliminate vulnerabilities. This automation reduces manual effort, minimizes exposure, and speeds up resolution.

Stop ransomware attacks as soon as they begin
Infrastructure Observability monitors storage for data encryption, a key indicator of a ransomware attack that is unfolding. When data encryption occurs, data becomes incompressible and cannot be deduplicated. Using an AI-based anomaly detection algorithm, Infrastructure Observability identifies these reducibility anomalies and alerts you when an attack is underway.

Incident details reveal the impacted data, the time of the attack, and which servers and applications were involved. This enables you to mitigate the attack by isolating suspicious servers or creating secure snapshots of unprotected storage groups to limit the damage.

Infrastructure Observability displaying ransomware detection

Enterprisewide risk dashboard simplifies cybersecurity assurance
Infrastructure Observability features a comprehensive cybersecurity risk dashboard, which displays risk levels for each Dell system in individual cards. You can filter the dashboard by risk level (e.g., low, medium, high), technology (e.g., servers, data storage, data protection), and custom tags (e.g., location, business unit, application).

Risk levels are determined by the severity of security misconfigurations, common vulnerabilities and exposures, and ransomware activity. Each card shows the number of issues per risk category, and you can click on a system's card to view detailed information and remediation recommendations.

Integration for automating ITSM, SIEM and SOAR
Infrastructure Observability's webhook, an API (application programming integration) pushes infrastructure cybersecurity risk notifications to third-party IT management applications. Allowing you to automate IT service management (ITSM), security information and event management (SIEM) and security orchestration, automation and response (SOAR) processes for speeding time to resolution.

Webhook will push its cybersecurity risk notifications for third-party applications such as: ServiceNow for ticketing, ELK Stack, Splunk and Rapid7 for security information and event management; Palo Alto Networks Cortex XSOAR; IBM QRadar and Splunk for security orchestration automation and response; and Slack and Teams for escalation. Infrastructure Observability's shared email notification and role-based access dashboards further improve efficiency.

Learn more about Dell APEX AIOps solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation with #DellTech

DELL Technologies

[1] *Dell User Survey, Dell Technologies, 2021. Actual results may vary.*
[2] *The Total Economic Impact™ Of IBM Instana Observability Cost Savings and Business Benefits Enabled By Instana Observability," Forrester, 2024. Actual results may vary.*
[3] *Customer research, Dell Analysis, 2023. Actual results may vary.*