August 9, 2023

Dynatrace Unveils Security Analytics, Providing Actionable Insights for Proactive Defense Against Threats to Cloud Applications

Leverages the Dynatrace platform's Davis AI to enable threat hunting and real-time detection and incident response

WALTHAM, Mass.--(BUSINESS WIRE)-- Dynatrace (NYSE: DT), the leader in unified observability and security, today announced the introduction of Security Analytics, a new Dynatrace® platform solution designed to help organizations better defend against threats to their hybrid and multicloud environments. Dynatrace® Security Analytics leverages Davis® AI, which combines predictive and causal AI techniques to provide security analysts with the precise answers and data context they need to prioritize and investigate threats and vulnerabilities. Later this year, Security Analytics will also include generative AI capabilities as part of Dynatrace's planned expansion to provide a hypermodal AI offering through Davis. In addition, Security Analytics now leverages Dynatrace® AutomationEngine to create automations and workflows that analysts can use to assess the impact of an attack, find the indicators of compromise (IOCs), or automatically trigger a response. Combining Davis hypermodal AI, precise answers with context, and intelligent automation empowers security analysts to defend against emerging cyber threats proactively. It also bolsters their organization's cybersecurity defense and overall security posture.

Security analysts often lose productivity due to disjointed tools and processes that require considerable human intervention. This approach can result in alerts going uninvestigated for months or years, posing significant risks to their organizations. Many teams rely on traditional Security Information and Event Management, or SIEM solutions, that monitor log data to find IOCs. This data lacks crucial context, such as the underlying cloud infrastructure and application topology, which can help narrow the scope of an investigation. Missing this context makes it difficult to use SIEM solutions to accelerate an investigation or identify and defend against cyber threats.

Allie Mellen, Senior Analyst at Forrester Research, wrote, "Security information and event management (SIEM) capabilities alone are no longer sufficient for security operations teams. Today's security analytics platforms combine features to enable analytics, investigation, automation, threat hunting, dashboards, and reporting to help security analysts be more effective." [i]

Dynatrace Security Analytics addresses these needs by fueling the answers and automation it delivers with logs, metrics, traces, and topology while keeping data context intact. This enables teams to identify and investigate threats that may be impossible to pinpoint from logs alone. Furthermore, Security Analytics adds to other Dynatrace application security

capabilities. These include:

- **Runtime vulnerability analytics**, which provides real-time detection and prioritization of vulnerabilities that have escaped into production environments.
- **Runtime application protection**, which detects and blocks common application attacks, like SQL injection, command injection, and JNDI attacks.

Dynatrace was recently ranked #1 in the Security Operations Use Case, with a score of 4.6 out of 5, in the 2023 Gartner Critical Capabilities for APM and Observability Report, which the company believes reflects the impact and customer value of its platform's application security capabilities.

Steve Tack, SVP of Product Management at Dynatrace, said, "In today's rapidly evolving threat landscape, organizations face an unprecedented risk of cyberattacks that can wreak havoc on their operations and customers' trust. With Dynatrace Security Analytics, analysts can quickly investigate and verify what happened and leverage observability and security data in full context to analyze and take proactive action to strengthen defenses. Combining these new security analytics with our platform's other application security capabilities enables our customers to successfully deliver digital transformation with the confidence that their hybrid and multicloud environments are well protected."

Dynatrace Security Analytics is available to customers today. For additional information, please visit the Dynatrace website or blog.

Gartner Disclaimer

Gartner, Critical Capabilities for Application Performance Monitoring and Observability, Mrudula Bangera, Padraig Byrne, Matt Crossley, Gregg Siegfried, 10 July 2023

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Dynatrace

Dynatrace (NYSE: DT) exists to make the world's software work perfectly. Our unified platform combines broad and deep observability and continuous runtime application security with the most advanced AIOps to provide answers and intelligent automation from data at an enormous scale. This enables innovators to modernize and automate cloud operations, deliver software faster and more securely, and ensure flawless digital experiences. That's why the world's largest organizations trust the Dynatrace® platform to accelerate digital transformation.

Curious to see how you can simplify your cloud and maximize the impact of your digital

teams? Let us show you. Sign up for a free 15-day Dynatrace trial.

Cautionary Language Concerning Forward-Looking Statements

This press release includes certain “forward-looking statements” within the meaning of the Private Securities Litigation Reform Act of 1995, including statements regarding the anticipated benefits of Dynatrace Security Analytics and the timing of the expansion of Davis AI to include generative AI. These forward-looking statements include all statements that are not historical facts and statements identified by words such as “will,” “expects,” “anticipates,” “intends,” “plans,” “believes,” “seeks,” “estimates,” and words of similar meaning. These forward-looking statements reflect our current views about our plans, intentions, expectations, strategies, and prospects, which are based on the information currently available to us and on assumptions we have made. Actual results may differ materially from those described in the forward-looking statements and will be affected by a variety of risks and factors that are beyond our control, including risks set forth under the caption “Risk Factors” in our Quarterly Report on Form 10-Q filed on August 2, 2023 and our other SEC filings. We assume no obligation to update any forward-looking statements contained in this document as a result of new information, future events, or otherwise.

---

[i]The Forrester Wave™: Security Analytics Platforms, Q4 2022

View source version on businesswire.com:
https://www.businesswire.com/news/home/20230809689107/en/

Kara McCrudden
kara.mccrudden@dynatrace.com

Source: Dynatrace