Datadog Adds Identity, Vulnerability and App-Level Findings to Security Inbox to Help DevOps and Security Teams Address Issues Quickly

November 27, 2023 at 12:00 PM EST

The new capabilities empower DevOps teams to improve security posture, from code to cloud to application, by focusing only on the security problems that matter

LAS VEGAS , Nov. 27, 2023 /PRNewswire/ -- Datadog, Inc. (NASDAQ: DDOG), the monitoring and security platform for cloud applications, today at AWS re:Invent added identity, vulnerability and app-level findings to Security Inbox. This provides engineers with one actionable view to improve security posture, without any additional overhead or friction. With these new features, Datadog shifts cloud security earlier in the software development lifecycle and empowers developers and security teams to address issues proactively.

Datadog's Security Inbox delivers a unified view of the top issues DevOps and security teams need to address to significantly reduce risk across cloud accounts, Kubernetes clusters, containers and applications. With the capabilities announced today, Datadog helps proactively detect and address identity and access-related risks with the general availability of its Cloud Infrastructure and Entitlement Management (CIEM). And Security Inbox's new vulnerability management capability detects, prioritizes—based on heuristics like exposure risk, probability of being exploited and all observability context—and helps remediate infrastructure vulnerabilities in hosts, containers and applications.

"Security Inbox gives DevOps and security teams a prioritized list of actionable fixes they can deploy to maximize improvements to their security posture," said Prashant Prahlad, VP of Cloud Security Products at Datadog. "With the added capabilities to Security Inbox, engineers can now proactively mitigate issues without requiring the security teams to inform them about the urgency or the impact of their security fixes. Meanwhile, security teams continue to save precious time lost to tedious contextualisation and triage work, and can choose to focus on overall security posture of their cloud estates."

With the new capabilities announced today, Security Inbox gives organizations:

- **Full App-to-Infrastructure Visibility:** Security Inbox unifies findings collected by Datadog Cloud Security Management and Application Security Management into a single view, simplifying the process of managing security issues.
- **Context-Based Prioritization:** The capability incorporates context from potential suspicious activity detected from cloud logs, application traces or file and process activity detected on the host, enabling teams to concentrate on issues with a high likelihood of impact.
- **Correlation and Attack Path Detection:** Datadog uses agentless cloud integrations, one agent and tracing libraries to map the relationships between an organization's entire stack, spanning from cloud resources and compute resources to applications. When a combination of risks suggesting a potential attack path in the environment is detected, a security issue is generated and displayed in Security Inbox.

These features are now generally available. To learn more, please visit booth #732 at AWS re:Invent or read more here: https://www.datadoghq.com/blog/security-inbox.

About Datadog

Datadog is the observability and security platform for cloud applications. Our SaaS platform integrates and automates infrastructure monitoring, application performance monitoring, log management, real-user monitoring, and many other capabilities to provide unified, real-time observability and security for our customers' entire technology stack. Datadog is used by organizations of all sizes and across a wide range of industries to enable digital transformation and cloud migration, drive collaboration among development, operations, security and business teams, accelerate time to market for applications, reduce time to problem resolution, secure applications and infrastructure, understand user behavior, and track key business metrics.

Forward-Looking Statements

This press release may include certain "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, or the Securities Act, and Section 21E of the Securities Exchange Act of 1934, as amended including statements on the benefits of new products and features. 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 are subject to a variety of assumptions, uncertainties, risks and factors that are beyond our control, including those risks detailed under the caption "Risk Factors" and elsewhere in our Securities and Exchange Commission filings and reports, including the Quarterly Report on Form 10-Q filed with the Securities and Exchange Commission on May 5, 2023, as well as future filings and reports by us. Except as required by law, we undertake no duty or obligation to update any forward-looking statements contained in this release as a result of new information, future events, changes in expectations or otherwise.

Contact
Dan Haggerty
press@datadoghq.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/datadog-adds-identity-vulnerability-and-app-level-findings-to-security-inbox-to-help-devops-and-security-teams-address-issues-quickly-301998043.html

SOURCE Datadog, Inc.