



Datadog Announces Security Monitoring

November 21, 2019

NEW YORK--(BUSINESS WIRE)--Nov. 21, 2019-- Datadog (Nasdaq: DDOG), the monitoring and analytics platform for developers, IT operations teams and business users in the cloud age, today announced Security Monitoring, a new product that enables real-time threat detection across the entire stack and deeper collaboration between security, developers, and operations teams.

Modern security teams work closely with developers and operations as they build new products, to help them protect against threats in cloud-native environments. At the same time, security teams increasingly require the same visibility that developers and operations do. To address these challenges, Datadog's Security Monitoring product processes monitoring data from the infrastructure, the network, applications, and security devices to surface potential threats. With threat detection rules directly operating in real-time on ingested streams, Datadog's Security Monitoring maximizes coverage without any of the traditionally associated performance or cost concerns.

"Our customers are moving into a world in which security must become a shared responsibility across engineering teams to address the increased complexity and scale of their environments," said Marc Tremzal, Director of Product Management at Datadog. "We built Security Monitoring to break down silos between security professionals and their DevOps peers, and provide real-time threat detection in modern hybrid cloud environments."

Datadog Security Monitoring provides powerful threat detection with the following capabilities:

- **Unique Security Insights:** Observability data, including infrastructure metrics, traces, and logs from Datadog's 350+ existing integrations, and security-related integrations including AWS GuardDuty, AWS CloudTrail, Okta, Google Suite, and others -- combined in one platform to provide high fidelity security signals.
- **Out-of-the-Box and Editable Threat Detection Rules:** Rules curated by Datadog to detect widespread attacker techniques, so users can get started in minutes, without professional services. Users can also write and fine-tune their own rules without learning a proprietary query language.
- **Real-Time Detection "Without Limits":** Rules are applied in real-time, as logs and events are ingested, with no prerequisite to index them.
- **Collaborative Investigations with Existing Tools:** Email, Slack, PagerDuty, JIRA, ServiceNow, etc. Reach developers and security users where they already work.

Datadog's Security Monitoring brings greater visibility with one centralized platform shared by development, operations, and security teams.

"Our developers and operations already rely on Datadog for observability, so we've been looking to leverage this comprehensive data for security," said Martin Stryček, Head of Infrastructure at Kiwi.com. "With Datadog's new Security Monitoring product, our AppSec team can analyze authentication events across all our applications with a single set of rules."

Security Monitoring will be demonstrated at Datadog's booth in The Venetian, #2814, at AWS re:Invent in Las Vegas, from Monday, December 2nd to Thursday, December 5th. For additional information, please visit the blog post [here](#).

About Datadog

Datadog is the monitoring and analytics platform for developers, IT operations teams and business users in the cloud age. Our SaaS platform integrates and automates infrastructure monitoring, application performance monitoring and log management to provide unified, real-time observability of 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 and business teams, accelerate time to market for applications, reduce time to problem resolution, understand user behavior and track key business metrics.

Forward-Looking Statements

This press release includes certain "forward-looking statements" within the meaning of federal securities laws, including statements concerning the potential advantages and capabilities of our Security Monitoring product. 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: risk of interruptions or performance problems associated with our products and platform capabilities; our ability to adapt and respond to rapidly changing technology or customer needs; the competitive markets in which we participate; general market, political, economic, and business conditions; and 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 November 13, 2019, 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.

Source: Datadog

For Datadog
Martin Bergman
press@datadoghq.com