Datadog Unveils Modern Approach to Cloud SIEM to Deliver Risk-Based Insights, Scalability, Cost Efficiency and Real-Time Detection

December 2, 2024 at 9:00 AM EST

Datadog's Cloud SIEM leverages modern architectures and machine learning to ensure organizations can meet their security goals without the limitations of outdated systems

NEW YORK, Dec. 2, 2024 /PRNewswire/ -- Datadog, Inc. (NASDAQ: DDOG), the monitoring and security platform for cloud applications, today announced its modern approach to Cloud SIEM, which doesn't require dedicated staff or specialized teams to activate the solution. This approach makes it easy for teams to onboard, de-risk migrations and democratize security practices while disrupting traditional models, which can be costly and resource intensive.



Existing SIEM (security information and event management) solutions face several significant challenges that put security teams at risk. Traditional SIEMs often struggle to integrate data from diverse sources, leading to fragmented visibility and delayed detection and response. As organizations grow and data volumes increase, legacy systems and their required dedicated teams become overwhelmed, resulting in inefficiencies at cloud scale and rising operational costs. The high amount of false-positive alerts from these traditional solutions can also lead to alert fatigue, causing critical threats to be overlooked.

Datadog's Cloud SIEM leverages modern architectures and machine learning to address these challenges and emphasize agility, scalability, cost-efficiency and real-time threat detection. Organizations like Lenovo, FanDuel, Carvana, University of Alabama at Birmingham (UAB) and Vanilla Technologies rely on this modern approach to rapidly onboard new sources for threat detection, help them prioritize security investigations and resolve issues quickly.

"Datadog Cloud SIEM's ability to add custom data sources helps the SOC at UAB improve our alerts. Using specific facets we are able to create high fidelity alerts and can pivot into investigating and responding seamlessly. This overall has improved our security posture," said Daniel Studdard, Information Security Engineer at the University of Alabama at Birmingham.

As part of Datadog's unified platform, features of Cloud SIEM include:

- **Risk-Based Insights**: Teams can correlate real-time signals and findings into entities in order to streamline the way security teams prioritize investigations. Risk scoring includes Cloud Security Management insights such as misconfigurations and identity risks, as well as expanded entity types like S3 buckets, EC2 instances, and SAML and web users, to help teams detect, prioritize and respond to threats.
- **15-Months Retention**: Datadog offers 15-months retention and Flex Logs with Cloud SIEM to provide customers with a flexible economic model that delivers powerful threat detection capabilities without overspending. This flexible approach allows organizations to scale security operations as needed while optimizing resources, enabling cost efficiency without sacrificing performance.
- **Security Operational Metrics**: Cloud SIEM provides deep insights into the performance of security teams, helping to assess how effectively they respond to and resolve threats in cloud environments. These metrics are readily available through pre-built dashboards and detailed reports, offering valuable data such as detection rule coverage, alert response times and investigation outcomes that help teams continuously optimize their threat response strategies.
- **Content Packs and Out-of-the-box Integrations**: With pre-built detection rules, dashboards and workflow automation tools tailored to integrations with leading technologies, organizations can leverage out-of-the-box content to accelerate threat detection and response. More than 30 integrations and Content Packs have been added in the past six months,

including Abnormal Security, Atlassian Organization Logs, Cisco Secure Endpoint, Cisco Umbrella DNS, Gitlab Audit Logs, Imperva WAF logs, Lastpass, Mimecast, SentinelOne, Sophos Central Cloud, Trend Micro Email Security, Trend Micro Vision One XDR and more.

- **Datadog Security Labs**: Backed by Datadog's Threat Detection Research and Engineering team, Cloud SIEM ensures continuous innovation and momentum in threat detection. With unparalleled expertise and data insights, Datadog empowers organizations to not only migrate seamlessly but also stay ahead of emerging threats in today's evolving security landscape.

"Today's security threats require a modern approach that can help teams reliably detect, prioritize, investigate and resolve issues," said Yash Kumar, Senior Director of Product at Datadog. "Datadog's Cloud SIEM delivers that modern approach with a unified platform for observability and security that provides easy onboarding into the product with out-of-the-box content, deep threat detection, full-stack context and visualizations."

To learn more about Datadog Cloud SIEM, please visit: https://www.datadoghq.com/product/cloud-siem/.

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, user experience monitoring, cloud security 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 8, 2024, 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-unveils-modern-approach-to-cloud-siem-to-deliver-risk-based-insights-scalability-cost-efficiency-and-real-time-detection-302319100.html

SOURCE Datadog, Inc.