Datadog's State of Cloud Security 2024 Finds Room for Improvement in the Use of Long-Lived Credentials Across All Major Clouds

October 21, 2024 at 4:05 PM EDT

The report found that 46% of organizations are using unmanaged users with long-lived credentials

NEW YORK, Oct. 21, 2024 /PRNewswire/ -- Datadog, Inc. (NASDAQ: DDOG), the monitoring and security platform for cloud applications, today announced its new report, the *State of Cloud Security 2024*. The report found that long-lived credentials continue to be a major risk for organizations across all cloud providers.

Long-lived cloud credentials never expire and frequently get leaked in source code, container images, build logs and application artifacts, making them a major security risk. Research has shown that they are the most common cause of publicly documented cloud security breaches. While the risks are well documented, Datadog's report found that almost half (46%) of organizations are still using unmanaged users with long-lived credentials.

According to the report, not only are long-lived credentials widespread across all major clouds, they are also often old and even unused. 62% of Google Cloud service accounts, 60% of AWS IAM users and 46% of Microsoft Entra ID applications have an access key older than one year.

"The findings from the *State of Cloud Security 2024* suggest it is unrealistic to expect that long-lived credentials can be securely managed," said Andrew Krug, Head of Security Advocacy at Datadog. "In addition to long-lived credentials being a major risk, the report found that most cloud security incidents are caused by compromised credentials. To protect themselves, companies need to secure identities with modern authentication mechanisms, leverage short-lived credentials and actively monitor changes to APIs that attackers commonly use."

Other key findings from the report include:

- Adoption of cloud guardrails is on the rise—79% of S3 buckets are covered by an account-wide or bucket-specific S3 Public Access Block, up from 73% a year ago—thanks to cloud providers starting to enable guardrails by default.
- More than 18% of AWS EC2 instances and 33% of Google Cloud VMs have sensitive permissions to a project. This puts organizations at risk as any attacker compromising the workload is able to steal associated credentials and access the cloud environment.
- 10% of third-party integrations have risky cloud permissions, allowing the vendor to access all data in the account or to take over the whole AWS account. 2% percent of third-party integration roles don't enforce the use of External IDs, which allows an attacker to compromise them through a "confused deputy" attack.

For the report, Datadog analyzed security posture data from a sample of thousands of organizations using AWS, Azure or Google Cloud.

Datadog's *State of Cloud Security 2024* is available now. To dive deeper into the findings, read the blog. Learn more about how Datadog helps companies secure their cloud environments.

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/datadogs-state-of-cloud-security-2024-finds-room-for-improvement-in-the-use-of-long-lived-credentials-across-all-major-clouds-302282005.html

SOURCE Datadog, Inc.