

Resurface Labs Joins Google Cloud Partner Advantage

Approved Integration with Google Kubernetes Engine Establishes a Foundation for Enterprise-Scale, Multi-Cloud API Security

BOULDER, CO, UNITED STATES, April 19, 2023 /EINPresswire.com/ --

[Resurface Labs, Inc.](#) today announced that it has joined the Google Cloud Partner Advantage program as Build

Partner, to better enable organizations with the ability to effectively manage their multi-cloud API attack surface. Leveraging the power and scalability of Google Kubernetes Engine (GKE), the Resurface Runtime API Security product establishes an exabyte-scale API Security Data Lake that comprehensively consolidates and analyzes API transactions from multiple API deployments

“

Being able to deploy Resurface Runtime API Security into a highly performant and scalable Kubernetes environment like GKE is a true game changer for enterprise-scale API security at runtime.”

Don Leatham, EVP Alliances and Partnerships, Resurface Labs

across the customer’s multi-cloud environment. Resurface continually monitors the API data lake for attacks, threats, and weaknesses, providing meaningful alerts and powerful investigation tools and views for DevOps and SecOps personnel.

As a Google Cloud partner, Resurface Labs offers customers the ability to augment their current perimeter-centric security (e.g., web application firewalls, API gateways) with runtime capture and analysis of complete API transactions. Key features include:

- Accelerated Time to API Security - Resurface Runtime API Security deploys in minutes into the customer’s GKE

environment with Helm charts tuned specifically for GKE

- Comprehensive Multi-Cloud Capture - A wide range of API transaction capture options are provided and can be deployed in a range of cloud-provider environments
- Full Security Context - Each API transaction is analyzed and tagged for attacks, threats and weaknesses, establishing security context that powers alerts, investigations, and forensics
- Global-Enterprise Scale - An exabyte-scale, distributed data query engine powers the



Resurface Labs

Resurface API Security Data Lake. Data is accessible via standard SQL as well as text searches, and the data model is open source, to facilitate access by a range of security tools

- Runtime Monitoring and Detection - The console continuously monitors the enterprise API security attack surface for inbound attacks and threats at runtime
- Alerts, Context, Guidance - Tunable alerts, that do not contribute to alert fatigue, provide DevOps and SecOps teams the security context and remediation guidance to quickly respond to API attacks and threats

"We are excited to be a Google Cloud Partner, working with Google Cloud to provide highly scalable runtime API security for Google Cloud customers concerned about their API attack surface," stated Don Leatham, EVP Alliances and Partnerships, Resurface Labs. "Being able to deploy Resurface Runtime API Security into a highly performant and scalable Kubernetes environment like GKE is a true game changer for customers seeking comprehensive, enterprise-scale API security at runtime."

"We are excited to welcome Resurface Labs to the Google Cloud Partner Advantage ecosystem," said Kim Lassetter, Global Director, Partner Advantage Program, Google Cloud. "By bringing its platform to Google Cloud, Resurface Labs' customers will have access to global, trusted cloud infrastructure and greater capabilities to effectively manage their multi-cloud API attack surface."

For additional information about Resurface Lab's Runtime API Security, please visit resurfacelabs.com.

About Resurface Labs Inc.

Resurface Runtime API Security provides comprehensive API transaction capture, analysis, and monitoring to help enterprises manage their API attack surface. Mapped to OWASP API Top 10, Resurface alerts on API attacks and threats, providing unfiltered and non-redacted data for full security context. Purpose-built for API data, Resurface captures complete request and response payloads into a highly scalable and performant security data lake, which enables deep inspection, pattern understanding, and API auditing.

Kimberly Doyle

Kimberly Communications

kb@kimberlycommunications.com

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/628643511>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire,

Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.