Dig for Technology

Riskified Lowers Transactional Risk

With Dig

Less than 1 day
data onboarding

2-hour alert
identification

Less than ½-day
ROI

Risk is not just the root of Riskified's name; it's part of the company's DNA.

A leading provider of online fraud detection solutions for world-leading ecommerce platforms, Riskified has a clear mandate – to understand, quantify, and minimize the risk of millions of consumer transactions crossing its path each day.

From the day it was established in 2013, Riskified began to accumulate and store consumers' personal identifiable information (PII) – first on-prem and then in the cloud. And as the company continued to grow, so did its data... as well as the risk of it being exposed or breached. Moreover, as a publicly-traded company, Riskified had to ensure the highest level of data governance and compliance, including SOX and ITGC, for the reams of data continuously moving across myriad state and country borders.

"At first, our CTO started a data governance initiative by creating a data catalog to keep track of data lineage, usability and freshness," Riskified CISO Yossi Yeshua says. "And then we added our security requirements on top of that."

Addressing visibility and risk

As part of those requirements, Riskified looked for appropriate tools to tackle two main areas – data visibility and risk. “Even though we had already invested in a cloud security posture management (CSPM) solution, it lacked deep data classification and discovery capabilities,” Yeshua says. “We are a data-driven company, but we couldn’t understand where the data was and how it was being stored. We couldn’t ‘know the unknown’ in order to apply governance. And we had no data visibility: We couldn’t see the data to confirm that what we had assumed to be there was actually there.” For Riskified, it was also essential to be able to identify data-related risks.

“In our AWS data that contains lots of PII, the type of information that consumers must provide when carrying out an ecommerce transaction,” Yeshua says. “But we didn’t have the data context to recognize existing risks. As a company in the risk assessment business, we appreciate the importance of identifying and quantifying the risk of sensitive data in our possession.”

So, Riskified embarked on a data security posture management (DSPM) solution search. The company checked out several offerings, but none of them were the right fit. That is, until Yeshua heard about Dig Security.

Mastering a customized terraform deployment

“After meeting with a dozen or so vendors, we discovered Dig and liked what we saw,” Yeshua says. To move the process forward, Riskified carried out a simultaneous PoC with Dig and other DSPM vendors at the end of 2022. “We build customized terraform modules, so it was vital to find a vendor that could work smoothly with that type of deployment,” he says. “Some of the vendors tried to integrate their solution into each AWS account, including creating resources for each. In contrast, Dig created a single, centralized account to facilitate account management and monitoring.”

Riskified also liked Dig’s agility and flexibility when it came to customizing its deployment, which took less than a day. And the company appreciated the fact that Dig delivered results rapidly. “Within just a few hours, Dig gave us visibility into our data,” Yeshua says. “So much so, that during the first 24 hours, the solution had already helped identify and alert us of two critical risks – sensitive public assets contained within private buckets – that our CSPM had missed.

> During the first 24 hours of deployment, Dig had already helped identify and alert us of two critical risks – sensitive public assets contained within private buckets – that our CSPM had missed."

Great UI, great team

"Dig's solution was more mature than the others," Yeshua continues. "Its UI was by far the best, making it easier to carry out searches. And the entire team, from top to bottom, including the CTO – who clearly understood our needs as well as cloud environments – was a cut above the rest."

And if that wasn't enough, Dig is a top design partner, according to Yeshua. "Dig is a mature company when it comes to understanding security. As a result, it's open to testing and integrating new features that we're using such as Torq, Snowflake, customized risks, and OCR."

While Dig's solution has been implemented only for a short time, it is already making a significant impact across Riskified's organization. "The solution gives our DevSecOps team the platform security and visibility we need to protect our data," Yeshua says. "It also provides information to our GRC team to better handle compliance risks. And it enables our FinOps team to reduce data scanning costs and to optimize data storage by identifying stale buckets and shadow data.

"We've benefited from Dig since our very first encounter with the company," Yeshua concludes. "We remove data from places where it shouldn't be found, and we have all but eliminated the risk of ongoing data breaches through Dig's data classification and discovery capabilities."

About Dig Security

Dig Security helps organizations discover, classify, protect, and govern their cloud data.
With organizations shifting to complex environments with dozens of database types across clouds, monitoring and detecting data exfiltration and policy violations has become a complex problem with limited fragmented solutions. Dig's cloud-native, completely agentless approach reinvents cloud DLP with data detection and response (DDR) capabilities to help organizations better cope with the cloud's data sprawl. Dig is founded by 3 cyber security veterans from Microsoft and Google, and is backed by Team8, CrowdStrike, CyberArk, SignalFire, Okta Ventures, and others

Dig Security