Dig for Financial Services

Tipalti Leverages Dig to Discover and Protect its Cloud Data

1 day onboarding

2 days full discovery

50% faster data threat detection time

Transforming and Accelerating the Accounts Payable Process

As the world's leading automated global payables solution, Tipalti handles both global partner payments and accounts payable workflows for high-velocity companies across the entire financial operations cycle. Helping companies scale quickly by making payables strategic with operational, compliance, and financial controls, Tipalti significantly reduces workload and accelerates financial close for over 2,500 customers.

With a near-100% customer satisfaction and customer retention rate, Tipalti stores and handles all of its data on a fully cloud-enabled platform. Despite having implemented CSPM across its AWS and Azure cloud environments over the years, the company required a solution that protects its sensitive customer data.

"Our fundamental security goal is data protection, which is foundational to the payments technology we're building," Tomer Kremer, CISO of Tipalti, says. "It's challenging to build a data protection program without a deep understanding of the data we own, how it's moving within the organization, and how it's consumed. That's why it was clear to me that we needed a DSPM solution for better visibility and mapping of our cloud data. Otherwise, we could miss something that would eventually damage us and our clients."

> **We needed a DSPM solution for better visibility and mapping of our cloud data. Otherwise, we could miss something that would eventually damage us and our clients."**

Acquiring a DSPM solution wasn't the only thing clear to Kremer. So was his decision to turn to Dig Security. "I knew [Dig CEO] Dan [Benjamin] from Dig's early days," Kremer says. "We discussed the company's security concept, and I shared with him my needs as a CISO. I even had the chance to be a design partner in developing some of Dig's solution requirements. So, when I arrived at Tipalti, I knew what Dig had to offer. Even though I evaluated another DSPM vendor, Dig's solution fit the bill."

And it was smooth sailing once Tipalti gave Dig the green light. "Initially we onboarded Dig to our cloud, where a large quantity of PII and other customer data that our clients handle is stored," Kremer says. "The process was quick and complied with several regulations to which the data is subject, including GDPR in Europe as well as state-level CCPA and NYDFS policies in the US."

Once Dig was on board, Tipalti utilized Dig for discovery purposes. "We received immediate value at the discovery stage," Kremer says. "Without Dig, it would have taken a couple of months of back and forth with a full-time employee to partially figure out what data we have and where it's located. With Dig, it took us only two days to gain full data visibility."

> **"Without Dig, it would have taken a couple of months of back and forth with a full-time employee to carry out partial data discovery. With Dig, it took us only two days to gain full data visibility."**

Responding Before It's Too Late

Dig's solution prioritizes Tipalti's data risks based on the importance of the data. It then delivers notifications via Slack and SIEM so that the DevOps team can take actions to remediate the risks. The solution also notifies Tipalti's DPO when data resides where it should not be located.

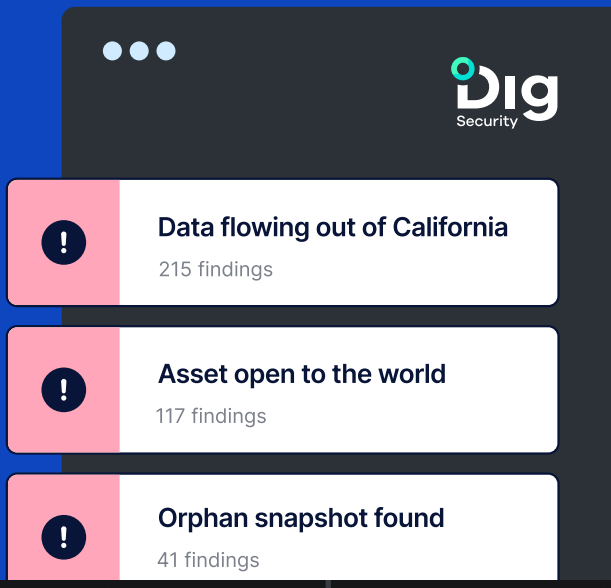
But above all, Dig sends alerts to Tipalti's SecOps team so it can respond in real time to events. "The solution drastically cuts our mean time to detect (MTTD), and as a result, our mean time to respond (MTTR)," Kremer says. "By knowing what data we have and where it's exposed, as well as receiving accurate alerts – we haven't had any false positives – we can respond before it's too late. That gives us real value." Even in the ever-changing cloud world.

"The public cloud represents a fast-evolving threat landscape, and Dig has helped us keep pace," Kremer says. "It's the most mature data security platform we've found for our cloud data stores, and it bridges the gap between the velocity of development and the need for data protection. And, of course, it offers visibility into all of our cloud data assets in real time so we can easily control them."

Tipalti's work with the Dig team to prioritize new capabilities and features has been "easy and effective," according to Kremer. Such satisfaction bodes well for the future relationship between the two companies.

"We plan on expanding coverage of the Dig solution so that it connects to our local SQLs and our DBaaS, Snowflake, to provide us with a comprehensive solution across our entire cloud environment."

> **By knowing what data we have and where it's exposed, as well as receiving accurate alerts, we can respond before it's too late, which gives us real value."**



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