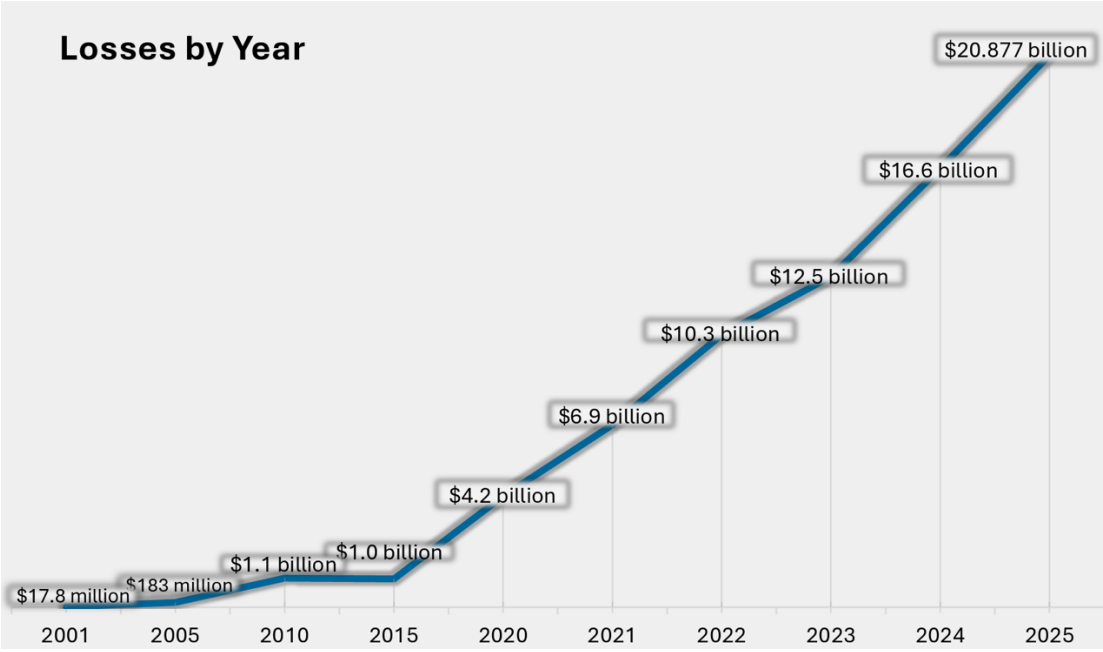
Why Mouro Capital Invested in Overwatch Data

At Mouro Capital, we've been hearing a common theme across businesses in financial services: AI doesn't just help the good guys. It helps the bad guys too, and in the closing stages of 2026, it's helping them faster. That growing imbalance is what drew us to Overwatch Data. The gap between the complexity of modern threats and the capacity of existing security teams represents a defining market opportunity, and we are proud to lead Overwatch Data's $15 million Series A alongside strategic participation from Visa Ventures and Capital One Ventures.

Overwatch Data is an AI-native, agentic risk-intelligence platform for fraud, cyber, and merchant-risk teams. Its agents plan, collect, process, analyze, and disseminate threat intelligence, turning what used to be a manual, alert-heavy grind into decision-ready action.

How Has AI Changed the Balance Between Attackers and Defenders?

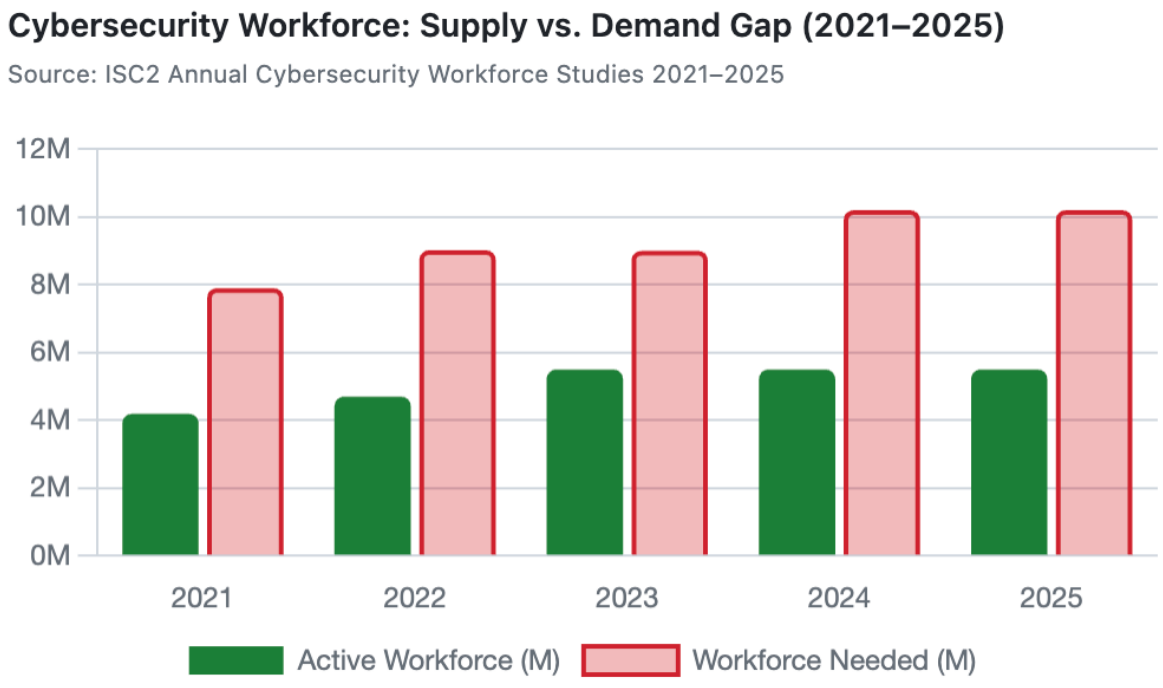
AI has given attackers a speed advantage over human defenders. Threat intelligence has always been an arms race, but human analysts and human attackers were once roughly matched in speed. AI has ended that. IBM X-Force's research found generative AI has cut the time to craft a convincing phishing email from roughly 16 hours down to about 5 minutes, putting attackers at close to 200x their prior productivity. Separate industry tracking found AI-generated phishing surged nearly 14-fold in a single month at the end of 2025. In other words, attackers now operate at machine speed.



Source: Federal Bureau of Investigation Internet Crime Report 2025. Jose A. Perez.

The line of defense is moving in the wrong direction at the worst possible time, and the reason is more specific than a simple staffing gap. The SANS Cybersecurity Workforce Report, published in March 2026, found that AI is "automating the entry-level work that has historically trained cybersecurity's next generation", meaning the same triage and investigation tasks junior analysts used to cut their teeth on are exactly the tasks AI tools now handle first. As a result, automation is removing the on-ramp junior analysts need to grow into senior roles.

Compounding that, the hiring budget that would once have gone toward developing junior talent is being redirected elsewhere. As compliance requirements from frameworks like the EU's NIS2 Directive and Digital Operational Resilience Act (DORA), and the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC), intensify, organizations are rebuilding their teams from the top down, hiring experienced specialists to meet immediate regulatory and capability demands rather than investing in the junior pipeline. In practice, AI is replacing entry-level work at the same time as the budget that used to train the next generation of analysts moves to senior hires. Fewer junior analysts training today means fewer experienced ones by the early 2030s, right as the threats they'd need to handle keep getting harder.



Source: Cybersecurity Statistics 2026: Breaches, Costs, Ransomware & Workforce Data. Axis Intelligence Research.

Put those two trends next to each other and the conclusion is hard to avoid: the only way to defend at machine-speed is with machine-speed infrastructure. That's the bet Overwatch is making.

How Is Overwatch Data Different From Other Threat-Intelligence Tools?

Overwatch Data's agents identify threats across its network and surface them to its customers, while most threat-intelligence tools are static, just surfacing alerts and leaving the thinking to humans. The platform's architecture is the reason we believe this business gets structurally harder to compete with over time. As more threats are detected through Overwatch (flagging a high-risk merchant, a fraud pattern, a suspicious transaction) the agents become sharper for every customer on the platform. Better detections attract more customers. More customers equals more bad actors mitigated.

That architectural advantage is what can carry Overwatch from a threat-intelligence point solution into the broader core risk infrastructure of any enterprise. This is the kind of position that gets more defensible as the company scales.

Numerous enterprises are adopting Overwatch to improve the efficiency and effectiveness of their security operations. Overwatch Data reports that customers using the platform are seeing 6x more critical threats actioned, detection three days faster, and 20+ analyst hours saved weekly, the kind of outcome that turns a security purchase into an obvious productivity investment. The value is therefore measured in both risk reduction and in the ability to scale security operations without proportional increases in headcount.

Who Are Overwatch Data's Founders?

Overwatch Data's founders, Arjun Bisen (CEO) and Zara Perumal (CTO), bring more than 25 years of combined experience in risk, AI and cybersecurity. Arjun spent 15 years in global risk across Stripe, Google, and Twitter (including leading Stripe's fraud, risk, and onboarding risk team), and began his career in the Australian Foreign Service, where he helped write the country's National Cyber Strategy. Zara has spent over a decade at the intersection of AI and cybersecurity, working on early agent systems at Google Assistant and later serving as tech lead for Google's Threat Analysis Group on influence operations.

Between them, they've sat on the defender's side of exactly the problem they're now building agents to solve. In late 2025, they brought on Jeff Needham as CRO, previously CRO of Flashpoint and Intel 471, two of the category's incumbents. The team is also composed of an engineering and sales organization built with the same care: a team that understands this problem space as deeply as the founders do, not one assembled generically and pointed at a hot category.



Source: Overwatch Data

Why Did Mouro Capital Invest In Overwatch Data?

Overwatch Data sits squarely in Mouro Capital's thesis of backing founders reshaping financial services through AI, data, and infrastructure, with a particular focus on automating the operational backbone of financial institutions. The timing is just as important in that AI-driven threat volume is already overwhelming fraud, third-party risk, and onboarding teams across the institutions we work with, and that pressure is only building.

Overwatch Data also complements Mouro's existing portfolio, building on investments in data privacy, safe model deployment, and bank-facing platform infrastructure through Skyflow, Alinia, and Hyperlayer. By extending this stack into risk-intelligence execution, Overwatch further strengthens the strategic value of our existing portfolio. We see real relevance across our broader portfolio in payments, identity, lending, capital markets, and enterprise AI, where merchant diligence, fraud triage, brand protection, and third-party risk reviews are common operational bottlenecks. That overlap creates room for genuine cross-portfolio learning as Overwatch's agents take on more of that workload.

"The Mouro team recognized early on that AI-driven threats require fundamentally new risk infrastructure, align with our long-term vision, and bring a deep financial services network and strategic partnership that goes far beyond capital to help us scale." - Arjun Bisen, CEO Overwatch Data

We're proud to lead this round and partner with Arjun, Zara, and the entire Overwatch Data team as they build the infrastructure enterprise risk teams need for an AI-scaled threat landscape. Overwatch has the opportunity to become a key part of how enterprises protect themselves in the future, and we are excited to support the team as they create a new standard for security operations.