transmit security

DATASHEET

# The Attack Architecture Your Controls Can't See

Autonomous offensive AI is coming. The window to prepare is now.

The breakthrough in new AI models like Mythos isn't the model, it's the architecture: a frontier model wrapped in a pipeline of goal-optimized agents that mirrors how a well funded, well organized nation-state offensive cyber unit might operate: reconnaissance, target analysis, exploit engineering, attack chaining, and iteration until successful. What once took an intelligence agency 20 to 50 specialists and two years now takes zero people and runs overnight.

The security industry is hyper-fixated on the headline use case: vulnerability discovery. This is the least of your concerns. When these new models are pointed at a business instead of a codebase, they can learn your applications, customers, processes, and controls, then work autonomously and persistently toward the goal they are given. With open-source models expected to reach these capabilities within months, and without the guardrails and governance or oversight of frontier labs - this power lands with every fraud ring that can write a prompt. Capabilities that were once nation-state-grade will become commodity tooling.

## The risk your current stack was never designed for:

- **The authenticated session is no longer proof of the customer.** Session hijacking has always been the Holy Grail for fraud: real device, real credentials, trusted signals. It stayed rare because it demanded elite skills to compromise. That barrier is collapsing.
- **Your fraud models can be reverse-engineered.** These new AI models can predict the majority of a rule-based fraud stack from public information alone, then refine to near-complete accuracy by testing your applications across thousands of distributed accounts feeding one centralized brain.
- **The attack itself will match no known pattern.** These architectures work in three stages: build a puzzle of your business through tens of thousands of individually innocuous probes, run simulations offline where you have zero visibility, then launch attacks that are fast, novel, and invisible to pattern-based

### The defense window is open. For now.

Everything after the initial reconnaissance is too late. Once the puzzle of your business is complete, the simulation and the attack happen where you can't see them and faster than you can respond. The only stage you can contest is the first one: deny these systems the puzzle pieces and neutralize the entire architecture. **No map. No simulation. No attack.**

detection. Every control you run today, cyber or fraud, looks for what's been seen before. This is engineered to find what hasn't.

## How do you get ahead?

This requires getting ahead of a problem the industry hasn't, yet: telling agentic traffic apart from human traffic. Agents are not bots. They adapt, they mimic human behaviour, and they route around challenges in a manner that bot detection and automated defenses will miss.

The Transmit Security approach is one of deep, ongoing research into every agentic platform itself, surfacing the tells each one carries no matter how it behaves. This yields three critical layers in defending against autonomous offensive attacks:

- **Visibility:** See which traffic is agentic, which platform it comes from, which accounts and sessions it touches, and what it's trying to do.
- **Control:** Govern agents and traffic through policy that evolves with your risk appetite, and;
- **Protect:** Block malicious agents and harmful activity, including from legitimate agents that are pushing boundaries and operating in the gray areas where rules don't exist yet.

Your customers' agents are already arriving: shopping, comparing, transacting on their owner's behalf. Treat every agent as a bot and you block revenue and exclude yourself from agent-driven commerce. Have no policy and you absorb the risk blind. The solution is friction-free passage for good agents and a closed door for the rest. You need visibility and control for both.

## Why Transmit Security

Transmit Security is uniquely architected for this challenge. The company was founded by reverse engineers with decades of experience building fraud and identity defenses that protect the world's largest institutions.

Our research teams reverse-engineer each agentic platform itself, frontier and open-source, building intimate knowledge of how each one operates. This is dedicated ongoing research, not a rules update. As new platforms and versions emerge, we take each one part and build the tooling necessary to keep the future of commerce secure. This infrastructure is proven: Transmit is ranked a Leader by Gartner, Forrester, and KuppingerCole.

***Contact your Transmit Security account team today for a no-obligation executive briefing with CEO Mickey Boodaei. This is not a sales pitch, it's a 45-minute assessment of your organization's security readiness for a future that isn't coming, it's here now.***