

Eclipses MTE[®] vs. Malicious Bots

THESIS

Detection is an arms race, elimination wins. Eclipses MTE enforces Zero Trust cryptographically by requiring a per-request, one-time MicroToken minted after a post-quantum handshake. Bots cannot mint, so they never touch your apps, GPUs, or data.

THE PROBLEM

- Nearly 50% of internet traffic is automated; more than 30% is malicious.
- Enterprises lose over \$100B annually through fraud, scraping, wasted cloud resources, downtime, and fines.
- Legacy defenses (WAFs, bot managers) depend on heuristics, device fingerprints, and behavioral scoring—costly, bypassable, and error-prone.

THE MTE APPROACH

MicroToken Exchange (MTE) inserts a cryptographic gate at the data layer. Each API, WebSocket, chatbot, or mobile request must carry a single-use MicroToken created after a quantum-safe handshake. Tokens expire instantly and cannot be replayed. Invalid traffic is dropped before it reaches the application, ensuring only cryptographically valid sessions consume compute resources.

WHERE IT WORKS

- APIs and Web/Mobile Apps
- WebSockets and Chatbots/LLMs
- IoT and Connected Vehicles
- Server-to-Server and Multi-Cloud Traffic

ROI & EFFICIENCY

- 60–80% reduction in bot-driven cloud waste
- Elimination of fraud and scraping before app tier
- Reduced need for legacy VPN/DPI appliances and bot tools
- **Example:** \$17M annual bot impact reduced to ~\$2.8M residual with MTE → ~\$14M net savings → 5,000% ROI, payback in weeks

COMPETITIVE EDGE

- **MTE:** Deterministic cryptographic elimination, zero false positives, utility pricing, broad coverage across APIs, AI, WebSockets, and IoT.
- **Legacy Vendors (Cloudflare, Akamai, HUMAN, Arkose):** Detection-based, bypassable, traffic still hits infrastructure, false positives remain, costs scale with traffic.

CONTROL-PLANE ADVANTAGE

Today, IAM and Zero Trust orchestrators define policy but rely on weak enforcement. MTE becomes the enforcement plane: policies are applied deterministically through MicroTokens at the data layer, across any cloud. Result: Zero Trust that is actually enforced.

EXECUTIVE TAKEAWAYS

- Eliminate—don't just detect—automated abuse and cloud waste.
- Predictable utility pricing (~\$25/container/year), aligned with cloud economics.
- Strong compliance alignment with provable per-request validation and no replayable secrets.
- Stickiness once embedded across enterprise workloads.