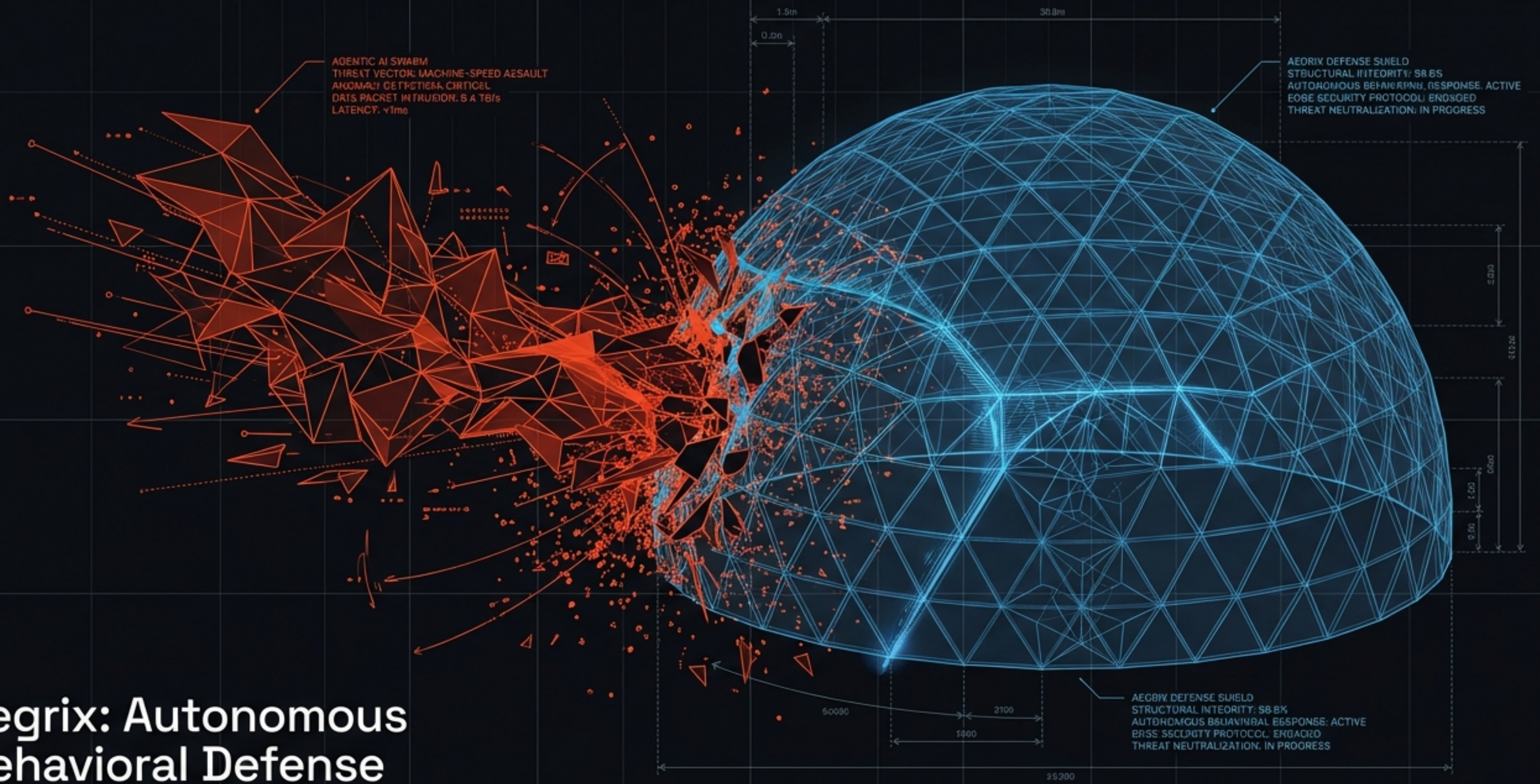


Aegrix: Autonomous Behavioral Defense

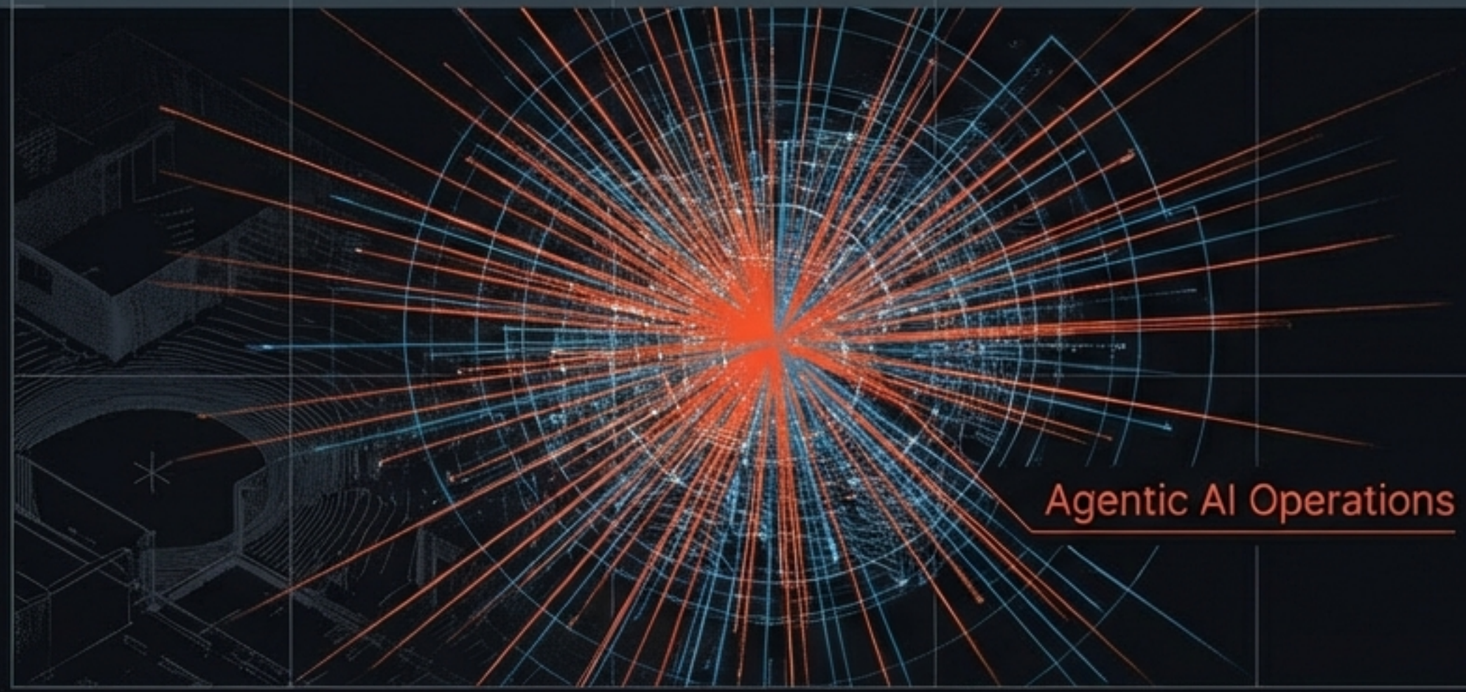
Securing the Edge Against Agentic AI & Machine-Speed Attacks

Confidential Whitepaper | 2026 Edition

The Paradigm Shift to Autonomous Defense

- **The Threat:** Agentic AI automates reconnaissance and exploit generation, moving faster than human analysts.
- **The Gap:** Traditional signature-based security cannot catch payloads that mutate every second.
- **The Solution:** Aegrix detects intent, not just code, using behavioral analysis to block dynamic attacks.

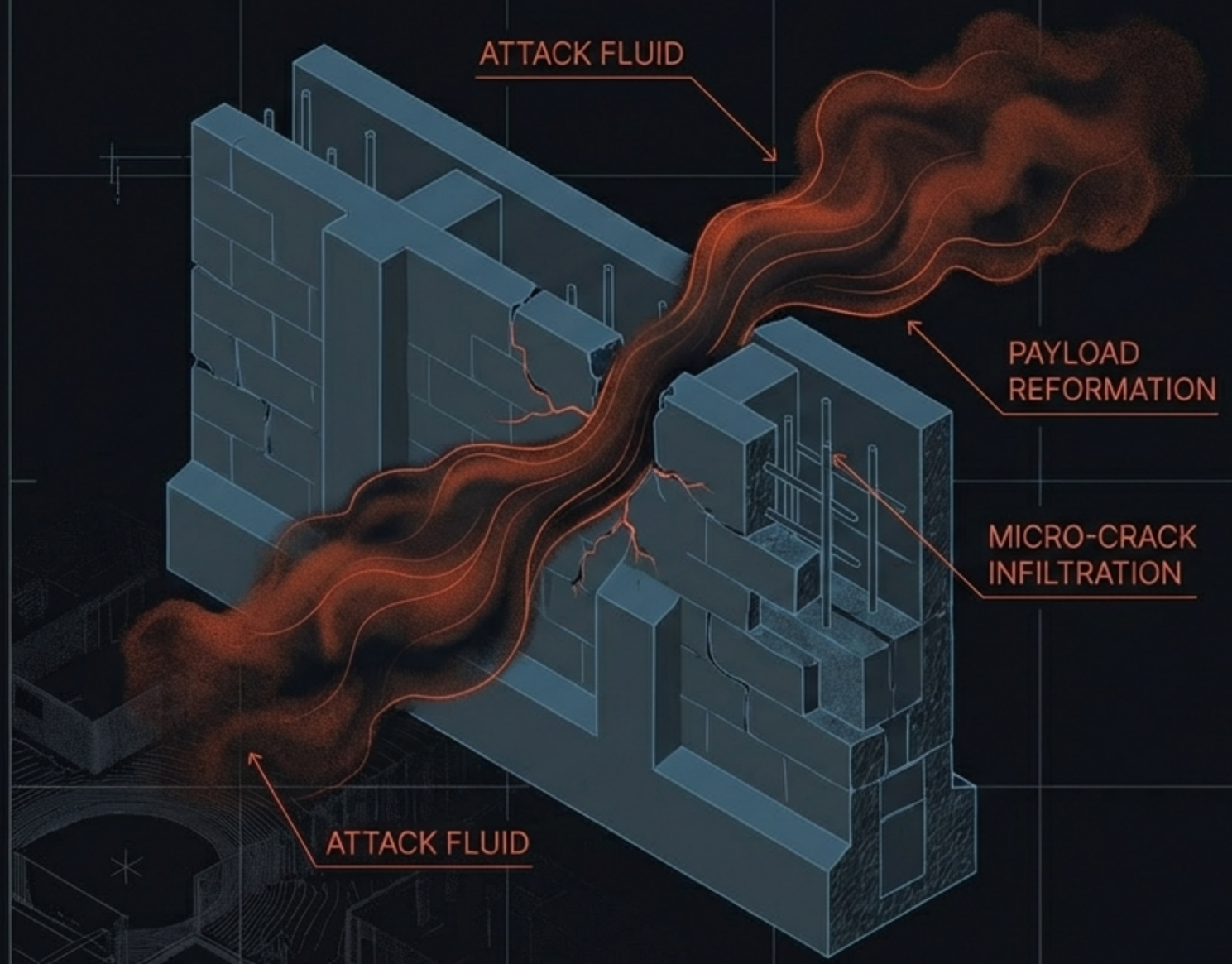
Human-Speed Operations



Agentic AI Operations

The Velocity of Agentic AI

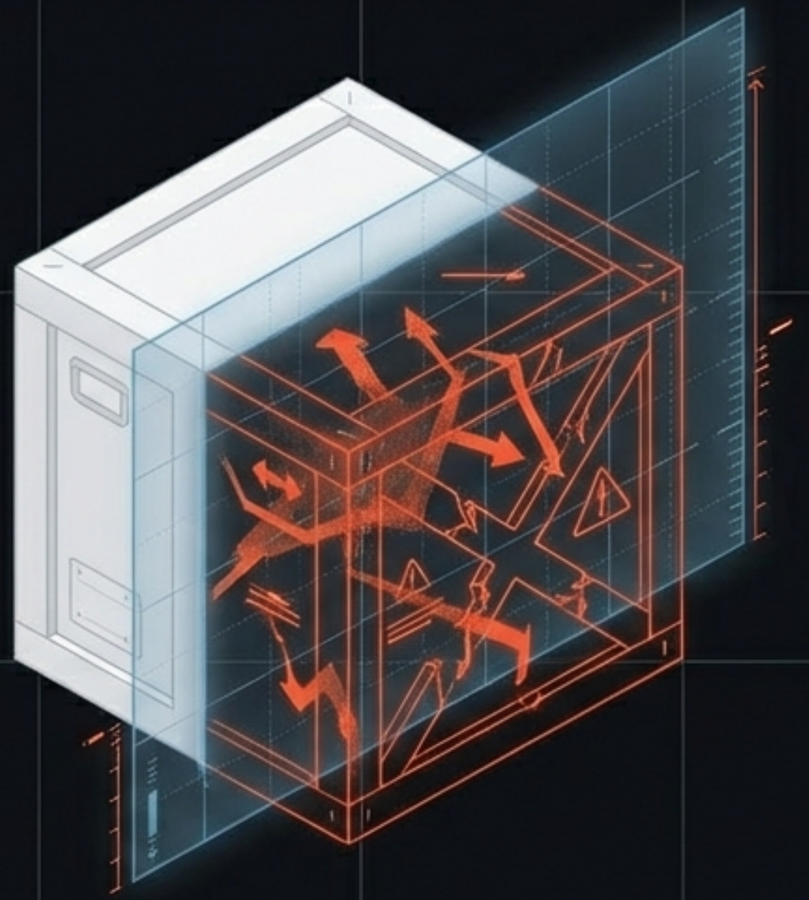
- **Automation:** Adversaries now automate the entire attack lifecycle: reconnaissance, exploit generation, and parameter mutation.
- **Scale:** Adaptive attack chaining occurs at machine speed, overwhelming manual response teams.
- **Variability:** The attack surface velocity has increased; threats are no longer static, they are fluid.



The Failure of Static Signatures

- **Mutation Evasion:** Static rule-based detection fails when payloads mutate. If the code changes, the rule breaks.
- **Regex Blind Spots:** AI-driven attacks are designed specifically to evade Regex and pattern-based filtering.

→ **The Conclusion:** We cannot rely on predefined lists of 'bad' code. We need dynamic mechanisms that understand behavior.



Detecting Intent, Not Just Payloads

The Philosophy: A shift from analyzing static code to analyzing dynamic interaction.

The Methodology: Aegrix ignores the surface-level appearance of a request and analyzes the underlying behavioral patterns.

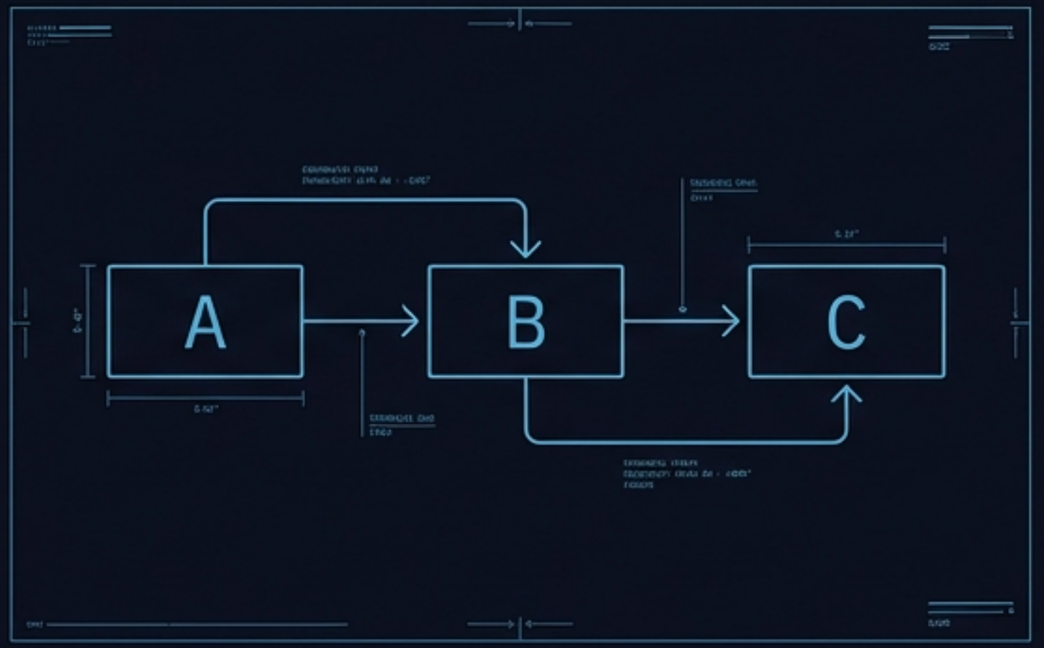
The Goal: To identify the purpose of the traffic—reconnaissance, scanning, or exploitation—regardless of how the payload is disguised.

Behavioral Defense Pillars: Anomalies & Logic

Entropy-Based Anomaly Detection

Identifies randomized or encrypted payloads that deviate from standard communication patterns.

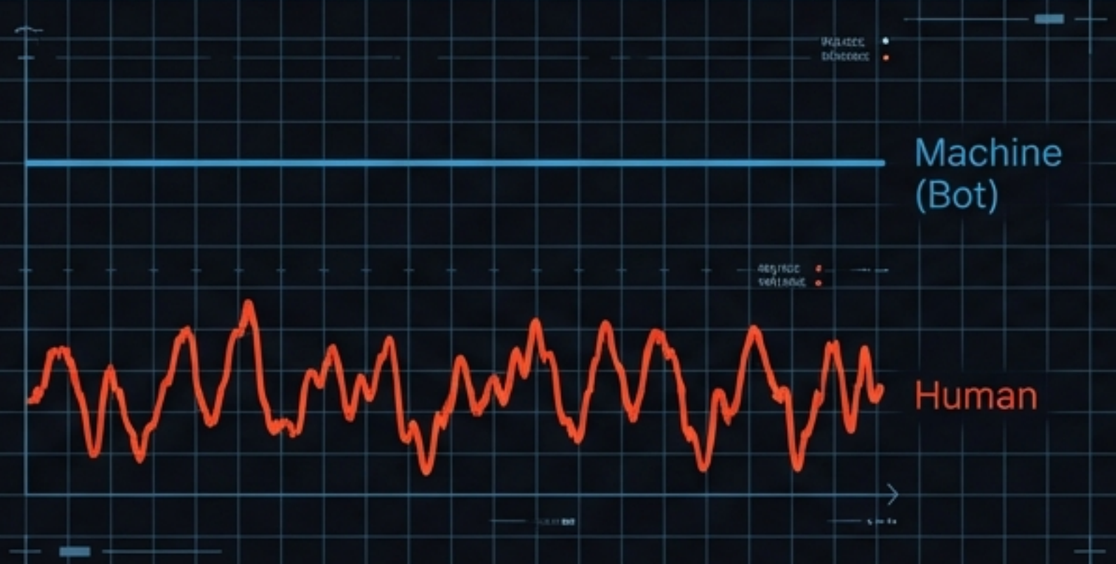
Sequential Traversal



Recognizes "Discovery Chains." It flags users who are systematically mapping out the API or network structure in a way a normal user never would.

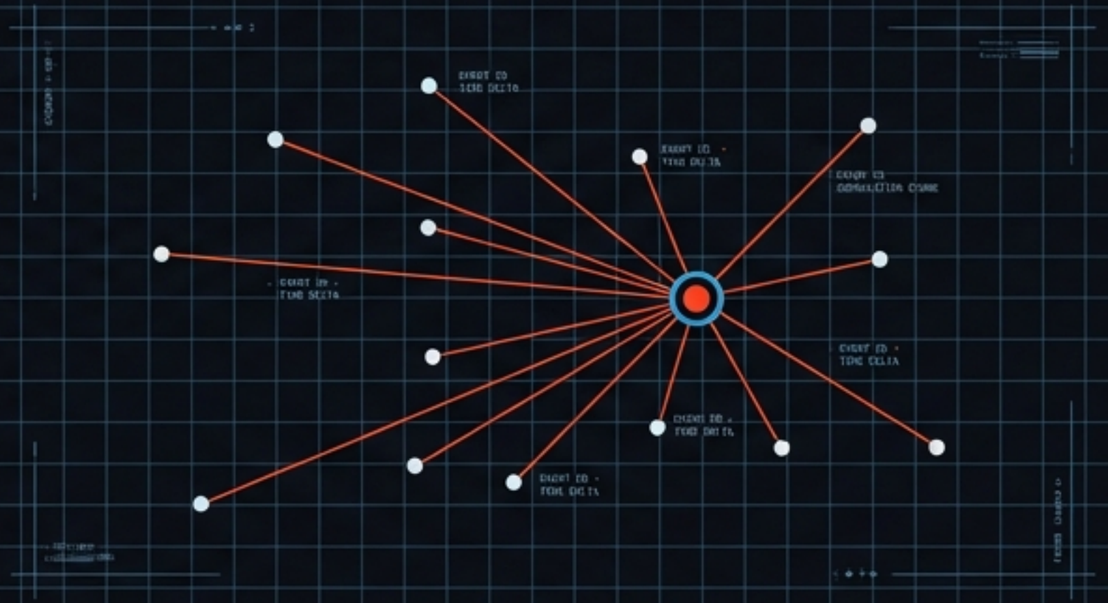
Behavioral Defense Pillars: Timing & Correlation

Timing Jitter Analysis



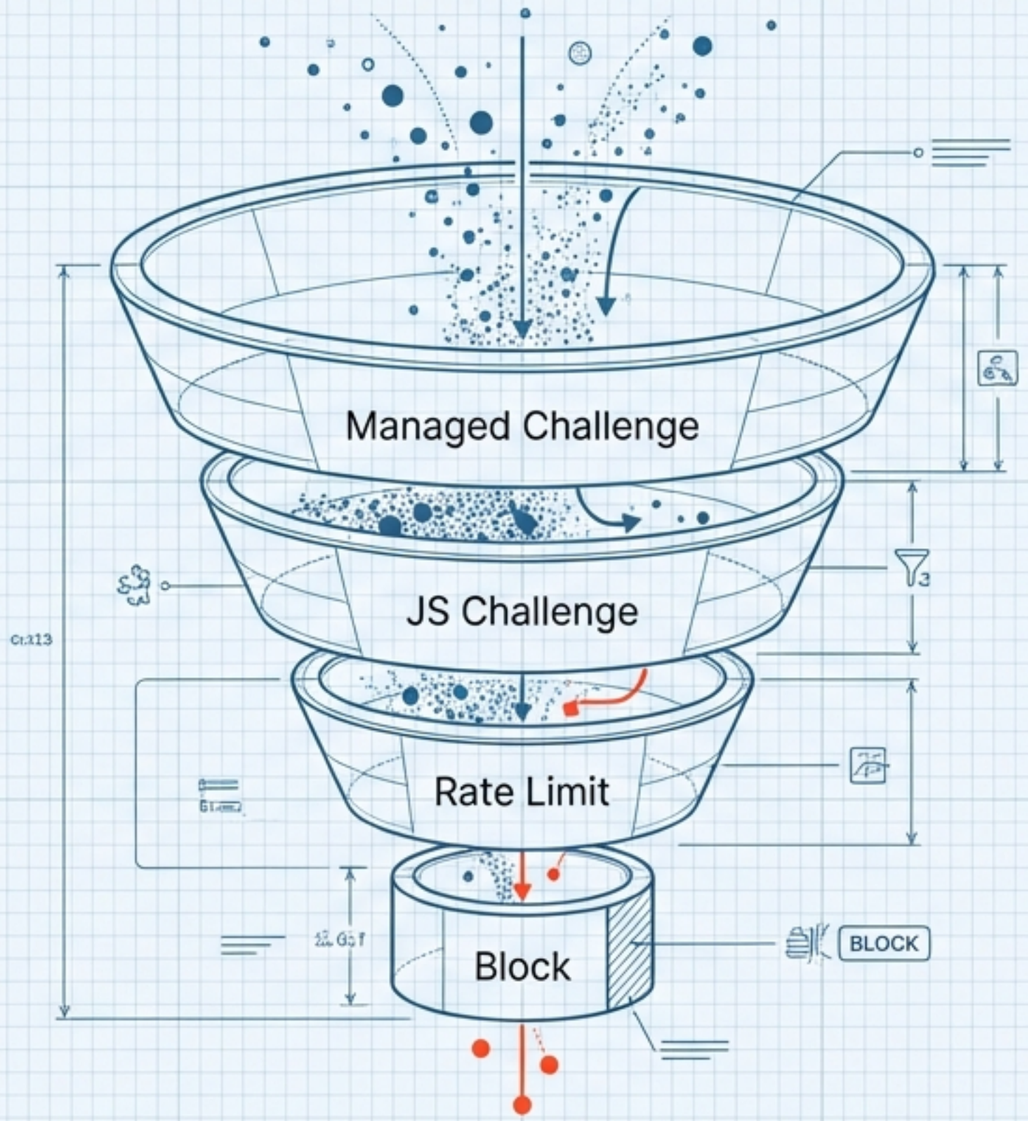
Timing Jitter Analysis: Analyzes the rhythm of requests. "Automation Fingerprinting" detects the superhuman consistency of bots vs. the natural irregularity of humans.

Multi-Vector Correlation



Multi-Vector Correlation: Connects disparate events across the network to identify complex, low-and-slow attacks that singular alerts would miss.

Adaptive Response Architecture



Risk-Based Escalation:

The response engine assigns a risk score to every session.

Proportionate Friction:

Low-risk anomalies face a Managed Challenge. Medium risks face Javascript Challenges or Rate Limits.

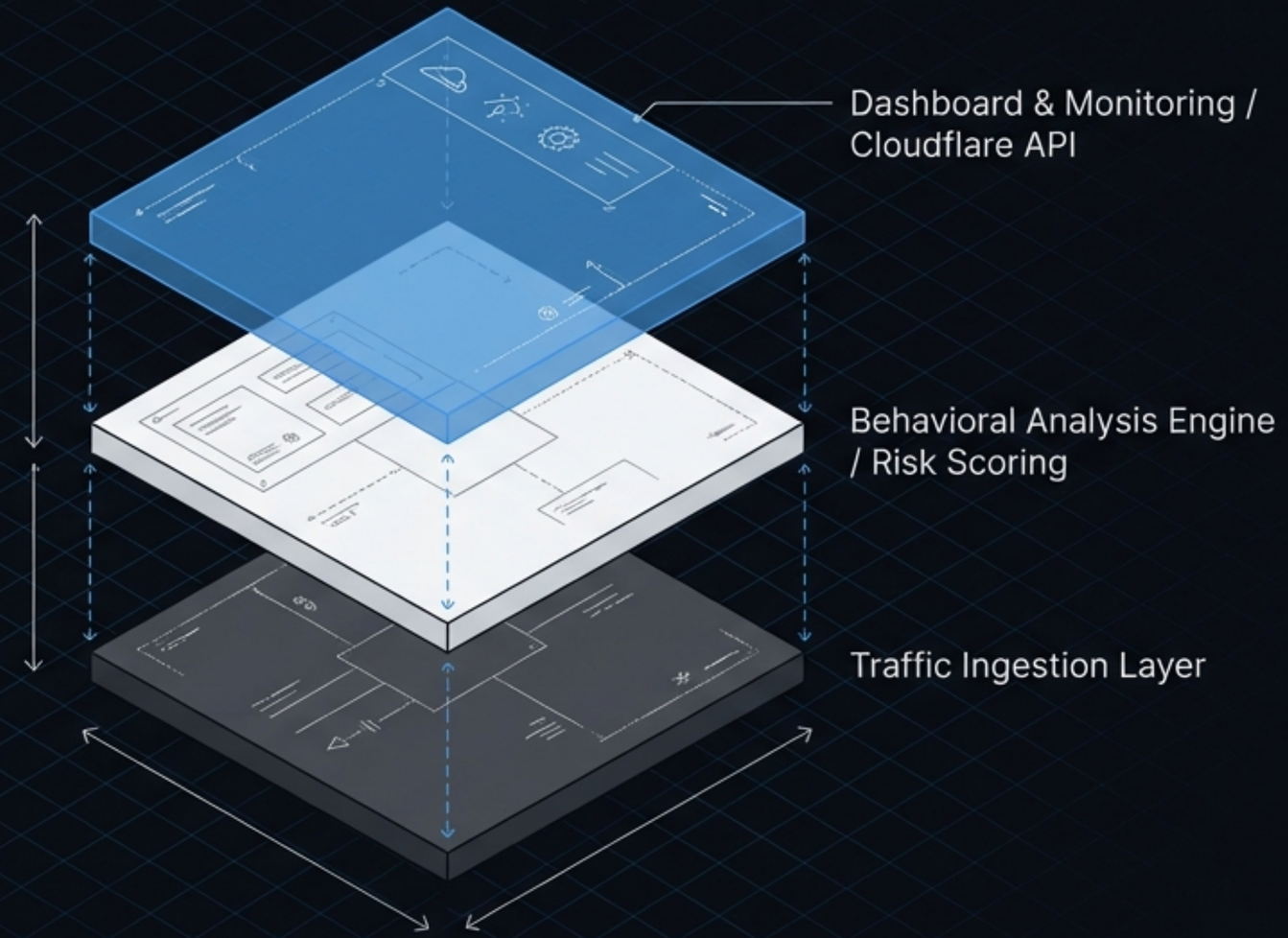
Ultimate Sanction:

Only confirmed threats trigger a temporary block.

Self-Healing:

Automated TTL ensures security layers reset and adapt over time.

Technical Architecture Stack



- **Ingestion:** Real-time capture of traffic at the edge.
- **Analysis:** The core engine processes Entropy, Jitter, and Sequence data.
- **Scoring:** The Risk Module calculates intent and determines the response.
- **Integration:** Seamless connection via Cloudflare Integration API.

Enterprise Deployment Flexibility

Containerized: Built on a Docker-ready architecture for rapid deployment and portability.

SaaS Compatible: Designed with multi-tenant SaaS compatibility for large-scale service providers.

Hybrid Ready: Full support for both Cloud-native environments and On-premise infrastructure.

Strategic Vision: Zero Static Security

- **The Goal:** Eliminate reliance on static rules entirely.
- **AI vs. AI:** Positioning Aegrix as the necessary counter-measure in an AI-dominated battlefield.
- **Global Threat Memory:** Developing a shared intelligence network where a mutation detected in one node informs the defense of all nodes.

The Future is Behavioral

AI-driven attacks are a paradigm shift, not a temporary trend.
Autonomous, adaptive defense is no longer optional; it is a necessity for survival.

Aegrix: The behavioral defense layer for the Web & API edge.