STORMBIRD

AI SOLUTION

BEHAVIORAL ANALYSIS

By tracking path patterns (such as navigation sequences) and client-side events (like mouse movements, clicks, scrolls, and timing), Stormbird builds a behavioral profile for each session.

Our AI continuously learns from these patterns, identifying deviations that indicate automation, scripted bots, or suspicious user behavior.

HONEYPOT

A honeypot-based approach to bot detection involves injecting fake yet realistic telemetry values that act as hidden integrity checks—any unexpected changes signal potential tampering.

To enhance this, AI is used to detect anomalies in telemetry data by first collecting both real and fake inputs, along with session details and timestamps

ANOMALY DETECTION

Anomaly Detection uses AI to analyze network traffic and identify unusual patterns—such as sudden spikes, abnormal connections, or high message rates—that signal potential bot activity. This real-time detection enables fast, intelligent threat response.

ASO AND IP RATING

This function establishes an AI-enhanced rating system to assess and track malicious ASOs and IPs.

AI models continuously analyze behavior patterns and historical data to refine these scores, enabling smarter identification of high-risk sources. Over time, this approach strengthens DDoS resilience and core service protection by anticipating threats and adapting defenses in real time.