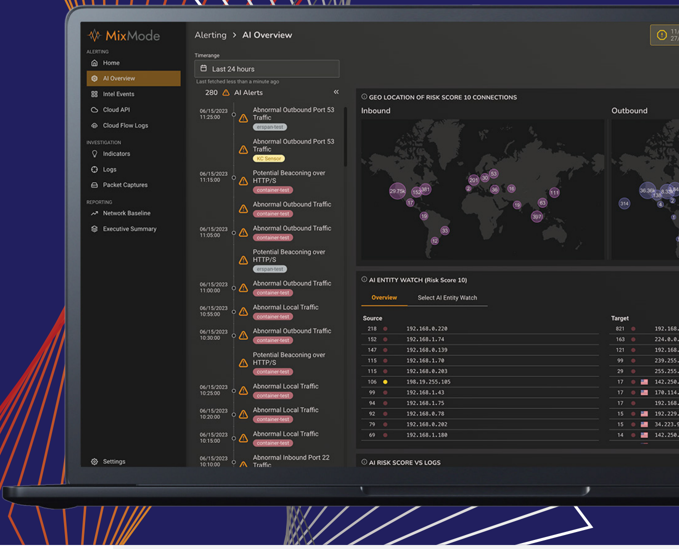
MixMode®

The MixMode Platform

Advanced Threat Detection Analytics Powered by Third Wave AI



06/15/2023 11:25:00 Abnormal Outbound Port 53 Traffic — erspan-test

Abnormal Outbound Port 53 Traffic — KC Sensor

06/15/2023 11:15:00 Potential Beaconing over HTTP/S — container-test

Abnormal Outbound Traffic — container-test

06/15/2023 11:05:00 Abnormal Outbound Traffic — container-test

Potential Beaconing over HTTP/S — erspan-test

06/15/2023 11:00:00 Abnormal Outbound Traffic — container-test

06/15/2023 10:55:00 Abnormal Local Traffic — container-test

06/15/2023 10:30:00 Abnormal Outbound Traffic — container-test

Potential Beaconing over HTTP/S — container-test

06/15/2023 10:25:00 Abnormal Local Traffic — container-test

06/15/2023 10:20:00 Abnormal Local Traffic — container-test

06/15/2023 10:15:00 Abnormal Local Traffic — container-test

06/15/2023 10:10:00 Abnormal Inbound Port 22 Traffic

Source			Target		
218	●	192.168.0.220	821	●	192.168.
152	●	192.168.1.74	163	●	224.0.0.
147	●	192.168.0.139	121	●	192.168.
115	●	192.168.1.70	99	●	239.255.
115	●	192.168.0.203	29	●	255.255.
106	●	198.19.255.105	17	●	142.250.
99	●	192.168.1.43	17	●	170.114.
94	●	192.168.1.75	17	●	192.168.
92	●	192.168.0.78	15	●	192.229.
79	●	192.168.0.202	15	●	34.223.9
69	●	192.168.1.180	14	●	142.250.

Today's advanced cyber threats overwhelm traditional defenses, demanding constant vigilance and straining resources. Organizations struggle to detect and respond in real-time, highlighting the need for more innovative security solutions.

The MixMode Platform is a patented AI-powered threat detection analytics solution purpose-built to detect known and novel attacks in real-time, at scale.

How it Works

Most cybersecurity solutions utilize First and Second Wave artificial intelligence in various ways. However, these still rely on rules-based systems that can only detect attacks with known signatures and cannot effectively scale to the size of a typical corporate network.

MixMode's Advanced AI is uniquely born out of dynamical systems (a branch of applied mathematics) and self-learns an environment without rules or training data. MixMode's AI constantly adapts itself to the specific dynamics of an individual network rather than using the rigid legacy ML models typically found in other cybersecurity solutions.

MixMode's AI utilizes self-supervised learning to understand a customer's environment to continually forecast what's expected to happen next. If what we see deviates from expected behavior, MixMode will highlight these events for further investigation. This also enables MixMode's AI to alert on the absence of expected events, which other solutions can't do.

The result is an AI-powered threat detection solution that analyzes data in real-time, at scale, to uncover known and novel attacks while empowering security teams to operate more effectively and efficiently.

Key Benefits

Reduce Alert Fatigue: Empower security teams to focus on high-priority threats with fewer notifications.

Improve MTTD: Transform MTTD (mean-time-to-detect) to MTTP (mean-time-to-prevent) with pre-attack indicators.

Decrease MTTR: Reduce MTTR (mean-time-to-respond) with rich context and correlation around threats.

Strengthen Security Posture: Detect in real-time with100% coverage for known and novel attacks.

Analyze at Scale: Ingest and analyze data in real-time, at scale, proven to handle over 1M records per minute.

Minimize Rule Writing: Minimize time spent on writing rules with continuously adapts with individual networks and the threat landscape.

MixMode®

MIXMODE
DATA SHEET

Stop wasting time chasing false positives and start focusing on the threats that matter.

No Rules or Tuning: Requires no initial configuration or ongoing tuning, saving time and resources for security teams.

Behavioral Insights: AI-powered behavioral analytics establish a continuous baseline of normal user and system behavior, enabling the detection of abnormal activities indicative of potential security threats.

Predictive Analytics: Forecast what's expected next to identify potential security threats and vulnerabilities, enabling proactive measures to stay ahead of evolving threats and adapt security measures accordingly.

Unified Network Visibility: Illuminate activities across your entire digital estate—on-prem, cloud, and all devices—through integrated, AI-powered telemetry analysis.

Scalability and Performance: Analyze large volumes of security data and events to effectively scale to meet the needs of organizations of varying sizes.

> *"The MixMode Platform equips our Technology Services' Security Operations Center with a comprehensive solution to rapidly identify and respond to cyber incidents, including ransomware and never-before-seen attacks."*
>
> **Dr. Brian Gardner, Chief Technology & Information Security Officer (CISO), City of Dallas**

Key Use Cases

Novel Attack Detection: Detect and mitigate advanced and evolving cyber threats in real-time, including: AI-generated attacks, Insider Threats, Supply Chain Attacks, Ransomware, and Identity Based Threats.

Threat Prioritization: Automatically prioritize detected security events based on AI confidence, potential impact, and relevance to the organization's specific threat landscape with AI-driven threat risk scoring.

Event Correlation: Connect the dots to understand all of the findings related to a specific event, including those based on multiple events.

Analyst Augmentation: Leverage AI to assist security analysts by speeding up investigations, correlating disparate data sources, and providing actionable insights to support decision-making.

SIEM Optimization: Integrate with existing Security Information and Event Management (SIEM) solutions to enhance their capabilities with AI-driven threat detection.

No rules. No tuning. No maintenance. Any environment.

Cloud Native | On-Prem | Hybrid

MixMode is the leader in delivering AI cybersecurity solutions at scale and is the first to bring a third-wave, context-aware AI approach that automatically learns and adapts to dynamically changing environments. Large enterprises with big data environments, including global entities in financial services, Fortune 1K commercial enterprises, critical infrastructure, and government sectors, trust MixMode to protect their most critical assets. Backed by PSG and Entrada Ventures, the company is headquartered in Santa Barbara, CA.

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai |