MixMode®

The MixMode Platform

Advanced Threat Detection Analytics Powered by Third Wave AI

The MixMode Platform is an AI-native cyber threat detection solution. It is purpose-built to detect novel and known attacks in real-time, at scale – even in disconnected and DDIL environments.

There is an exploding number of novel attacks originating from adversarial nation states. The reality is that legacy, rules-based systems cannot address these new and evolving attacks. MixMode solves this problem efficiently and effectively. That is why MixMode is increasingly being adopted by the US Department of Defense, US Intelligence Community, and Critical Infrastructure (e.g. power, water, transportation).

MixMode's Advanced AI is uniquely born out of the dynamical systems branch of applied mathematics. This proprietary AI contextually learns an environment without rules or historical training data. It continuously creates evolving forecasts of a network rather than relying on legacy ML models or LLMs that are prone to hallucinations. No tuning or retraining is required.

Through self-supervised learning, MixMode forecasts expected behavior and flags deviations that may indicate pre-attack or in-progress activity. It also detects the absence of expected activity - a powerful indicator of sophisticated adversary tactics.

The result is an AI-powered threat detection solution that delivers real-time insights, supports decisive action, and scales to mission-critical-environments - while reducing alert noise and empowering security teams to operate more effectively, often at a lower overall cost.

Key Benefits

Detect Unknown Attacks: Uncover complex novel attacks (Including nation-state attacks) that rule-based systems miss.

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

Cut Through the Noise: Drastically reduce the number of alerts compared to signature-based tools, allowing operators to be much more targeted with their threat hunting and analysis.

Deploy Anywhere: Functional in fully disconnected, air-gapped, and DDIL environments - no internet or cloud dependencies.

No GPU Required: Operates without the need for GPU acceleration, supporting lightweight, efficient deployment on existing hardware and reducing SWaP (Size, Weight, and Power).

MixMode

MIXMODE
DATA SHEET

Key Use Cases

Novel & Known Attack Detection: Detect advanced and evolving cyber threats in real-time, such as: Insider Threats, Ransomware, Zero Day, and Identity-Based Threats.

Insider Threat Detection: Continuously monitor user activity to detect suspicious behavior that may indicate an insider threat. The platform autonomously learns and alerts on changing behaviors instead of white-listing specific users.

Analyst Augmentation: Leverage AI to assist security analysts and speed up investigations, map the attack timeline from early indicators to post-event activity, and provide actionable insights to support decision-making.

Improve SOC Efficiency: Empower SOC teams to focus on the real threats that matter, enabling them to spend time on high-value analysis, not simply combing through alerts. This saves SOC teams hundreds of hours and allows them to be strategic, efficiently and proactively hunting for malicious events in their environments.

Flyaway Kits & Tactical Use: MixMode is successfully deployed in Flyaway Kits, putting the power of AI in the hands of forward-operating military and intelligence units. Our platform requires no GPU infrastructure, integrates easily with portable stacks, and provides real-time situational awareness.

Whether supporting permanent installations or forward deployments, MixMode is built for versatility. The platform operates in connected or disconnected environments, requires no GPUs, and fits seamlessly into existing infrastructure—minimizing footprint and reducing SWaP. This ensures mission success, even at the tactical edge.

Key Results

Reduce Alerts: MixMode produces far fewer alerts than signature-based tools and helps users identify the real threats quickly among the noise of all the alerts from their other tools.

Time-to-Value: Rapidly deploy and detect threats other platforms miss on day one.

AI Built for Modern Defense: Built on proprietary and patented AI that is in use at the DoD and US Intelligence Community.

Real-Time Visibility: Enable immediate situational awareness, allowing operators to detect, assess, and respond—before the damage is done.

Deployment Flexibility & Tactical Readiness

MixMode has been successfully deployed in a wide range of operational environments:

- On-Premise Networks
- Air-Gapped & DDIL Environments
- OT Networks
- Tactical Networks
- Private Cloud & AWS
- Flyaway Kits

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.