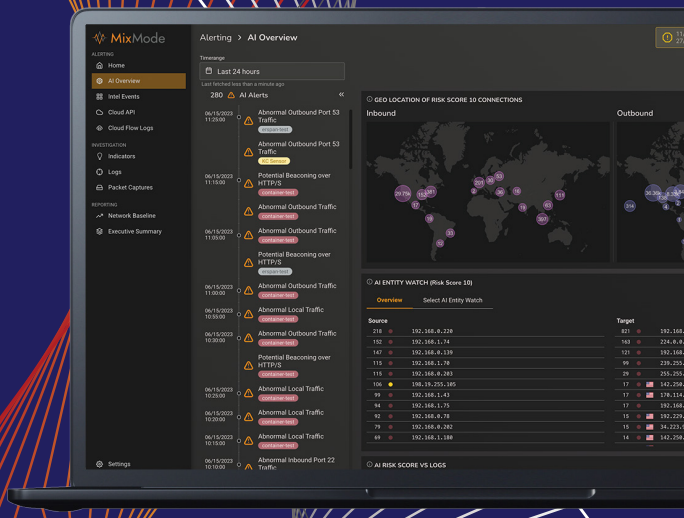
MixMode®

The MixMode Platform

Advanced Threat Detection Analytics Powered by Third Wave AI



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

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 self-learns an environment without rules or historical training data. MixMode's AI constantly adapts itself to the specific dynamics of an individual network rather than using the rigid legacy ML models or LLM/GPTs prone to hallucinations. No tuning or retraining is needed.

MixMode's AI utilizes self-supervised learning to understand a customer's environment to continually forecast what's expected to happen next. When potential harmful activity is seen as deviating 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 could be indications of preattack activity.

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

Key Benefits

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

Detect Unknown Attacks: Detect unknown attacks (including nation-state attacks) within minutes.

Decrease Costs: Reduced costs by tens of millions per year through automation, tool consolidation and storage.

Analyze at Scale: Ingest and analyze data in real-time, at scale, proven to handle over 100 Gbps or billions of records per month.

"MixMode was deployed remotely in under an hour and detected threats on day 1 that other platforms and their human operators had missed. MixMode's AI platform is now the core intelligence layer for our Security Operations Center."

— City of Phoenix

MixMode

MIXMODE
DATA SHEET

Key Use Cases

AI-Generated Attack Detection: MixMode's patented self-learning AI platform masters an environment without predefined rules or training data, customizing to the specific dynamics of individual networks, rather than relying on more generic machine learning models typically found among competitors.

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

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

SOC Automation: The MixMode Platform includes the ability for SOC teams to automate the novel attack detection and prioritization of all attacks. This saves SOC teams hundreds of hours and allows them to be strategic. This includes forensic capabilities – including full packet capture and file extraction that enables security teams to automatically and proactively hunt for malicious events in their environments.

Insider Threat Detection & Response: MixMode's dynamical threat detection platform continuously monitors user activity to detect suspicious behavior that may indicate an insider threat.

"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."

– City of Dallas

Key Results

Proven Cost Savings:
$50M+ in cost savings delivered to U.S. municipalities in the last 3 years.

SOC Efficiency:
93% reduction in alert volume within the first week of deployment.

Time-to-Value:
Deployed in under 1 hour, detecting threats other platforms missed on Day 1.

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

MixMode's AI delivers real-time, pre-emptive threat detection at a fraction of the cost—eliminating expensive GPU dependencies, bypassing historical data requirements, and outperforming LLMs and other ML tools with breakthrough time series prediction capabilities powered by dynamical systems to reduce infrastructure, labor, and licensing costs.

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.