MixMode

ENTERPRISE CYBER ANOMALY DETECTION POWERED BY THIRD-WAVE AI

MixMode is a purpose built cybersecurity anomaly detection platform which combines the functionality of SIEM, NDR, NTA and UEBA to deliver faster and more accurate detections, dramatically increase productivity and efficiency, and decrease wasted time, effort, and resources associated with legacy cyber tools. Enterprise security teams use MixMode in the cloud or on-premises for threat and anomaly detection, zero-day attack identification and false-positive alert reduction across any data stream.

The platform is powered by patented unsupervised AI that is uniquely adaptable to the environment it monitors, can predict what's coming before it happens, and evolve on its own meaning it requires zero written rules to function and removes the need for constant human oversight of the AI.

Forbes Gartner IDC

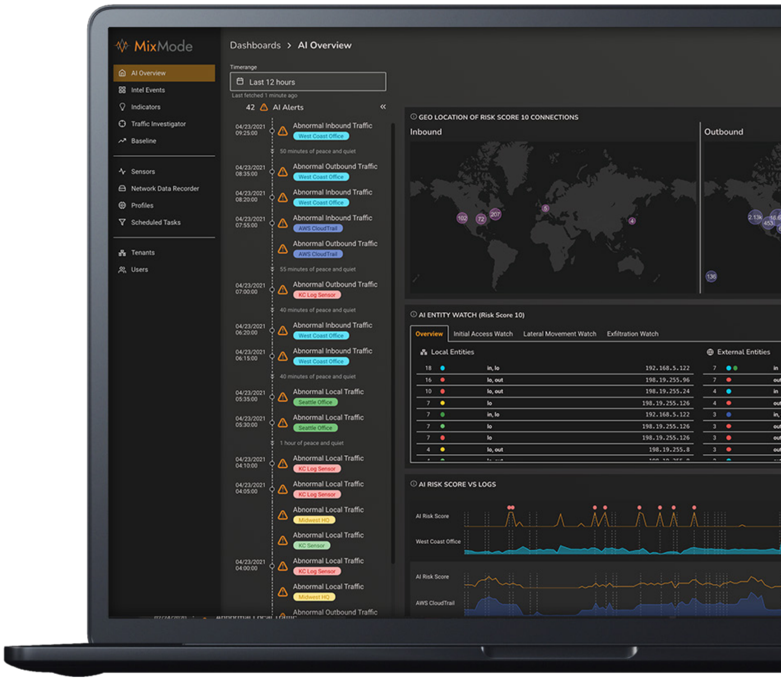
> *"MixMode can detect zero-day attacks through sophisticated anomaly detection powered by an advanced unsupervised AI. As per our research, so far, MixMode seems to be the only example of a cybersecurity platform with this capability."*
>
> \- Ritu Jyoti, VP of AI Research, IDC

Next-Gen Detections
MixMode detects all known threats, but is the first cybersecurity platform to detect zero day no signature attacks.

No Rules AI
MixMode's AI requires no human rules or training to operate and learns on its own over time.

ROI in Minutes
Users can deploy MixMode in less than an hour and start surfacing anomalies immediately.

95% Better Alerts
MixMode surfaces 95% less security alerts than traditional tools but has shown over 100% greater alert accuracy.



42 AI Alerts

04/23/2021 09:25:00 Abnormal Inbound Traffic — West Coast Office
50 minutes of peace and quiet
04/23/2021 08:35:00 Abnormal Outbound Traffic — West Coast Office
04/23/2021 08:20:00 Abnormal Inbound Traffic — West Coast Office
04/23/2021 07:55:00 Abnormal Inbound Traffic — AWS CloudTrail
Abnormal Outbound Traffic — AWS CloudTrail
55 minutes of peace and quiet
04/23/2021 07:00:00 Abnormal Outbound Traffic — KC Log Sensor
40 minutes of peace and quiet
04/23/2021 06:20:00 Abnormal Inbound Traffic — West Coast Office
04/23/2021 06:15:00 Abnormal Inbound Traffic — West Coast Office
40 minutes of peace and quiet
04/23/2021 05:35:00 Abnormal Local Traffic — Seattle Office
04/23/2021 05:30:00 Abnormal Local Traffic — Seattle Office
1 hour of peace and quiet
04/23/2021 04:10:00 Abnormal Local Traffic — KC Log Sensor
04/23/2021 04:05:00 Abnormal Local Traffic — KC Log Sensor
Abnormal Local Traffic — Midwest HQ
Abnormal Local Traffic — KC Sensor
04/23/2021 04:00:00 Abnormal Local Traffic — KC Log Sensor
Abnormal Local Traffic — Midwest HQ
Abnormal Outbound Traffic

Local Entities

18	●	in, lo	192.168.5.122
16	●	lo, out	198.19.255.96
10	●	lo, out	198.19.255.24
7	●	lo	198.19.255.126
7	●	in, lo	192.168.5.122
7	●	lo	198.19.255.126
7	●	lo	198.19.255.126
4	●	lo, out	198.19.255.8

External Entities

7	● ●	in
7	●	out
4	●	in
4	●	out
3	●	in,
3	●	out
3	●	out
3	●	out

MIXMODE'S SELF-SUPERVISED THIRD-WAVE AI

Patented AI Backed By Over 20 years of Research and Data
The industry is full of Cybersecurity Providers touting their "revolutionary AI," so we understand why security professionals are tired of broken promises. MixMode's patented AI, built by Chief Scientist Dr. Igor Mezic with over 20 years of experience building complex AI for DARPA and the DoD, is a massive step forward, solving some of the biggest problems in Cybersecurity today.

Most security tools leverage first or second wave AI technology that use a combination of rules & thresholds or static "training" data to make decisions about your data and can take between 6-24 months of learning to be effective. MixMode is the first available instance of patented third-wave AI in cybersecurity, and is able to provide actionable alerts about your network in only 7 days.

MIXMODE AI

SELF-ADAPTING

NO HUMAN TRAINING OR TUNING

CONTEXT AWARE

7 DAYS TO VALUE

WHY THE AI IS DIFFERENT AND WHY THAT MATTERS

SUPERVISED	MIXMODE SELF-SUPERVISED
12-24 month training period	7-day training period
Dynamically changing attack signatures	Understands its changing environment based on contextual information
Reliance on constant operator tuning and management	Auto-tuning and self-maintaining
Manipulation by Adversarial AI	Difficult to fool because its behavior adapts to new conditions
Reliant on rules and historical intelligence - not predictive	Predictive: Detection of security events that have never been observed (zero day events)