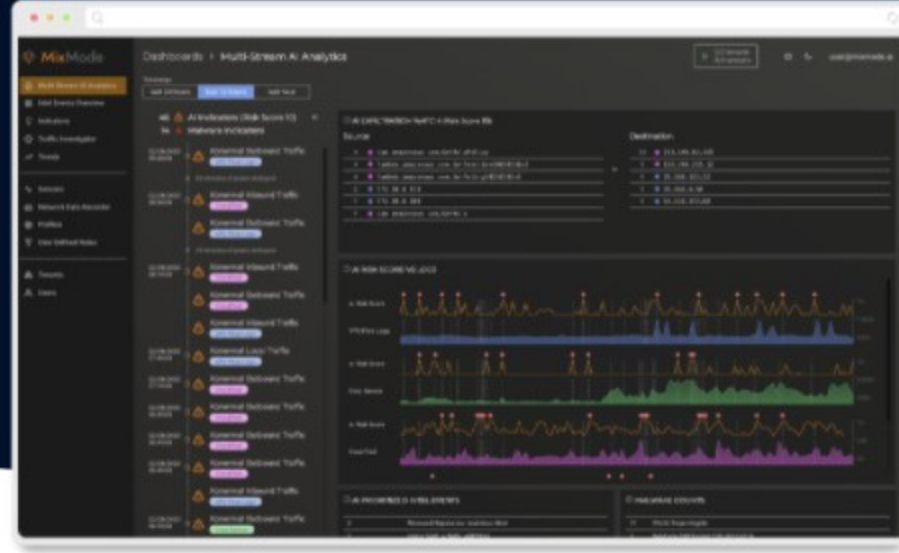




## ANOMALY DETECTION

Predictive and real-time threat and anomaly detection powered by self-learning artificial intelligence with 95% less false positives.

[SCHEDULE A DEMO](#)



## THE NEXT GENERATION OF ANOMALY & THREAT DETECTION

Arm your security operations center with the most powerful AI for threat and anomaly detection across any data stream.



### DATA AGNOSTIC ANOMALY DETECTION

MixMode's advanced threat and anomaly detection operates effectively and independently regardless of data format and type. Identify threats and anomalies in network traffic, log, API, time series, cloud data and more.



### NO RULES OR TUNING NECESSARY

MixMode's Third Wave Unsupervised AI, can learn about your network, create an evolving baseline, and start identifying anomalies in the first hour. A typical AI takes around 18 months to understand the nuances of a network and provide value in the identification of anomalies and alert reduction.



### ZERO-DAY ATTACK DETECTION

MixMode's AI constantly adapts to evolving network conditions using advanced threat and anomaly detection, effectively preventing exploitation and zero-day vulnerabilities before damage is done.

### CUSTOMER STORY: DETECTING AN ATTACK NOT FOUND ON THREAT INTEL

Learn how MixMode was able to prevent an attack on a customer's network using only context-aware AI and anomaly detection.

[READ THE CUSTOMER STORY](#)



## MORE ACCURATE DETECTION WITH LESS NOISE

On average organizations spend \$1.3 million, or 21,000 hours of wasted time, investigating false positive and negative security alerts. MixMode's AI can filter out the noise and surface only alerts that truly matter allowing your security team to focus and take action on real threats.

[SCHEDULE A DEMO](#)

## GET STARTED NOW



Equip your SOC with the most powerful AI in Cybersecurity today.

[GET STARTED NOW](#)



MixMode

