



# THE MIXMODE PLATFORM FOR CRITICAL INFRASTRUCTURE

## Real-time Threat Detection and Response at Scale

Critical infrastructure, which includes energy, transportation, water, and telecommunications sectors, plays a vital role in the functioning of societies and economies. However, the growing dependence on digital systems and interconnectivity has exposed these sectors to various cyber threats. The consequences of successful attacks on critical infrastructure can be severe, ranging from disruption of essential services to potential safety risks and economic losses.

Traditional security measures are often insufficient to combat the sophistication and scale of these targeted threats, as well as unable to analyze the vast amount of data generated by these diverse systems to detect threats effectively.

The MixMode Platform helps Critical Infrastructure organizations detect and respond to threats in real-time, at scale, providing deep visibility to identify threats and proactively defend against sophisticated attacks. The MixMode Platform is the world's first commercially available cybersecurity platform built on Third Wave AI (as defined by DARPA). The Platform can be seamlessly installed in minutes, immediately acclimating itself to autonomously learn, understand, adapt, and evolve without relying on rules, training, or human tuning.

The result is a truly autonomous defense system that dramatically enhances security programs, detects threats others miss in real-time, and delivers tangible business outcomes in a matter of days..

### How it Works

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

The MixMode Platform is the only generative AI cybersecurity solution built on patented Third Wave AI for threat detection and response. MixMode's self-learning AI was born out of the dynamical systems branch of mathematics and adapts itself to the specific dynamics of each network, understanding and evolving to identify threats as they arise.

## KEY BENEFITS

### Real-time Detection

Real-time and predictive dynamic threat detection for novel and known attacks.

### Increased Efficiencies

Uplevel existing investments, do more with less, and save time by focusing on the threats that matter.

### Seamless Integration

No rules, training, onboarding, or tuning required, delivering tangible results in days.

### Enhanced Visibility

Contextual dashboards with AI-informed insights and detailed visibility.

### Proven Scalability

Easily monitor large volumes of data in real-time to quickly detect and mitigate threats without increasing spend.

## MIXMODE IS THE ONLY CYBERSECURITY PLATFORM THAT CAN PREDICT AND SURFACE ZERO-DAY ATTACKS IN REAL-TIME, AND IS PROVEN TO REDUCE FALSE POSITIVES AND DELIVER 99% ALERT PRECISION



### ENERGY & UTILITIES

Protect critical infrastructure, and guarantee operations of vital services that could impact millions.



### MANUFACTURING

Maintain critical operations, protect intellectual property, and ensure product integrity.



### OIL & GAS

Prevent disruptions in energy supply, safeguard the environment, and ensure the safety of personnel and surrounding communities.



### PUBLIC SAFETY

Sustain the integrity and reliability of emergency response systems to ensure the safety and well-being of citizens.

*“MixMode can detect zero-day attacks through sophisticated anomaly detection powered by an advanced self-supervised 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**

## KEY USE CASES

### Attack Detection

Real-time detection of advanced threats, including:

- AI-Generated Attacks
- Insider Threats
- Supply Chain Attacks
- Zero-day
- Ransomware
- Zero Trust
- Identity Threats

### SIEM Augmentation

Enhance SIEM capabilities by ingesting and analyzing large volumes of data in real-time and automating the threat detection process

### Cloud Detection and Response

Defend cloud applications and infrastructure (AWS, Azure, GCP) against known and unknown threats.

## NO RULES. NO TUNING. NO DATA LIMITS. ANY ENVIRONMENT.



MixMode is the leader in delivering generative AI cybersecurity solutions at scale. MixMode offers a patented, self-learning Platform designed to detect known and unknown threats in real-time across cloud, hybrid, or on-prem 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.

Learn more at [www.mixmode.ai](http://www.mixmode.ai).