MixMode®

THE MIXMODE PLATFORM FOR FEDERAL

Third Wave AI Threat Detection and Response for Mission Critical Defense

Government agencies at the federal level handle vast amounts of sensitive and classified information, making them prime targets for cyber threats. The sheer scale and complexity of government networks, coupled with the increasing sophistication of attack techniques, pose significant obstacles to timely and accurate threat detection. Traditional security measures often struggle to keep pace with rapidly evolving attack vectors, resulting in a heightened risk of successful breaches. Furthermore, insider threats, advanced persistent threats, and nation-state-sponsored attacks further compound the challenges federal government agencies face. To effectively defend against these threats, federal government agencies need advanced and proactive solutions to identify and respond to emerging threats in real-time.

The MixMode Platform helps Federal Agencies detect and respond to threats in real-time, at scale, providing deep visibility across complex networks to detect 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 interaction.

The result is a truly autonomous defense system that enables federal government agencies to enhance their cybersecurity posture, strengthen their defense capabilities, and safeguard critical assets and information vital to national security and public trust.

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

AI-Driven 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.

Deployment Flexibility

Flexible deployment options with cloud, containerized and fully disconnected environments.

STAY ONE STEP AHEAD OF EVOLVING THREATS WITH AN ADAPTIVE DEFENSE THAT ELEVATES PROTECTION AND PERFORMANCE

Advanced Persistent Threats (APTs): Detect sophisticated APTs carried out by nation-state actors or well-funded cybercriminal groups designed to gain unauthorized access to sensitive data, disrupt operations, or conduct espionage over time.

Malware and Ransomware: Identify malicious software, including ransomware, that can infiltrate systems, steal data, disrupt operations, or hold critical systems hostage until a ransom is paid.

Supply Chain Attacks: Secure the integrity of your complex supply chain to defend against attacks targeting third-party vendors or software supply chains.

Phishing and Social Engineering: Stay ahead of Social engineering techniques that exploit human vulnerabilities to manipulate individuals into divulging confidential data or granting unauthorized access.

Insider Threats: Prevent unauthorized access to systems that compromise data security or disrupt operations from within the organization.

Emerging Technologies: Secure newly adopted technologies (cloud computing, Internet of Things (IoT), and artificial intelligence) to protect against vulnerabilities, data breaches, or unauthorized access.

> *“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

Zero Trust

Augment Zero Trust strategies to effectively identify abnormal behavior, detect advanced threats, and mitigate potential risks

NIST Framework

Ensure compliance with NIST guidelines and bolster overall cybersecurity posture.

DEFEND Phase 3

Real-time monitoring, analysis, and correlation of vast amounts of data to identify and respond to sophisticated attacks proactively.

Attack Detection

Real-time detection of advanced threats, including:

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