THE MIXMODE PLATFORM FOR HEALTHCARE ORGANIZATIONS

Real-time Threat Detection and Response at Scale

Healthcare organizations are prime targets for cybercriminals seeking to exploit sensitive medical records, personally identifiable information, and valuable research data. The vast and diverse ecosystem of healthcare, encompassing hospitals, clinics, research institutions, and connected medical devices, creates a complex attack surface that requires constant vigilance. Additionally, the rapid digitization of healthcare processes and the adoption of electronic health records have introduced new vulnerabilities and increased the potential for cyber threats.

The challenge lies in detecting and responding to threats effectively within this complex environment, as traditional security approaches often lack real-time visibility and detection.

The MixMode Platform helps healthcare organizations detect and respond to threats in real-time, at scale, to gain deep visibility, identify anomalies, and proactively defend against sophisticated attacks, safeguarding patient privacy and maintaining the integrity of critical healthcare systems. 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 system's branch of mathematics and adapts itself to the specific dynamics of each network, understanding and evolving to identify threats as they arise. 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 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. The MixMode Platform is the only cybersecurity solution that can predict and surface zero-day attacks in real-time and is proven to reduce false positives and deliver 99% alert precision.

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.

DETECT THREATS OTHERS MISS WITH AN ADAPTIVE DEFENSE THAT ELEVATES PROTECTION AND PERFORMANCE

Ransomware Attacks: Detect malicious actors encrypting sensitive patient data and demand a ransom for release.

Data Breaches: Protect against attacks designed to steal patient records, personally identifiable information (PII), and medical data.

Social Engineering: Uncover social engineering techniques, such as phishing, spear-phishing, or pretexting, commonly used to manipulate employees to gain access.

Advanced Persistent Threats (APTs): Identify sophisticated APTs designed to infiltrate networks and remain undetected, including targeted attacks and advanced malware.

Insider Threats: Minimize insider threats, including employees, contractors, or partners with authorized access to sensitive data.

Third-Party Risks: Identify risks associated with third-party relationships to prevent potential vulnerabilities.

"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.