MixMode®

THE MIXMODE PLATFORM FOR FINANCIAL SERVICES

Real-time Threat Detection and Response at Scale

The financial services industry is a prime target for cybercriminals due to its sensitive data. The ever-evolving threat landscape, the increasing sophistication of attacks, and the high value of sensitive financial data make it crucial for these organizations to have robust threat detection capabilities.

Detecting threats in the complex and dynamic environment of financial services is no easy task, as it requires constant monitoring, deep visibility, and the ability to differentiate legitimate activities from malicious ones. The sheer volume of transactions, diverse systems and applications, and compliance requirements further complicate the detection process for security teams tasked with identifying and responding to threats quickly and effectively while ensuring uninterrupted operation.

The MixMode Platform helps financial services organizations detect and respond to threats in real-time, at scale, safeguarding their valuable assets and maintaining the trust of their customers. The MixMode Platform is the only generative AI cybersecurity solution built on patented Third Wave AI for threat detection and response. 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 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.

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. MixMode is the only cybersecurity platform that can predict and surface zero-day attacks in real-time and is proven to drastically 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.

STAY ONE STEP AHEAD OF EVOLVING THREATS WITH AN ADAPTIVE DEFENSE THAT STRENGTHENS YOUR SECURITY POSTURE

Advanced Persistent Threats (APTs): Detect sophisticated APTs designed to infiltrate networks and remain undetected, including targeted attacks, social engineering, 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.

Mobile and Online Banking Security: Protect mobile apps, online banking portals, and digital payment platforms from malware, phishing attacks, and account hijacking attempts.

Unauthorized Access: Prevent unauthorized access to customer data, financial information, and transaction records.

Vulnerabilities in Legacy Systems: Identify and secure legacy systems with security vulnerabilities due to outdated software, inadequate patching, or poor system architecture.

"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:

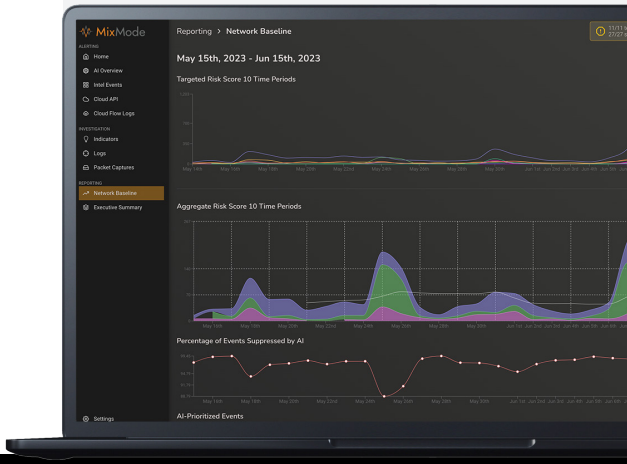
- AI-Generated Attacks
- Insider Threats
- Supply Chain Attacks
- Zero-day
- Ransomware
- Zero Trust
- Identity Threats

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.