MIXMODE ANOMALY DETECTION PLATFORM

Forbes

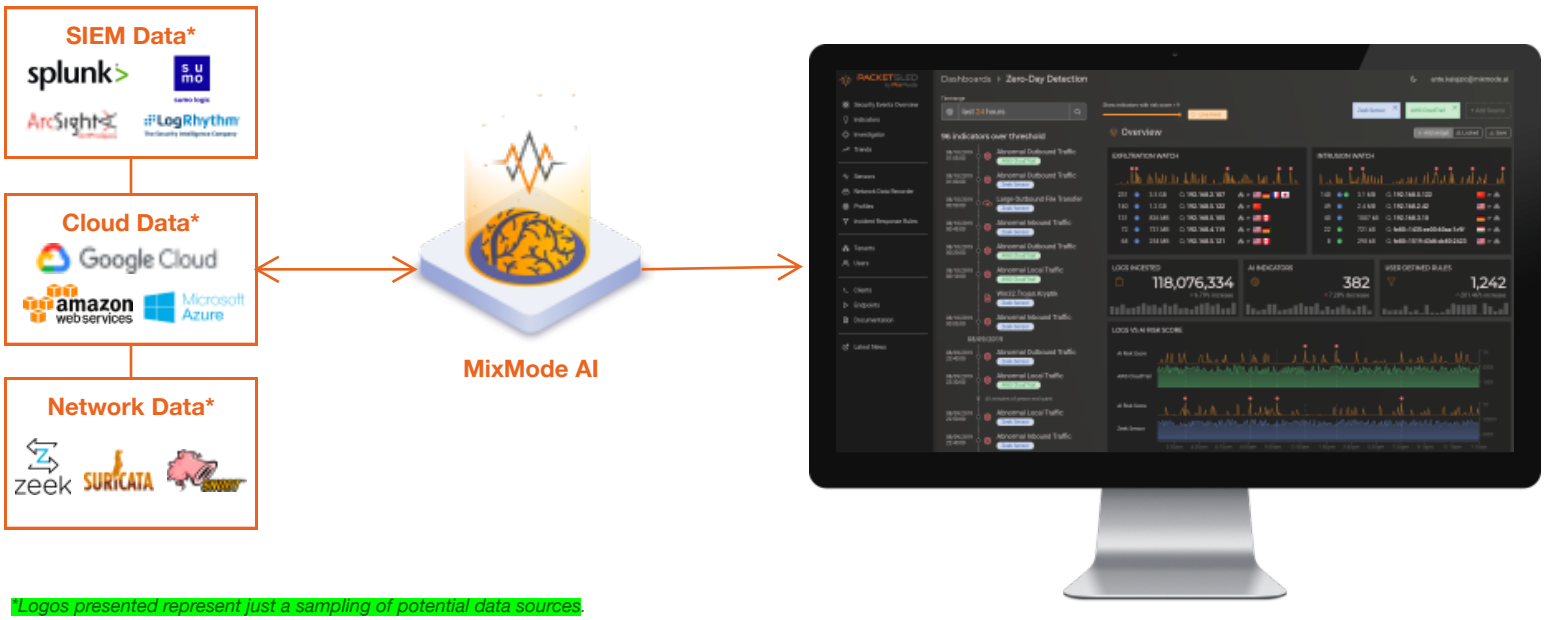
MixMode Named Top 25 Machine Learning Startups

Great Security Programs Start with Great Data

MixMode has developed a platform that leverages the first-ever deployment of Context-Aware, Third-Wave AI (as defined by DARPA) in cybersecurity to solve the challenge of zero-day threats and precise alerting. MixMode's proprietary Self-Supervised AI allows for analysis across multiple streams of data.

MixMode's AI-Enabled, Anomaly Detection Platform helps security teams solve the information overload problem by building three baselines of the given network (exfiltration, infiltration, movement and lateral) to surface zero day anomalies, drastically reduce the number of false positive alerts and automate the threat identification process. MixMode extends the life of your existing platforms by adding intelligence and predictive capabilities, leading to reduced workloads on existing SOC teams so they can be more proactive, predictive and efficient.

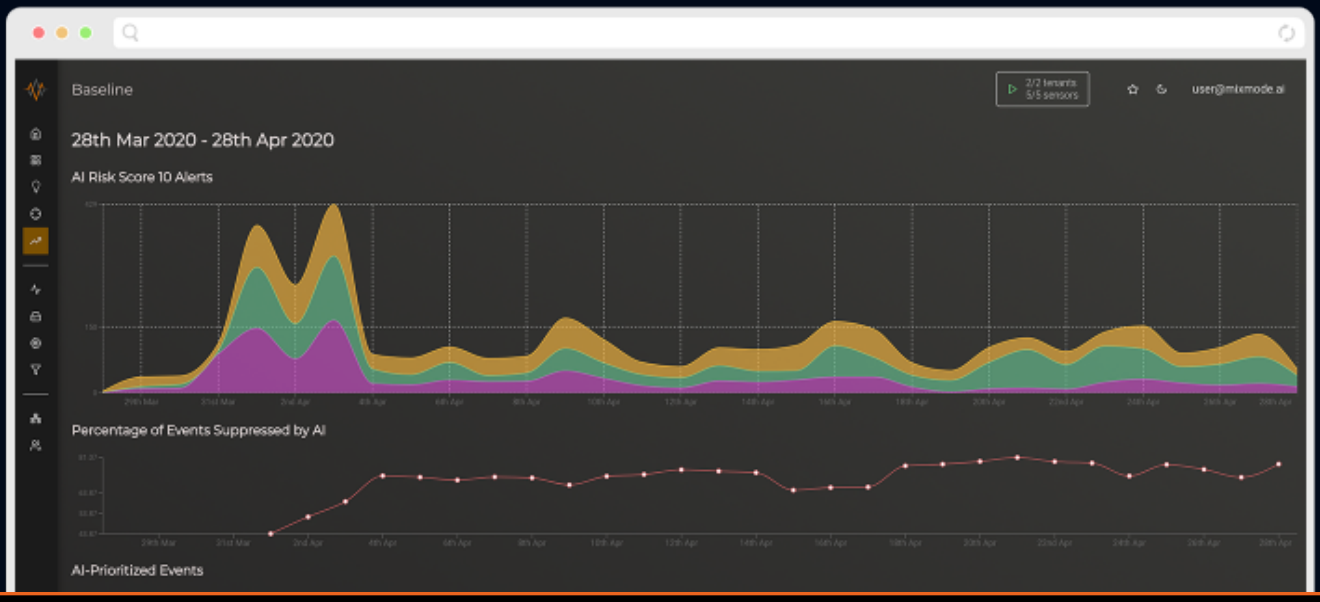
Data Flow



**Logos presented represent just a sampling of potential data sources.*

"MixMode starts learning from the first five minutes it is deployed, does not require historical data, and is adapting actively to the dynamic changes in massive amounts of network data."

- Ritu Jyoti, AI Analyst, IDC



MixMode is the foundation of a security program, providing insights on layers 2-7, identifying anomalous activity from threats and specifying the IPs that are at the source of the issue. Our AI-driven platform delivers predictive analytics within 7 days of deployment, a 25x improvement versus competing AI/ML systems requiring 6-24 months to train data and tune. With 95% alert reduction and predictive, zero-day detection, our customers' SOCs are more productive and dramatically reduce their enterprise risk level. MixMode can be deployed in the cloud, on-premise, or in hybrid environments and starts providing insight through it's AI in less than 7 days.

"With all the AI-based tools being marketed of late, it is becoming all-too-easy to miss the wheat for the chaff. But I can assure you that MixMode is the real deal."

- Ed Amoroso, Former CISO AT&T

Why Enterprises Work with Us

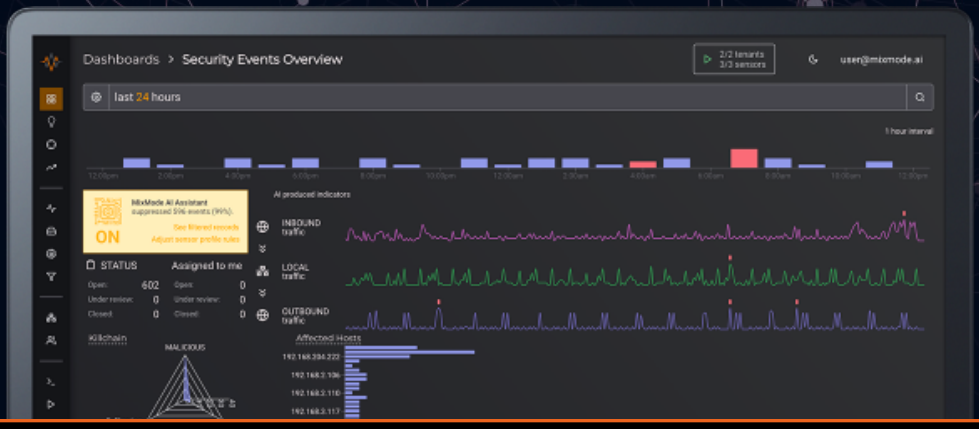
Alert Quality Improves the Whole Program
Extends the life of a SIEM, SOAR, etc.

7 Days to Network Baseline and ROI
vs 24 months for competitors

Zero Day Attack Detection Beyond Threat Intel
Predictive capability with documented case studies

MixMode Features & Benefits

- **Network Forensics & Analytics**
- **Continuous Network Baselining**
- **On Prem and Cloud Correlation**
- **Zero Day Attack Identification**
- **Full packet capture**
- **Deep packet inspection**
- **Flexible Integrations**
- **95% Alert Reduction**
- **Layer 2-7 Visibility**
- **Multi-tenancy**
- **Deployment Flexibility**



MIXMODE'S CONTEXT-AWARE AI

Patented AI Backed By Over 20 years of Research and Data

The industry is full of Cybersecurity Providers touting their "revolutionary AI," so we understand why security professionals are tired of broken promises. MixMode's patented AI, built by Chief Scientist Dr. Igor Mezic with over 20 years of experience building complex AI for DARPA and the DoD, is a massive step forward, solving some of the biggest problems in Cybersecurity today.

Most security tools leverage first or second wave AI technology that use a combination of rules & thresholds or static "training" data to make decisions about your data and can take between 6-24 months of learning to be effective. MixMode is the first available instance of patented third-wave AI in cybersecurity, and is able to provide actionable alerts about your network in only 7 days.

Self-Supervised Learning

MixMode's Artificial Intelligence can interpret, learn and respond to behavioral activities surrounding network data self-supervised and without the need for human input.

7 Days to Create a Baseline

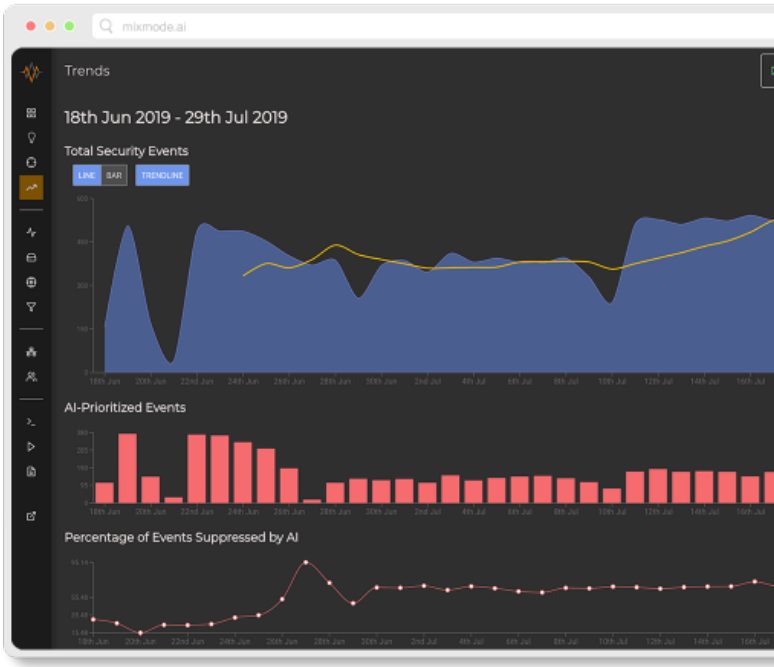
AI generates baseline of network in only 7 days rather than other systems which take 6-24 months on average. This dramatically shortens your time to value by providing full AI insights in less than a week.

Context Aware

MixMode's AI understands what your network should look like at any given time based on past underlying network data and feeds that are available. MixMode takes into account the totality of the events on the network, rather than viewing events in isolation.

Alert Reduction and Precision

The platform prioritizes which events should be investigated by security teams to prevent possible attacks by noting that certain events are aggregates of indicators and should be solved first. Typically MixMode has shown to decrease false positive alerts by more than 95% for most enterprises. > See case study here



"The goal is to make AI security more adaptive on its own rather than relying on rules that need to be constantly revised to tell it what to look for....The MixMode system is always updating its baseline of behavior so humans never have to fine-tune the rules."

- Chris O'Brien, VentureBeat

WHY THE AI IS DIFFERENT AND WHY THAT MATTERS

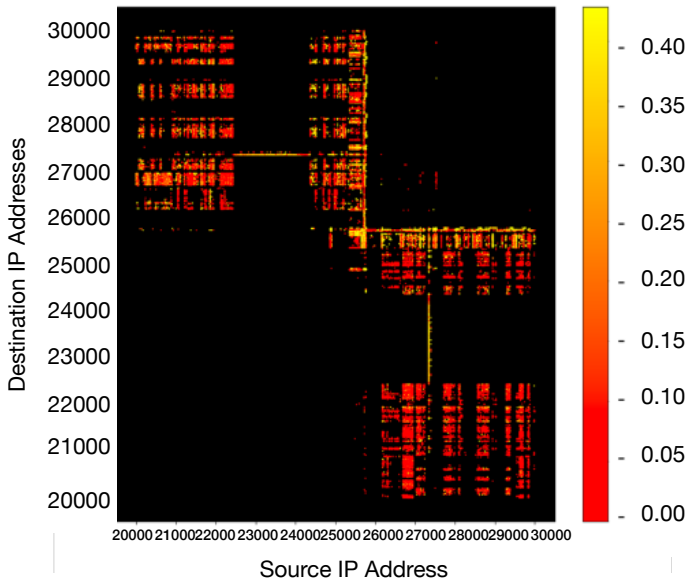
SUPERVISED	MIXMODE SELF-SUPERVISED
12-24 month training period	**7-day training period**
Dynamically changing attack signatures	**Understands its changing environment based on contextual information**
Reliance on constant operator tuning and management	**Auto-tuning and self-maintaining**
Manipulation by Adversarial AI	**Difficult to fool because its behavior adapts to new conditions**
Reliant on rules and historical intelligence - not predictive	**Predictive: Detection of security events that have never been observed (zero day events)**

Baselining Your Network

MixMode's AI creates a network baseline using the theory of Koopman Mode Decomposition, invented by its Chief Scientist and CTO in 2005, and patented for network security use by MixMode. It encodes the various spatial and temporal patterns of the data in the so-called Koopman Modes. These mathematical objects can encode the regular patterns of any timestamped data source. The MixMode platform can ingest, analyze and provide insights for on premise network data, cloud network data, CloudTrail logs and data exported from other alerting platforms. When the AI system is deployed to the timestamped data of network flows, the key learned elements are network Koopman modes – patterns that represent common behavior on the network over a specific timescale.

Surfacing Anomalies and Predictive Threat Detection with AI

MixMode's AI computes patterns of network interaction over many different timescales, and contrasts the pattern over a short interval of 5 minutes with what was seen previously. If the patterns deviate, an assessment of the security risk implied in the deviation is computed and presented to the user.



Pattern of interaction on a network on the daily timescale.

"MixMode begins learning in the first few minutes, produces useful results in about an hour and can construct a complete enterprise baseline in a week."

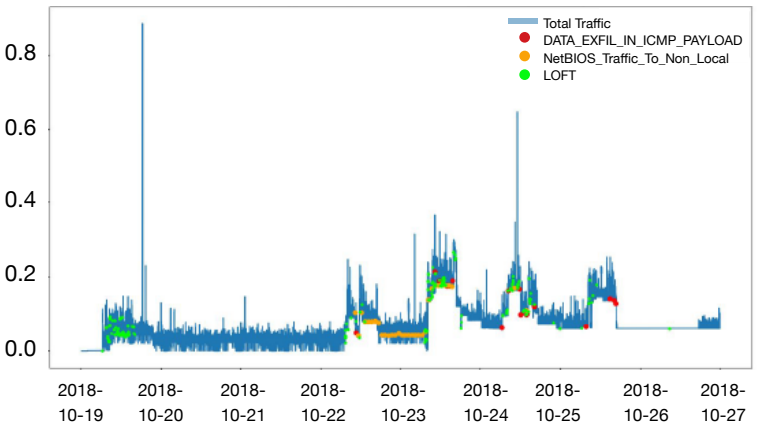
- Peter R. Stephenson, PhD, University of Leicester

Even if the threat is Zero-Day, the self-supervised nature of MixMode's dynamic learning algorithms is able to recognize it. In addition, if the risk is low, the deluge of alerts presented to the user is minimized, eliminating false positives.

Alert Precision & Alert Reduction Through Deep Network Understanding

MixMode's platform knows which alerts you should be paying attention to before you do. Our Context-aware AI monitors your network, using the created baseline to understand the entire system and learning from mistakes made along the way. The platform prioritizes which events should be investigated by security teams to prevent possible attacks by noting that certain events are aggregates of indicators and should be solved first. It is a known feature of AI systems that it is hard to build an algorithm that at the same time enables Zero-Day threat detection (and thus minimizes false negatives), and at the same time features few false positives. It is again the ability of MixMode's Koopman Mode Decomposition based AI to capture dynamic behavior on the network that is at the core of enabling such performance.

The figure above we show the time trace of the total volume of traffic on a network, shown in blue, and occurrence of several alerts from the Zeek sensor, such as Large Outbound File Transfers, shown in green. It is clear to the human eye that the patterns of larger volumes and larger number of alerts are correlated. The human intelligence would immediately conclude that most of these alerts are in fact false positives – it is simply that the total traffic has increased and thus the file sizes in that total traffic are larger as well. The exception is one green dot at the far right, where the total volume of traffic is low and non-fluctuating, and the alert occurs during nighttime. MixMode's AI detects that alert as worth investigating, just like a human analyst would, based entirely in its self-supervised, uncurated learning algorithm. Typically, MixMode has been shown to decrease false positive alerts by more than 95% for most enterprises.

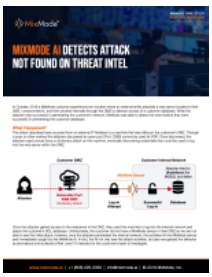


Total traffic in range and timestamps of logged alarms with nearest traffic datapoints

"Our value is tied directly to the speed at which we can react. If we can move quickly, we can prevent the spread, which means less data is infected, and fewer resources have to work on cleanup. MixMode AI quickly identifies anomalies so we can alert our clients and start our investigations."

- Travis Peska, Nisos' Managing Director of Network Operations

Resources



Customer Case Study: MixMode AI Detects Attack not Found on Threat Intel - MixMode

> Read more

Third-party Whitepaper: Unsupervised AI for Complex Network Security

> Read more

> More case studies, whitepapers, and data sheets