MULTI-STREAM SECURITY INSIGHTS AND PREDICTIVE THREAT DETECTION THROUGH UNSUPERVISED AI

AI-Enabled Network Security Monitoring for Cloud, On-Premise, or Hybrid Environments

Enterprise security teams today face a massive uphill battle. Breaches are on the rise, the attack surface is constantly shifting and bad actors are using new and more innovative techniques to hack into networks. In addition, the shortage of security staff and an ever-increasing number of alerts to sift through every day may make this task seem insurmountable.

MixMode has developed a platform that leverages the first instance of Context-Aware, Third-Wave AI in cybersecurity to solve this problem. MixMode's proprietary Unsupervised AI allows for analysis across multiple streams of data.

MixMode's AI-Enabled, Multi-Stream Network Security Platform ingests and analyzes any network data stream, whether in the cloud, on premise or in hybrid environments to correlate and prioritize the work for security teams. MixMode leverages patented, unsupervised, third-wave AI to provide predictive insight into anomalous activity, correlate and identify threats, and reduce alert noise, all in a single pane of glass.

Key Benefits

Complete Visibility Over Your Security Environment

MixMode allows you to analyze data across platforms including Cloud, SIEM, Endpoint, Firewall, and Wire Data. Analysts have the context needed to make cross-platform decisions on a single screen.

Multi-Stream Network Security Correlation

MixMode's Context-Aware Artificial Intelligence correlates data across security platforms to recognize patterns and identify threats based on information gathered from multiple streams.

Predictive Threat Detection

MixMode's Unsupervised AI is predictive in two ways. It knows what tomorrow's traffic at 3pm should look like based on models of previous traffic. Second, it is able to detect subtle anomalies in a network including beaconing and other elements that are precursors to a breach. It builds a generative model that understands a baseline of your entire environment including cloud, network, firewall, SIEM, and endpoint. This model is then used to compare expected behavior with current conditions to predict a threat as early as possible.

Intelligent Monitoring

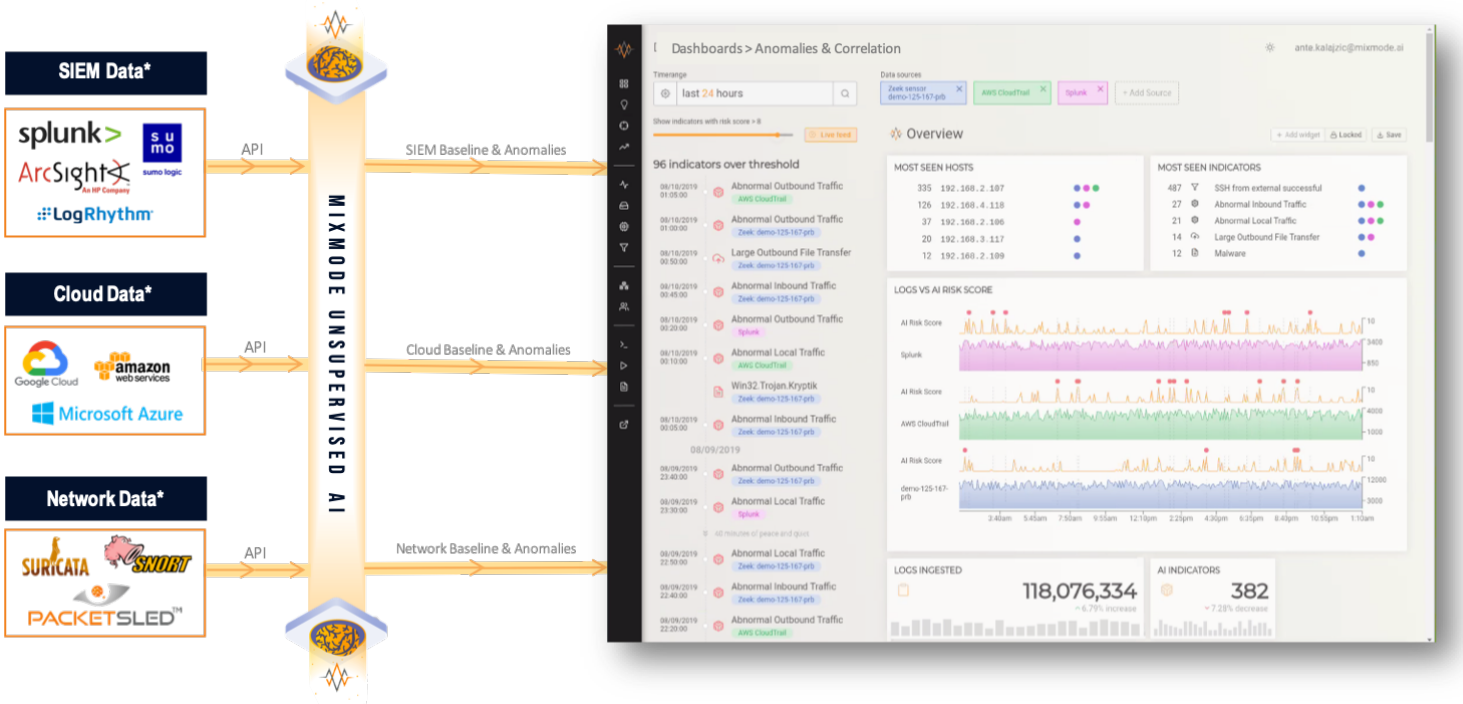
Using a combination of MixMode's baseline and a variety of threat and intelligence feeds, our Unsupervised AI compare's expected behavior with anomalies to pinpoint and surface threats in real time.

Zero-Day Attack Identification

Zero-Day Attacks exploit unknown vulnerabilities which make them almost impossible to stop with traditional security tools. MixMode's Context-Aware AI makes Zero Day detection possible by understanding your network's specific expected behavior to determine the existence of a threat that would not be detected by intelligence.

Alert Precision and Reduction Across Multiple Platforms

Most enterprise security teams have six or more different security systems generating over thousands of security alerts a day. Through a deep understanding of normal environment behavior, MixMode's Third-Wave AI helps reduce the occurrence of false positive alerts across multiple platforms by up to 90%.



Logos presented represent just a sampling of potential data sources.

MixMode's AI

MixMode's purpose-built AI leverages algorithms that were fine-tuned over a twenty-year period of deployment for various projects at the US Dept of Defense and DARPA. In adopting these AI algorithms, MixMode created a platform unlike anything else on the market — Unsupervised Artificial Intelligence tailored to the specific challenge of cybersecurity and false positive alert reduction.

MixMode's AI evaluates your network's dynamic behavioral patterns across multiple streams of data and establishes a baseline for normal business operations. This baseline evolves with your network and provides the necessary context for anomaly detection and the delivery of security alerts that are precise and actionable. More importantly, the MixMode solution provides results that are tailored to your specific deployment as opposed to solutions that are based on static training data.

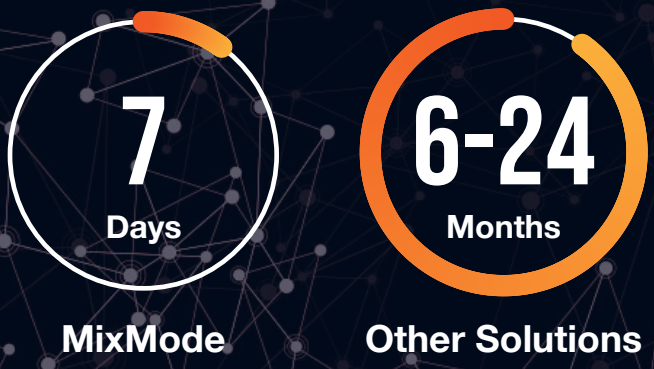
Capabilities

Unsupervised Learning
Most AI must be trained by a human or given a set of rules to learn by. MixMode understands your network unsupervised by human input or rules based learning.

Context-Aware
By creating a baseline of normal network behavior, MixMode pinpoints and surfaces anomalous behavior as it arises ensuring nothing slips through the cracks.

7 Days to Value
Most AI takes between 6-24 months to learn about and understand a network before it can provide valuable and actionable insights. MixMode's Third-Wave AI can do this in only 7 days.

Time to Value



"MixMode's AI significantly reduces false positive alerts, creating an opportunity for us to be ten times more efficient with our resources in monitoring and reacting to actual threats."

- Meghan Gorman, Founder & CEO
HighCastle

Features

Correlation Across Multiple Data Streams
MixMode ingests and analyzes data from Cloud, SIEM, Firewall, Network, and Endpoint to flag anomalies within each individual data stream and provide correlations across the platform.

Zero Day Attack Identification
By understanding new network conditions, observing all information and detecting any unusual behavior, MixMode constantly adapts to evolving security conditions for zero day detection of security events.

90% Alert Reduction
Reduce your false positives by 90%. Through an intelligent understanding of your networks normal behavior, MixMode can easily identify and filter our false positive security alerts and reduce false negatives as well.

Forensics & Analytics
With the use of threat intelligence attack detection and behavioral analysis, MixMode gives you visibility and prioritized actions for your team to mitigate risk.

Full Packet Capture
Full forensic packet capture allows you to monitor and intercept all data packets crossing your network in real-time and are stored, ready for deep packet inspection.

Deep Packet Inspection
Keep a forensic record of all network traffic to not only identify attack sources quickly but also "replay" the traffic to see other vulnerable areas of infection.

Anomaly Detection
Through a deep understanding of your environment's baseline behavior, MixMode can pinpoint anomalies in real time.

Multi-Tenancy
Whether you are an MSSP managing a portfolio of customers or an enterprise with disparate divisions or subsidiary organizations, multi-tenancy allows you to have a single view across all of your organizations without the need to co-mingle data.

Layer 2-7 Visibility
MixMode provides deep network visibility and monitors for Layers 2 through 7 of the OSI model to ensure you never miss a potential threat.