Vendor Profile

MixMode: An Unsupervised AI-Driven Anomaly Detection Platform

Ritu Jyoti

IDC Opinion

Artificial intelligence (AI) and machine learning (ML) are redefining every aspect of cybersecurity today. From improving organizations' ability to anticipate and thwart breaches, protecting the proliferating number of threat surfaces with Zero Trust Security frameworks to making passwords obsolete, AI and ML are essential to securing the perimeters of any business. By 2024, with proactive, hyperspeed operational changes and market reactions, AI-powered enterprises will respond to customers, competitors, regulators, and partners 50% faster than their peers. Digital transformation (DX) initiatives will be supported by artificial intelligence capabilities, providing timely critical insights, richer and immersive user experiences, and improved business outcomes. AI will be a true differentiator, with services that run from edge to core to cloud and hybrid and multi cloud deployments as the new norm. Organizations that master AI will take off; those that don't will dwindle. In addition:

- Today, CISO jobs come with low budgets, long working hours, a lack of power on executive boards, a diminishing pool of trained professionals they can hire but also a constant stress of not having done enough to secure the company's infrastructure against cyberattacks, and continuous pressure due to newly arising threats.
- As per Capgemini's *Reinventing Cybersecurity with Artificial Intelligence* report published last July, as digital businesses grow, their risk of cyberattacks exponentially increases; 21% of enterprises said their organization experienced a cybersecurity breach leading to unauthorized access in 2018. Enterprises are paying a heavy price for cybersecurity breaches. One-fifth of enterprises report losses of more than $50 million, 69% of enterprises believe AI will be necessary to respond to cyberattacks, and 73% of enterprises are testing use cases for AI for cybersecurity across their organizations today with network security leading all categories.
- IDC believes that MixMode's leverage of the first instance of context-aware, third-wave AI in cybersecurity to solve security team challenges is technically elegant and compelling. Network communications is the foundational data source for detecting and investigating security threats and anomalous or malicious behaviors within that network. As per customer data, rules-based and supervised learning AI systems are 20x less efficient and cause security professionals to run into the same issues and many times make them worse (e.g.,

alert fatigue). Billions are spent on products like an SIEM or SOAR that do not operate efficiently because they are ingesting too much data and an overwhelming number of false positives. "Garbage in, garbage out."

- MixMode's proprietary Unsupervised AI allows for analysis and predictive anomaly detection across multiple streams of data in real time, at scale. We expect that with growing deployments, the platform will grow more accurate and effective — especially for hybrid cloud architectures.

In This Vendor Profile

This IDC Vendor Profile examines and reviews offerings from MixMode, a private enterprise cybersecurity software company. This document reviews how MixMode's AI-enabled, multistream security platform empowers security teams to solve the information overload problem by combining and correlating data across SIEM, firewall, cloud data, and wire data into one platform and drastically reduce the number of security alerts and automate the threat identification process.

Situation Overview

Introduction/Background

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. Cyberteams are overwhelmed with data and false-positive alerts — resulting in "alert fatigue." A survey by the Cloud Security Alliance recently found that half of enterprises have six or more tools that generate security alerts. Among IT security professionals, 31.9% report that they ignore alerts because so many are false positives. This leads to billions in waste on shelfware and products that are being ignored by SOC teams. It also leads to an increasing number of breaches because SOC teams cannot identify the real alert among the millions of false positives. This death spiral of more spend and more breaches is largely because most cybersecurity platforms and systems are entirely rules based. These historical systems rely on historical threat intel feeds and rigid rules that drive massive volumes of false positives and have no predictive capability. 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.

Company Overview

MixMode is an AI-focused cybersecurity private company using patented third-wave AI originally developed for projects at DARPA and the DoD. MixMode's Network Traffic Analysis (NTA) platform provides deep network visibility and predictive threat detection capabilities, enabling businesses' security teams to perform real-time and retrospective threat detection and visualization efficiently. Used by breach response teams worldwide, security analysts and SOC teams can integrate MixMode into their playbooks and SIEMs or utilize MixMode on a standalone basis to transform investigation time, cost, and expertise required to respond to persistent threats, malware, insider attacks, and nation-state espionage efforts.

The company is headquartered in Santa Barbara with an additional office in San Diego. It has approximately 20 employees and has raised a total of $13.3 million in funding over four rounds. The company's latest funding was raised on February 25, 2019, from a venture series.

The executive team consists of highly accomplished industry veterans like John Keister and Igor Mezic. John Keister, CEO, is a serial entrepreneur with 20+ years of experience as a founder, executive, board director, and investor in both public and private technology companies. He previously cofounded two search and analytics companies that each grew to $100+ million in revenue and went public. Keister was also an early stage investor in companies such as OfferUp, Limeade (ASX: LME), buuteeq (acquired by Priceline), and Sparq (acquired by Yahoo!). Igor Mezic, CTO and chief scientist, has spent his career developing highly complex algorithms and artificial intelligence for data analytics. He graduated with a doctorate from Caltech, holds five patents, and is a professor of mechanical engineering at the University of California, Santa Barbara. He has been working on ML and AI projects for DARPA and the DoD for 20 years. MixMode's AI is the first commercial use of third-wave AI as defined by DARPA.

Company Strategy

Product Strategy

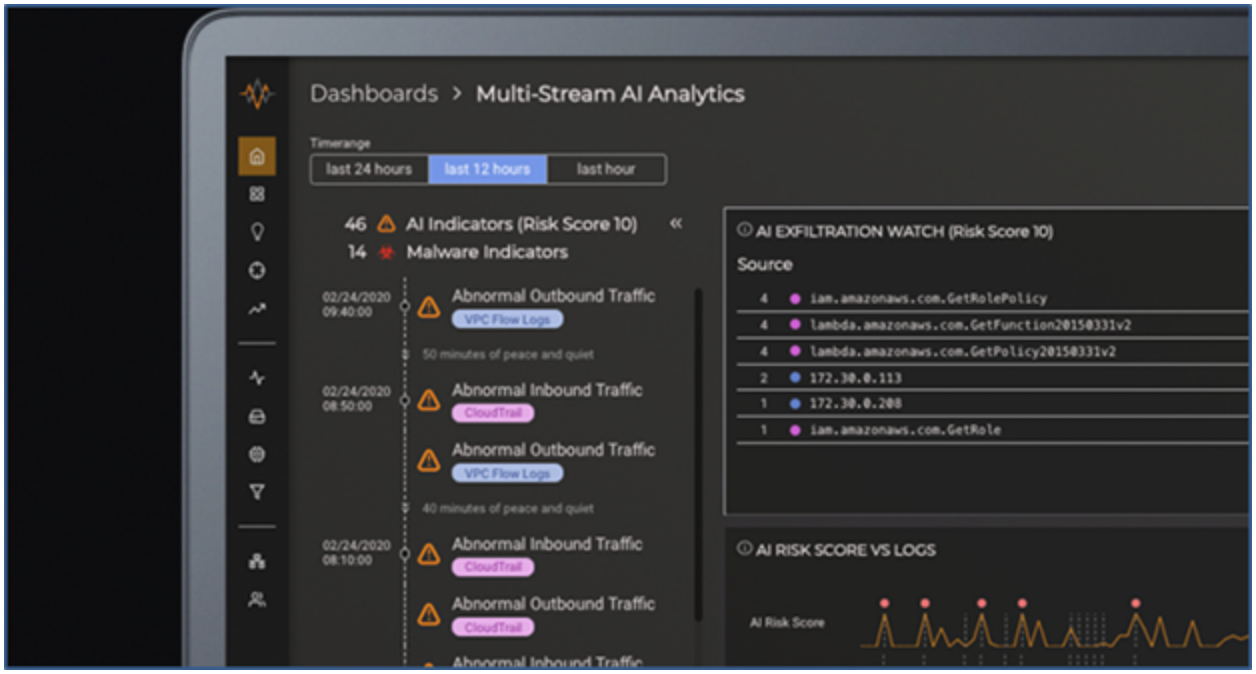
Simplicity, interoperability, and flexibility are core to a successful product strategy. MixMode's Network Traffic Analysis platform is foundational in providing actionable data on specific exfiltration, infiltration, and lateral threats on an enterprise network. MixMode can present what happens between the enterprise endpoints and how the enterprise network is interacting with the outside world, using predictive AI. Using its flexible REST API, these alerts can be easily shipped to an enterprise existing SIEM or SOAR or proprietary analytics engine. In a world where cyberteams have limited cash and people resources, MixMode is a fundamental part of a healthy security program for enterprises. MixMode offers multiple deployment options: MixMode cloud, on premises, and in customer VPC.

Product/Service Offerings

MixMode is an AI-driven NTA platform with intuitive GUI that is built to deliver precise and predictive alerts for public cloud, on-premises, or hybrid environments (see Figure 1).

FIGURE 1

MixMode Platform



Source: MixMode, 2020

MixMode's core capabilities are:

- **Multistream network security correlation:** MixMode's NTA platform supports multistream security insights and predictive threat detection through Unsupervised AI across any data stream. 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. MixMode's context-aware AI correlates data across security platforms to recognize patterns and identify threats based on information gathered from multiple streams.
- **Predictive threat detection:** MixMode's self-tuning and Unsupervised AI is predictive in two ways. First, it knows what tomorrow's traffic at 3pm should look like based on the models of previous traffic. Second, it can 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 the 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, MixMode's Unsupervised AI compares expected behavior with anomalies to pinpoint and surface threats in real time.

- **Zero-day attack notification:** Zero-day attacks exploit unknown vulnerabilities that make them almost impossible to stop with traditional security tools. MixMode's context-aware AI makes zero-day detection possible by understanding an enterprise 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%.

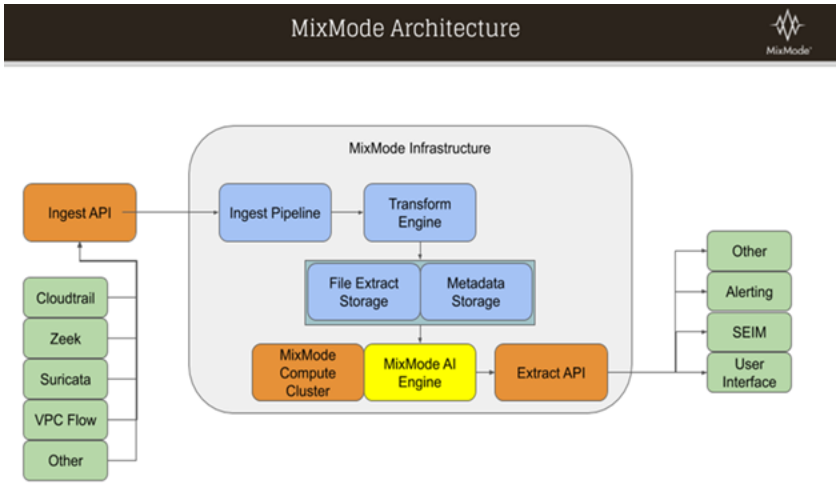
The sections that follow describe the set of underlying technologies supporting the core capabilities listed previously (see Figure 2).

Technologies

As opposed to a rule-based system, a machine learning–based AI utilizes historical data on the network and can, based on such historical data, set the aforementioned thresholds for the rules, as well as perform analysis of deviations from the previously observed behavior on the network. However, the large amount of data flowing on a typical corporate network requires a massive, computationally expensive learning effort that can last months or longer. And once the learning is finished, the dynamics of the network might have already changed, and the learning would need to start anew. The aforementioned description, although simplified, establishes the two biggest obstacles to introducing an effective AI system into network security: the dynamically changing network environment and the large amount of dynamically evolving, unlabeled data. The resolution of this problem is the introduction of the "third wave," dynamically learning, computationally efficient platform that 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. MixMode's technology provides such a platform — based on mathematical algorithms invented in 21st century — and represents a huge step forward in AI for network security.

FIGURE 2

MixMode Architecture



Source: MixMode, 2020

Supervised Versus Unsupervised Machine Learning

Supervised learning is a type of machine learning where labeled historical data is supplied as an input to an algorithm that is then trained to recognize labeled patterns. The algorithm is required to recognize newly acquired data as being of a certain type that was already present in the historical data. A typical use of such algorithms is in image recognition. Deep neural networks are often capable of recognizing objects in new images based on similar objects in many labeled images that they have been trained on. In contrast, unsupervised learning does not require prior labels. It classifies objects it sees in historical data with its own, internal labels. This is how humans in fact learn. The key to learning in this way is establishing a baseline (static background) and the deviation (motion).

In network security, zero-day threats, or even threats obtained as modifications of the well-known ones, do not come precisely labeled. Thus reliance on an unsupervised learning AI system is a necessity. But even here, the dynamically changing network profile renders the use of off-the-shelf algorithms, such as clustering algorithms, inefficient. And the issue of the large historical data sets is to be avoided.

Baselines and Anomalies

Ideally, an AI system needs to be able to discover the underlying normal and abnormal patterns on the network automatically, and dynamically adapt to them. Bayesian methods, based on the 19th century Bayes' theorem, assume a certain prior and update it with the acquisition of new data. However, there is quite a bit known about the type of dynamics that a typical network exhibits over time. As a simple example, traffic volume will be smaller over the weekend than during workdays in a typical corporate environment. An AI system does need to consider — learn — such regularities, including regularities in the "stochastic" part of the network behavior that depends on freewheeling

human exchange over the network. MixMode's AI does that using the theory of Koopman Mode Decomposition, invented by its chief scientist and CTO in 2005, and patented for network security use by MixMode. The methodology is adapted to the specifics of network data. It encodes the various spatial and temporal patterns of the data in the so-called Koopman Modes. These mathematical objects encode the regular patterns of dataflow — on a network, on CloudTrail, in alerting platforms, or on any other time stamped data source. When the AI system is deployed to the time-stamped data of network flows, the key learned elements are network Koopman modes — patterns that represent common behavior on the network over a specific timescale.

Capturing Dynamics

MixMode's AI computes such patterns of interaction over many different timescales and contrasts the pattern over the next short interval of five 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. Even if the threat is zero day, the unsupervised nature of MixMode's dynamic learning algorithms can recognize it. In addition, if the risk is low, the deluge of intel and notices presented to the user is minimized, eliminating false positives. Thus MixMode's third-wave AI makes its decisions on zero-day threats and false positives based on the intuitively transparent concept of interaction of network elements over variety of timescales — in the same way a human would — but utilizes its massive computational powers to do it efficiently.

Capturing Correlations

Correlations of activities — in time, space, and across data sources — are of critical importance to network security analysts and part of the innovation that MixMode is introducing into the security space. For example, a network analyst would expect that the observation of an intrusion into the system, could be followed by lateral movement on local hosts, and attempt to exfiltration of the data from the local network. In MixMode's AI case, time dynamics is incorporated into the guts of the algorithm. Correlations can also exist in space. Such deviations can be at the level of a few individual IPs. This is another powerful feature of MixMode's AI approach: It points out the network analyst's anomalous behavior, tracing it down to an individual IP.

False Positives and Negatives

It is a known feature of AI systems that it is hard to build an algorithm that enables zero-day threat detection (and thus minimizes false negatives) and features a few false positives at the same time. It is 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.

Adversarial AI

For any AI platform in network security, it is important that it protects from an adversarial AI system. MixMode's AI relies on learning the baseline patterns — normal, coherent and normal, random (caused by free-willed human actions) — and detecting anomalous as a difference of current behavior with those normal patterns in an unsupervised manner. Thus, for an adversarial AI to beat it, it would have to learn precisely what MixMode's AI knows. But in that process, MixMode's AI would likely detect the learning behavior as anomalous and report it. The resilience to adversarial AI is a built-in feature to MixMode's third-wave platform.

Key Differentiators/Strengths and Weaknesses

MixMode's platform differentiators are the following:

- Helps improve an enterprise security program — extends the life of SIEM, SOAR, and so forth by significantly increasing the alert precision
- Improves time to value (Average time to implement an AI system is 6–24 months with ongoing tuning. MixMode network baseline and time to value is typically 7 days with little to no tuning and maintenance.)
- Helps detect zero-day attacks through sophisticated anomaly detection powered by an advanced Network Traffic Analysis tool with AI (As per our research, so far, MixMode seems to be the only example of NTA platforms with this capability.)

Helps reduce false-positive alerts up to 95% and supports immediate productivity and efficiency gains, as noted by customer references

Business Strategy

MixMode's business strategy is 100%+ revenue growth per year. Its target market is large enterprises and MSSPs including targeted verticals (e.g., technology, finance, media, healthcare, and government). It is offered as a SaaS as well as via annual subscription.

Future Outlook

As industries shift their business models to digital-centric, data-driven customer interactions and services, they need advanced cybersecurity tactics to make sure customer data and assets always remain safe. The cyberdefense industry is investing efforts in the awareness and propagation of cyber-resiliency methods and practices. In the new world of dynamic attack surfaces and threat vectors, cyberdefense mechanisms must continuously evolve to work upon unlabeled data, which is under the purview of unsupervised learning.

For example, in the highly complex world of Internet of Things, exponential growth is occurring in the number of devices connected to the cloud for a myriad of use cases. Unsupervised learning through the usage of deep neural networks is being leveraged for attack prevention and intrusion detection. Most IoT zero-day attacks have no prior context or patterns or indications. Therefore, supervised learning approaches just don't work effectively. This is where unsupervised learning has the widest potential. The coverage and success rate are not comprehensive today, but it is the only effective way of handling such events that have not been seen before. IDC believes this area to evolve rapidly over the next couple of years.

Essential Guidance

Advice for MixMode

At IDC, we believe MixMode can benefit from the following:

- MixMode should work together with security departments in organizations or through partners to help businesses identify where deploying AI in cybersecurity can bring the most value and then help them establish appropriate goals and success metrics.

- With data privacy being topmost concern for organizations, MixMode should drive awareness on its approach of handling encrypted data traffic for analysis and the associated pros and cons.
- MixMode should continue to partner with its customers to expand its coverage and improve upon its accuracy and success rate.

Learn More

Related Research

- *Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration Forecast, 2019–2023: Finding and Mitigating the Adversary* (IDC #US44778919, December 2019)
- *IDC FutureScape: Worldwide Artificial Intelligence 2020 Predictions* (IDC #US45576319, October 2019)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com