MIXMODE CLOUD DETECTION AND RESPONSE FOR MICROSOFT AZURE

Real-time Threat Detection at Scale for Large Data Environments

Security teams have historically struggled to keep up with threats and signals across a patchwork of poorly integrated solutions that fail to cover the breadth of workloads, clouds, and devices businesses run on. With the increasing adoption of cloud computing, security teams face new challenges in securing their cloud environments. Microsoft Azure is no exception.

As organizations embrace the power and flexibility of Microsoft Azure for their cloud infrastructure, security teams encounter unique challenges in ensuring the security and compliance of their cloud environments. Organizations must address these challenges head-on by leveraging advanced cloud security solutions tailored to Azure.

MixMode's Cloud Detection and Response for Azure provides real-time monitoring of your cloud infrastructure, capable of ingesting and analyzing large volumes of diverse cloud data across Azure Network Watcher, Azure Activity Logs, and on-premises network traffic. MixMode's CDR for Azure solution is part of The MixMode Platform, the world's first commercially available cybersecurity platform built on Third Wave AI (defined by DARPA). The Platform can ingest and analyze large volumes of cloud data from multiple sources in real-time to detect threats that typically evade traditional security measures.

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

Unlimited Scalability

Easily monitor large volumes of data within your Azure environment, including Azure Activity Logs and on-premise network data.

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.

STOP WASTING TIME CHASING FALSE POSITIVES AND START FOCUSING ON THE THREATS THAT MATTER.

Real-time Threat Detection: Real-time and predictive dynamic threat detection for novel and known attacks at scale.

Systematized Investigations: Full packet capture with file extraction, deep packet inspection, and the ability to query metadata or full packets.

Guided Response: Remediation recommendations with linked intelligence and the Mitre ATT&CK Framework.

Automated Threat Hunting: Automate hunting queries and proactively hunt for malicious events with full with our User Defined Rules functionality.

"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, VP of AI Research, IDC

KEY CAPABILITIES

Correlate Large Data Sets

Correlate Activity Log traffic with NSG Flow Logs and/or SIEM logs to identify IPs that cause issues across these data streams.

Comprehensive Insights

Utilize Activity Log to monitor API calls into your Azure environment and NSG Flow Logs to access IP traffic in and out of your Azure VPC.

Unified Visibility

Gain visibility into Activity Logs and NSG Flow Logs on one platform..

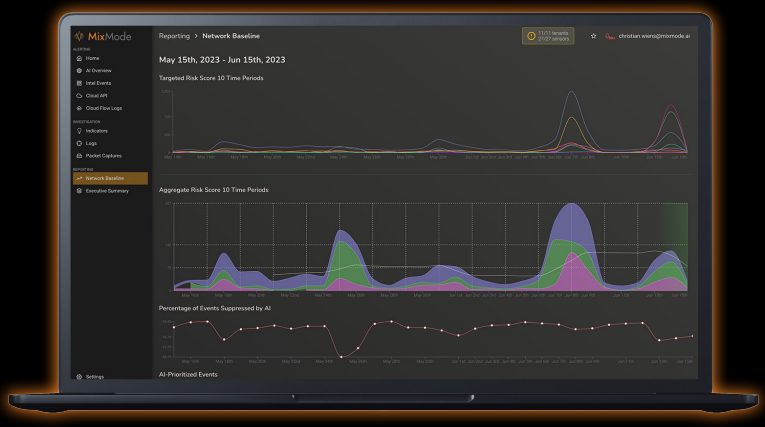
Correlate and Search

Correlate data across and investigate threats to preserve forensic records outside your Azure environment.

Threat Intelligence Integration

Enriched alerts with threat information and the MITRE ATT&CK framework.

NO RULES. NO TUNING. NO DATA LIMITS.



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.