
MixMode
SELF-LEARNING PLATFORM FOR CYBER AT SCALE
NO RULES – ONLY RESULTS

MIXMODE: WHAT WE DO

Provide real-time, precision threat detection at scale.

Cloud Native

Grounded in Dynamical Systems

Detects known and novel attacks

Large Scale Environments

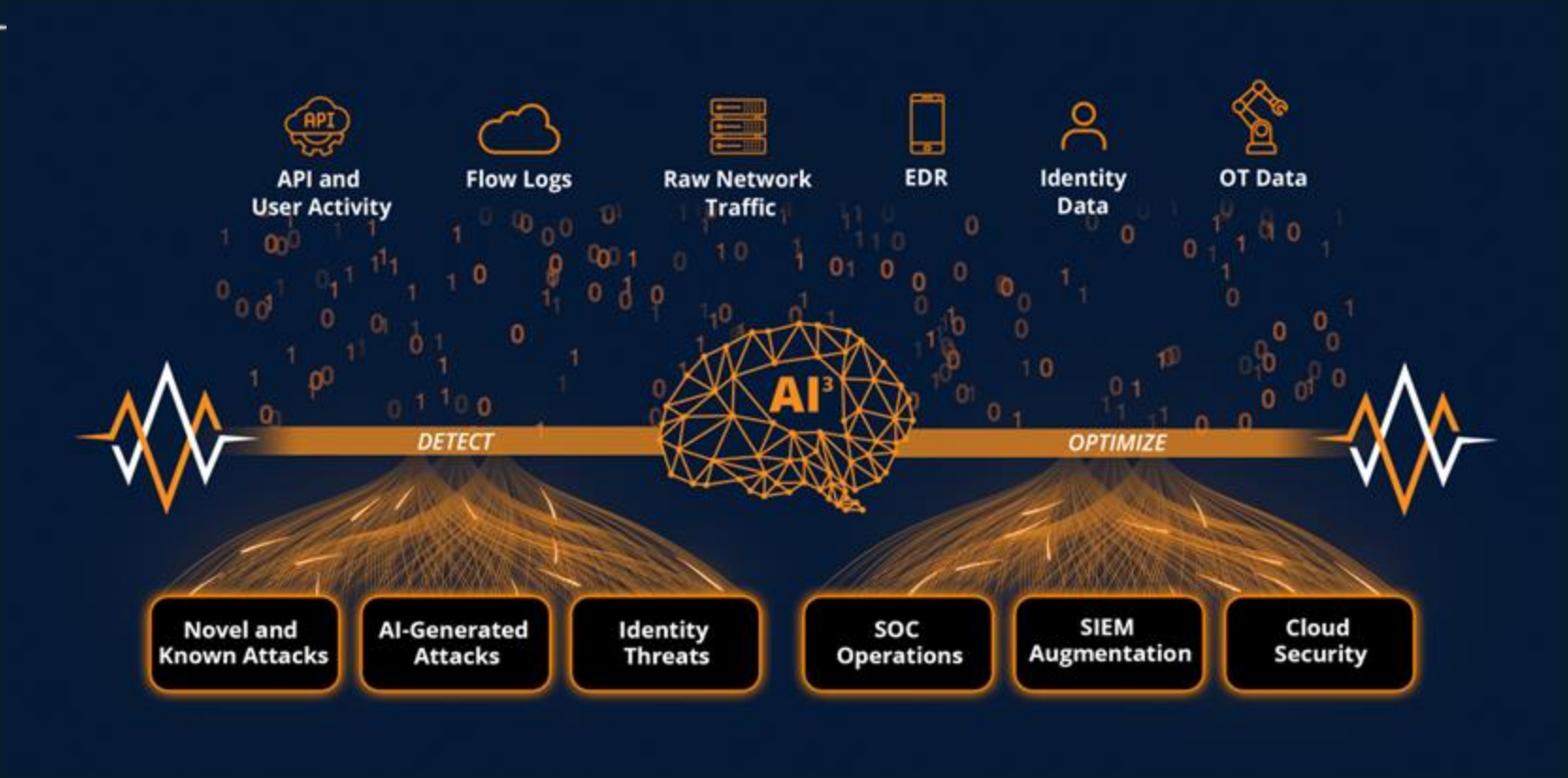
Seamless Integration

Learns, Adapts and Evolves

WHY MIXMODE'S AI IS DIFFERENT

	 SELF-SUPERVISED	 CONTEXT-AWARE	 PREDICTIVE	 GENERATIVE
3rd Wave AI	**Does not require any human operator to tune.**	**Independently able to identify in context patterns and trends, independent of historical data or contextual models.**	**Identifies pre-attack behaviors and anomalies indicative of a forthcoming attack with a live and ever evolving baseline.**	**Operates on day one without a pre-existing or established baseline. Learns, adapts and evolves to understand patterns of both appropriate and anomalous behavior.**
1st & 2nd Wave AI	Addresses security challenges based solely on historical data clustering and human inputs (labeling, training and rules).	Based only on the clustered, labeled and trained data it is fed by human operators. Incapable of AI insights outside of clustered data context.	Has no predictive capabilities because it is dependent on aggregate, normalized, historical information and rules.	Static baseline cannot evolve without human training and intervention. Takes on average 12-24 months of human training and tuning before it can provide value.

HOW IT WORKS


API and User Activity
Flow Logs
Raw Network Traffic
EDR
Identity Data
OT Data
AI³
DETECT
OPTIMIZE
Novel and Known Attacks
AI-Generated Attacks
Identity Threats
SOC Operations
SIEM Augmentation
Cloud Security

THANK YOU

APPENDIX

WHY OUR TECHNOLOGY IS UNIQUE

- MixMode offers the only Generative AI Cybersecurity Solution built on Patented Technology for Threat Detection and Response
- MixMode is the only threat detection platform that detects zero day and novel attacks in real-time and at scale
- MixMode is not one size fits all and tailors to your environment

"As a result of its AI innovations, MixMode can more easily ingest and analyze large amounts of data from customer logs than its competitors to create an evolving forecast of normal behavior."

– Gartner
AI in Security Attack Detection

THE MIXMODE PLATFORM

Real-time threat detection and response for:

- Cloud Detection and Response
- Network Detection and Response
- Identity Threat Detection and Response
- SOC Optimization

No rules. No training. No tuning. No data limits.

PROVEN MISSION OUTCOMES

Speed

Real-Time Detection

Known + Novel Attack Detection

Focus on What Matters

Scale

No Writing Rules

No Historical Training Data

No Tuning, Maintenance

Savings

Software + People

Save on Storage

Consolidate Tools

RECAP

- *Breakthrough Approach with Seamless Integration*
- *Proactive & Predictive Detection for Known and Unknown Threats*
- *Lower Cost of Ownership with Minimal Time Investment*
- *Proven Scalability Across Cloud, On-Prem and Hybrid Environments*

CASE STUDIES

CUSTOMER SUCCESS STORY: LARGE UTILITY PROTECTING CRITICAL INFRASTRUCTURE

Challenges

1. Inability to detect sophisticated threats and vulnerabilities due to log centric strategy
2. Limited experienced resources for manual rule-building
3. Lack of visibility due to the absence of a comprehensive SIEM solution capable of effectively handling and analyzing all logs.

With MixMode

1. Immediate Results: Identified active, novel attacks existing investments had missed: (Man in the Middle attack detection, +8 different attacks)

2. Increased Efficiency & Clear Visibility: Effective Alert Prioritization with focus on top 10% within the first 7 days of deployment

"If you have to **secure the entire network**, and you could only get one platform, we would use **MixMode**."

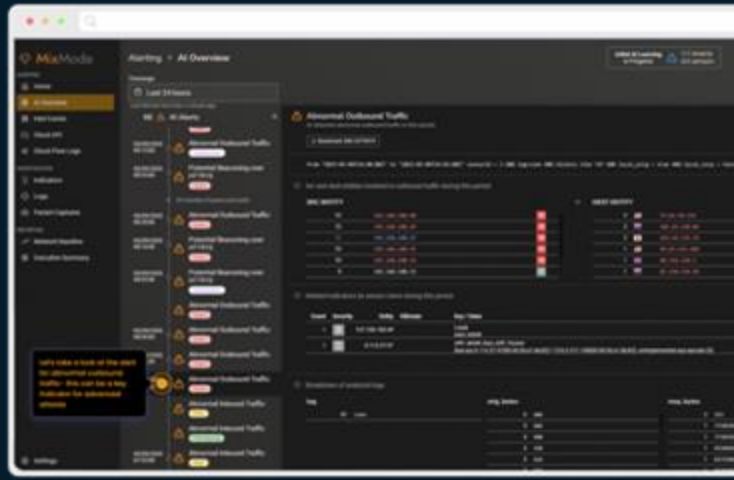
- Utility Executive

SOLUTIONS

ZERO TRUST

Easily integrate advanced network traffic analysis and threat detection capabilities to enable Zero Trust Journey:

- **Real-time Monitoring:** Continuously monitor and analyze network traffic for potential threats and anomalies.
- **Behavioral Analysis:** Leverage generative Third Wave AI that learns, adapts, and evolves to understand appropriate and anomalous behavior patterns.
- **Real-time Threat Detection:** Identify known and unknown threats, including zero-day attacks and advanced persistent threats (APTs).
- **Identity Attack Detection:** Integrate with IAM systems or ingest identity log data to help Combat identity-based threats.
- **Automation and Orchestration:** Automate manual processes without requiring training data or human operator involvement.
- **Visibility and Analytics:** Comprehensive visibility across an organization's entire infrastructure.



CLOUD DETECTION AND RESPONSE

Defend cloud applications and infrastructure from known and unknown threats.

- **Real-time Detection at Scale:** Ingest large volumes of cloud data in any format and type from multiple disparate systems to provide precision real-time threat detection
- **Increased Visibility Across Your Cloud Environment:** Monitor all cloud traffic, API calls and log data for active account misuse and advanced tactics & techniques that typically go undetected
- **Enhanced Investigations and Forensic Capabilities:** Faster investigations using full packet capture with file extraction, deep packets inspection, and the ability to query metadata or full packets

IDENTITY THREAT DETECTION AND RESPONSE

Detect threats in Okta and other IAM solutions

- **Real-time Detection at Scale:** Ingest large volumes of data across your identity ecosystem to detect threats in real-time, at scale.
- **Increased Visibility Across Your IAM Environment:** Continuously monitors and correlates behavioral, access, and log data to proactively identify threats.
- **Enhanced Investigations & Forensic:** Faster investigations using full packet capture and raw log querying for in-depth investigations.

Beta

okta

Developing

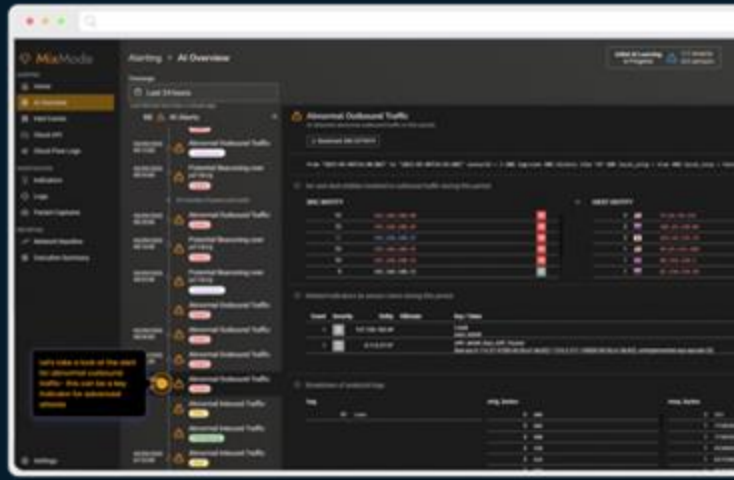
Microsoft Active Directory

aws

NETWORK DETECTION AND RESPONSE

Defend your network infrastructure from known and unknown threats.

- **Real-time Detection at Scale:** Ingest large volumes of network data in any format and type from multiple disparate systems to detect suspicious activity and traffic, unauthorized access attempts, and unusual data transfers.
- **Increased Visibility Across Your Network Environment:** Monitor all network traffic for granular visibility into network communication patterns, protocols, and data flows.
- **Enhanced Investigations and Forensic Capabilities:** Faster investigations using full packet capture with file extraction, deep packets inspection, and the ability to query metadata or full packets



SOC OPTIMIZATION

Consolidate your security infrastructure today for unified visibility, advanced threat detection, and rapid response across hybrid environments.

- **Real-time Detection at Scale:** Ingest large volumes of network data in any format and type from multiple disparate systems to detect suspicious activity and traffic, unauthorized access attempts, and unusual data transfers.
- **Consolidate Tool Sets:** The MixMode Platform integrates key capabilities found in SIEMs, UEBA, Threat Detection and Response, and other cybersecurity solutions.
- **Increase Efficiencies:** Reduce costs and complexity by collapsing your security stack into an integrated platform optimized by the only generative AI purpose built for threat detection and response

MISC.

MIXMODE: REAL-TIME THREAT DETECTION AT SCALE

API and User Activity

Flow Logs

Raw Network Traffic

EDR

Identity Data

OT Data

AI³

MixMode Applied prior to ETL

MixMode Dashboard

Cold Storage

SIEM / Data Lake

20%-80% Reduction in SIEM/Data Lake Storage

Results

- Real time novel/zero day protection across all machine generated data
- Focus on what matters
- No rules, no tuning, no human operators
- Triage, correlation, investigation across cloud, on-prem, and OT
- Vendor consolidation

MixMode

DEPLOYMENT

On-Premises
Network / OT Traffic

VM/HW Sensor

Public Cloud Data

API

Log Data
Endpoint, Identity etc.

API

Intel Feed

API

MixMode AI
(SaaS or On-Prem)

API / Syslog / JSON

Observability Pipeline
SIEM
SOAR
(Optional)

MixMode

AWS DATA SOURCES AND CAPTURE

Amazon EC2

VPC Flow Logs

VPC Flow Logs contain information on network traffic flows within entire VPCs, subnets, or specific network interfaces (ENIs) such as: source IP, destination IP etc.

Amazon S3 with SNS Topic

MixMode UI

AWS Services
(DynamoDB, Kinesis, SQS, Lambda, EKS etc.)

CloudTrail

CloudTrail provides event history of your Amazon Web Services account activity: what users, services or API's accessed what, when etc

MICROSOFT DATA SOURCES AND CAPTURE

Network Security Group and Application Security Group

Azure Flow Logs

Capture information about IP traffic flowing in and out of Azure resources. Flow logs show source/destination IP, port, protocol etc. for network communications. TFlow logs are useful for monitoring traffic patterns and detecting threats.

Activity Monitor

Azure Activity Logs

CloudTrail logs record management operations and API calls against Azure resources. This includes things like creating a VM, accessing storage, updating firewall rules, deploying ARM templates etc. CloudTrail provides a record of privileged administrative actions.

Microsoft Graph API as a Source

(AD and Audit Logs, Sign in Logs)

Via API

Storage V2 with Connection String

MixMode UI

GOOGLE DATA SOURCES AND CAPTURE

Network Security Group and Application Security Group

VPC Flow Logs

These capture information about network traffic going to and from Google Cloud VPCs. The flow logs include metadata like source/dest IP, port, protocol etc. They help monitor traffic patterns and detect anomalies.

Cloud Pub/Sub Topic

MixMode UI

Activity Monitor

Cloud Audit Logs

These logs record API calls, user activities, service configuration changes and other events related to Google Cloud management. The audit logs provide visibility into admin actions across GCP services.

WHAT ARE NOVEL ATTACKS

Novel Attacks are designed to bypass legacy rules and signature systems:

APT + Zero Day

Insider Threat

Signature-less

Supply Chain

Living off the Land

Model Poisoning

THANK YOU