Russell Gray | MixMode, Inc.

Table of Contents

"Some people call this artificial intelligence, but the reality is this technology will enhance us. So instead of artificial intelligence, I think we'll augment our intelligence."

- Ginni Rometty, IBM CEO

What is Artificial Intelligence?

Artificial Intelligence (AI) is everywhere these days. If you read the news you will see the likes of Elon Musk, Mark Zuckerberg and Eric Schmidt - among others - debating the intent and risks of a future with AI But what exactly are they talking about and why does it matter so much?

At its core AI is about creating systems that allow computers to do things that traditionally require human intelligence. It makes it possible for computers to learn from prior experience, incorporating input and feedback to refine future results. If you use SIRI or Alexa you are engaging an AI powered device that is learning from you every day. The more we use it, the more it learns and increases the accuracy of its results. AI is about giving a computer a small degree of the decision making process that humans use.

THE BENEFITS OF LEVERAGING AI

AI automates repetitive learning and discovery.

AI adds intelligence to existing tools.

AI is more accurate than humans at some tasks.

AI turns data in a competitive advantage.

AI can save an organization time and money.

MixMode™

Artificial Intelligence vs. Machine Learning

What's the Difference?

ARTIFICIAL INTELLEGENCE

A broad concept referring to the science of training machines to replicate human learning and decision making.

Created in the 1950s, Artificial Intelligence is the process of training computers to perform human tasks. Using the human brain as an example, AI endeavors to replicate how our brains take in the world around us in terms of inputs (data) and outputs (decision-making, problem solving).

MACHINE LEARNING

The method by which a computer learns and acts without an explicitly programmed function.

A possible component of AI that enables a computer to learn from experience. Machine Learning (ML) systems look for patterns and draw conclusions based on the data it sees rather than programming. ML is an application of AI that provides the system with the ability to automatically learn and improve from prior experience rather than algorithms.

ARTIFICIAL INTELLEGENCE

AI endeavors to increase the chance of success without concern for accuracy.

MACHINE LEARNING

ML endeavors to increase accuracy without regard for success.

ARTIFICIAL INTELLEGENCE

AI is complex problem decision making via simulated natural intelligence.

MACHINE LEARNING

ML allows the AI system to learn from the data to maximize the successful performance of a task.

MixMode™

Putting it All Together

ARTIFICIAL INTELLEGENCE IS THE FIELD

Artificial Intelligence is not always smart. It can be as simple as the programming on your robot vacuum or the rules that govern a filtering or alerting system.

MACHINE LEARNING IS A TECHNIQUE

Machine Learning is an approach to AI, but it is not solely used within AI There are ML uses that fall outside of AI ML is a system that can recognize patterns by using examples rather than specific programming.

DEEP LEARNING IS A FORM OF ML

Deep Learning (DL) is a set of techniques for implementing ML. DL is used for recognizing patterns within the aforementioned patterns themselves.

AI IN CYBER SECURITY

AI in the cybersecurity field usually refers to supervised machine learning and a large number of the tasks addressed are not actually human-related.

> “Every conceivable optimization opportunity has some form of machine learning applied to it.”
>
> - Srikanth Thirumalai, Amazon VP of Search

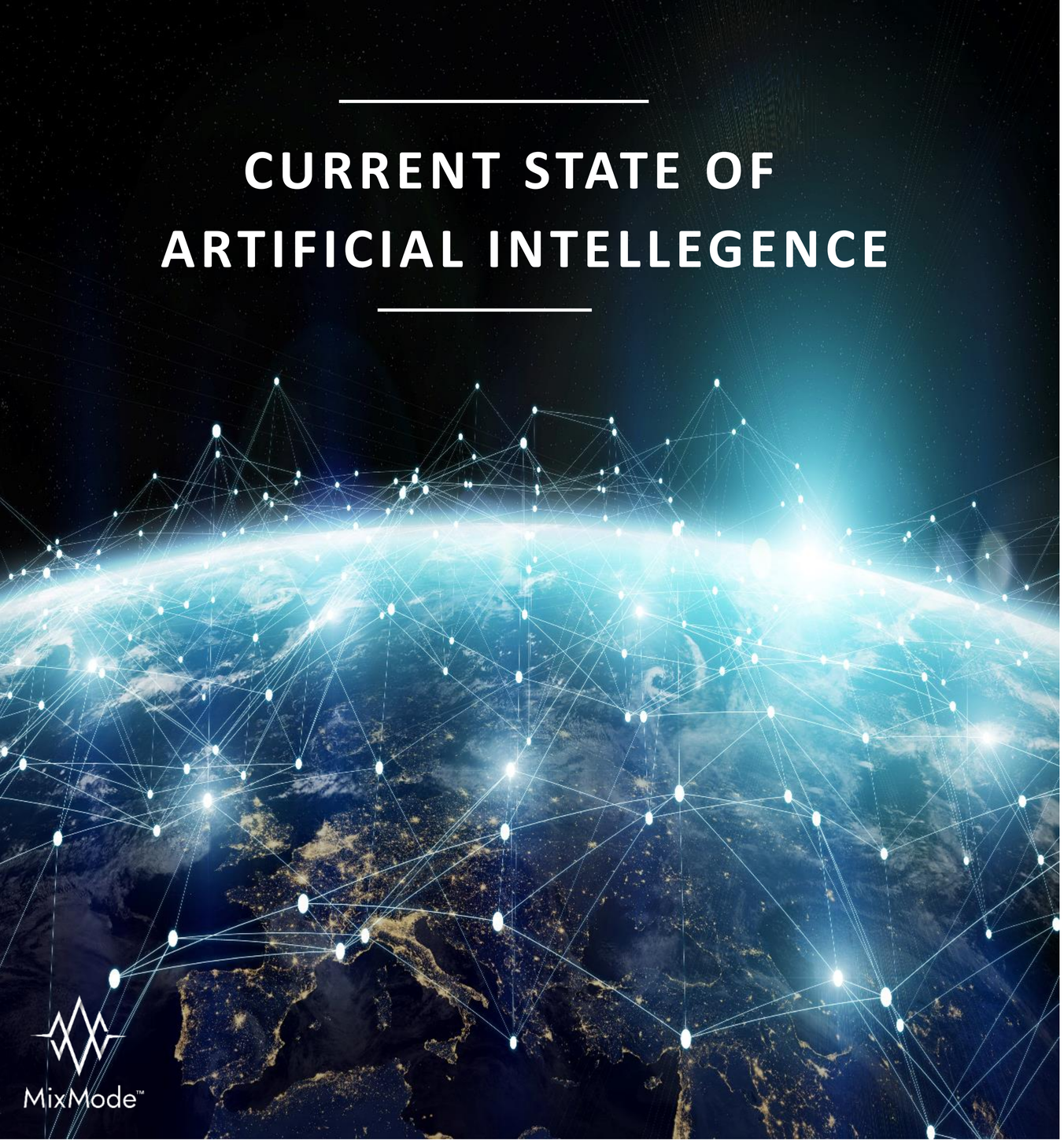
Establishing a Baseline

Artificial Intelligence in cybersecurity uses machine learning to identify malicious behavior or malicious entities. The challenge in this application is how the AI defines what's normal in your environment so that it can determine what represents an anomaly and ultimately a threat.

Within Machine Learning there are 2 primary forms used to establish a baseline and identify what's normal: Supervised Machine learning & Unsupervised Machine learning. Supervised Machine Learning is performed using training data (or prior knowledge) of what the desired output should be. Supervised learning is typically used for classification or regression where the goal is to map inputs (training data) to outputs (the environment where it is deployed) and identify specific relationships or structure within the input data that allows it to effectively produce correct output data. Commonly used algorithms include: logistic regression, naive bayes, support vector machines, artificial neural networks (deep learning), and random forests.

Unsupervised Learning, on the other hand, does not utilize training data to infer outputs, but rather it infers the structure present within a set of data points from the data itself. That is, an unsupervised learning AI identifies the inherent structure of the data it observes without using explicitly-provided labels. The typical method of unsupervised learning used in cybersecurity is clustering where the classes are unknown and therefore the inherent groupings are discovered by the AI itself.

Both methods have their value-added applications, strengths & weaknesses.



AI is Categorized by DARPA into Three Types (Waves)

1

Expert Knowledge

Rules & Thresholds

Supervised Learning

2

Statistical Learning

Training Data

Unsupervised Learning

3

Contextual Adaptation

Context-Aware

Each wave has some similarities, its own capabilities and limitations.

Out of the three, the third wave is the newest and most powerful.

See: A DARPA Perspective on Artificial Intelligence.
by John Launchbury

Rules Based AI

First wave AI systems are capable of implementing simple logical rules for well-defined problems, but are incapable of learning, and have a hard time dealing with uncertainty.

First wave AI systems examine the most important parameters in each situation they need to solve and reach a conclusion about the most appropriate action to take in that case. The parameters for each type of situation need to be identified in advance by human experts.

The hallmark of First Wave AI is input from an expert who takes their knowledge and creates rules. Programmers figure out how to solve a particular problem, then turn their insights into code. An example of this is a traditional rules-based alert or notification system wherein a set of static thresholds are set and then data is run against these rules to determine if an action should be taken.

POSITIVES OF RULES BASED AI

- First wave systems are good at static, particular facts.

NEGITIVES OF RULES BASED AI

- First wave is bad at perceiving the outside world or learning.
- First wave systems find it difficult to tackle situations it has never seen before and taking knowledge and insights derived from given situations and applying them to new, evolving problems.

MixMode™

Statistical Learning

Statistical Learning (or Supervised Learning) systems are good at understanding the world around them and can learn and adapt to many different situations when trained adequately.

In Second wave AI systems, developers don't teach the computer specific rules or thresholds (first wave) but rather develop statistical models for certain types of problems and then train these models on real world scenarios to increase precision and accuracy. This is an example of Supervised Learnning. They are great at understanding the world around them and adapting to things not seen before, however, they lack the logical reasoning capacity to ensure accuracy in all situations. Second wave systems are also only as good as the training data they are given. They are typically used for speech and image recognition as well as autonomous driving cars.

An example of second wave technology is an artificial neural network where data goes through multiple computational layers - each of which processes the data in its own way. While accurate, the training of these layers is a laborious process. Finally, second wave AI presents a causality challenge wherein we cannot explain the exact way an input is translated into an output or the data that is used to reach a given decision.

POSITIVES OF STATISTICAL LEARNING AI

- Second wave systems are good at perceiving the outside world and learning.

NEGITIVES OF STATISTICAL LEARNING AI

- Second wave is bad at logical reasoning. The primary issue with second wave is that we can't really explain or understand how they come to the conclusions that they do. There is also a risk of training data set manipulation.

Context-Aware AI

Context-Aware AI (or Unsupervised AI) leverages the system's understanding of its own environment to build explanatory models to allow the characterization of real world abnormalities.

Third wave AI systems are able to train themselves unsupervised by human input, using numerous statistical models, to understand the world they inhabit. The system is able to leverage information from several different sources to reach a well-reasoned, explainable conclusion.

Further, over time the system learns how its model should be structured and dynamically shifts to perceive the world in terms of that model. It will then use this world understanding to make decisions. In other words, the system will discover for itself the logical rules which end up shaping its decision-making process.

POSITIVES OF CONTEXT-AWARE AI

- Third wave systems take the view given by the previous waves but includes the context of its own surroundings.
- Third wave AI resolves the issues presented with the previous waves and is capable of unsupervised learning.
- Third wave AI is able to take data from statistical models, identify patterns in this data, create logical rules, and incorporate information from multiple sources to reach a conclusion on its own.

> "Third wave AI is ROBUST as it depends on generative models that cannot be easily fooled by small changes in the supplied (observed) information."
>
> - Dr. Igor Mezic, MixMode CTO

MixMode™

Cybersecurity Examples

1. RULES & THRESHOLDS

Most tools on the market today are utilizing first wave technology in some form. Think of monitoring and alerting systems where a rule or threshold is set by default and then manually tuned by human operators. The result of these systems is generally a lot of alert noise and time spent tuning alert rules for dynamic environments.

2. SUPERVISED LEARNING (STATISTICAL LEARNING)

The most prevalent form of AI in cybersecurity is Supervised Learninng. Regression-based statistical analysis utilizes knowledge sourced from existing data to develop a basis of understanding for future data. This form of Machine Learning relies on static training datasets to have an understanding of the world it is addressing.

3. (UNSUPERVISED LEARNING) CONTEXT-AWARE

The most advanced application of AI within the cybersecurity domain is the third wave context-aware system. These systems utilize portions of waves one and two but instead of relying on static rules and training data, a third wave system uses an awareness of its own dynamic environment to develop rules, identify patterns and reach conclusions.

MixMode™

Why Context-Aware AI Matters?

While there is not much debate about whether AI can be useful in the cybersecurity domain, a more valid question is whether all forms AI are equal to the task? (hint: they're not)

FIRST WAVE

First wave AI cybersecurity systems are traditional rules-based alerting tools whereby a generic threshold is applied to all environments with the burden of tuning falling on the end-user.

The Result

Too much alert noise. Too much time spent tuning for dynamic environments. False positives & false negatives.

SECOND WAVE (SUPERVISED LEARNING)

Second wave AI Cybersecurity systems are better than first wave because they do not rely on static rules but are limited by the training data the system uses to learn how to spot threats.

The Result

Less alert noise but an inability to adapt to the unforeseen. In addition, a vulnerability lies within the training data method. Hackers can foil security algorithms by targeting the data they train on. Per DARPA, "Skewed training data creates mal-adaptation of second wave systems." Finally, second wave systems are not adept at dealing with scenarios they have never seen before.

MixMode™

BEST ELEMENTS

Third wave context-aware AI essentially takes the “best” parts of waves 1 & 2 and combines them with an environmental awareness and ability to learn from its own surroundings.

PATTERN RECOGNITION

By focusing on the patterns of normal business activity, third wave systems are able to easily identify anomalous activities that when compared to attack signatures and vectors can yield actionable data.

SUPERIOR DEFENSE

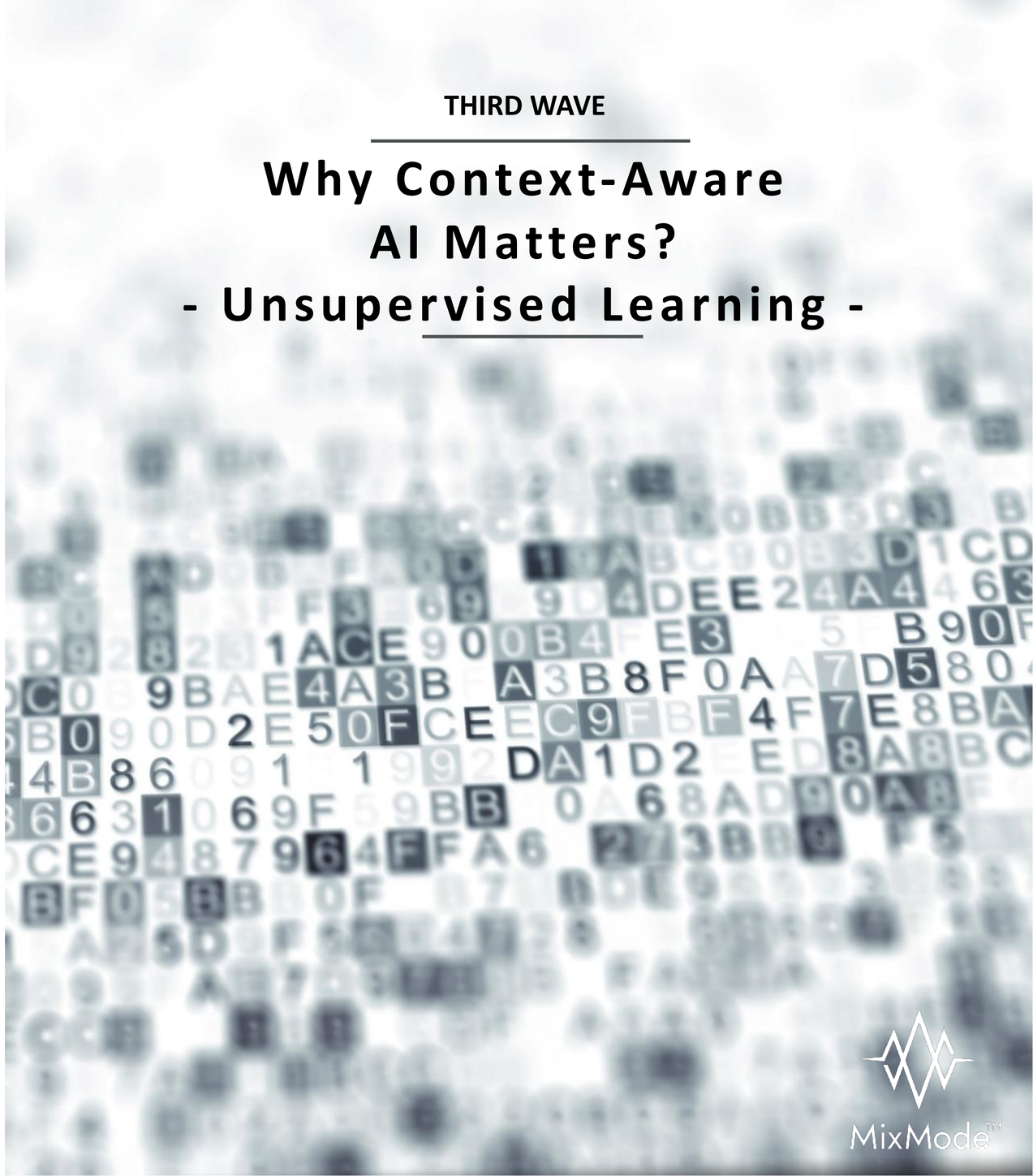
Today’s cyber attacks are more sophisticated and, in some cases, state sponsored. Mounting an effective defense requires new approaches. Protection at the perimeter and a strategy built around intrusion prevention is no longer sufficient.

ZERO DAY PROTECTION

Next-generation cybersecurity will be constructed around detections based on end-user usage patterns and anomalies. Because it is not based on static training data, unsupervised learning is the best method for detecting zero-day attacks.

THIRD WAVE

Why Context-Aware AI Matters?
- Unsupervised Learning -



MixMode™

In Summary

EVERYONE SAYS THEY HAVE AI

AI is everywhere and the term is often misused or confused with machine learning. AI has been around since the 1950s so a system's claim that they incorporate AI into their platform is not a default statement about its utility or applicability.

AI MATTERS

When done correctly, AI can provide your business with compelling results. AI systems can help automate repetitive tasks, learning and discovery of new information. They yield more accurate results and can be a competitive advantage for your organization.

NOT ALL AI IS CREATED EQUAL

AI comes in 3 forms (waves) and they are each good at performing specific types of tasks. When evaluating a solution ask yourself whether the type of AI employed is the best for a given task or problem to be solved.

CONTEXT-AWARE IS THE KEY

Context-aware or Unsupervised AI (wave 3) is the latest technology. It employs the strengths of waves one and two while allowing the system to learn from its own environment. It is more flexible than wave one systems and more accurate than wave two systems when deployed in dynamic environments that change frequently (such as corporate networks).

"Our experience shows that companies can begin to protect their systems by integrating AI into their security, starting now."

- Goosen, Rontojannis, Deutscher, Rogg, Bohmayr and Mkrtchian.

Artificial Intelligence is a Threat to Cybersecurity. It's Also a Solution

MixMode™

MixMode

MixMode’s solution PacketSled is the AI driven network monitoring and forensics platform of choice for security teams globally. Used by enterprises and MSSPs for real-time network analysis, threat hunting and incident response, the platform leverages continuous stream monitoring and retrospection to provide network forensics and security analytics. Security teams can integrate PacketSled into their orchestration engine, SIEM or use PacketSled independently to dramatically reduce the resources required to respond to threats, malware, insider attacks, and nation state espionage efforts.

The company has been named an innovator in leading publications and by security analysts, including SC Magazine, earning a finalist award in 2018 and 2019 for "Best Computer Forensic Solution.” Based in Santa Barbara and San Diego, the company is backed by investors including Keshif Ventures and Blu Venture Investors. For case studies, continuous product updates and industry news, please visit us at www.MixMode.ai or follow us @mixmode.

MixMode™

Third Wave AI With MixMode

A typical security and IT team spends an average of **395 hours** per week and over **$1.3 million** per year chasing false positives alerts.* Powered by context-aware artificial intelligence, MixMode's PacketSled platform delivers network monitoring, deep forensic analysis and incident response. Our solution drastically lowers false positives (by 90% or more) as compared to a typical rules-based monitoring system.

Alert Efficiency

MixMode's context-aware AI uses its evolving knowledge and analysis of your network to reduce the volume of security events delivered and increase the precision and context of he alerts that are delivered.

Context-Based Action

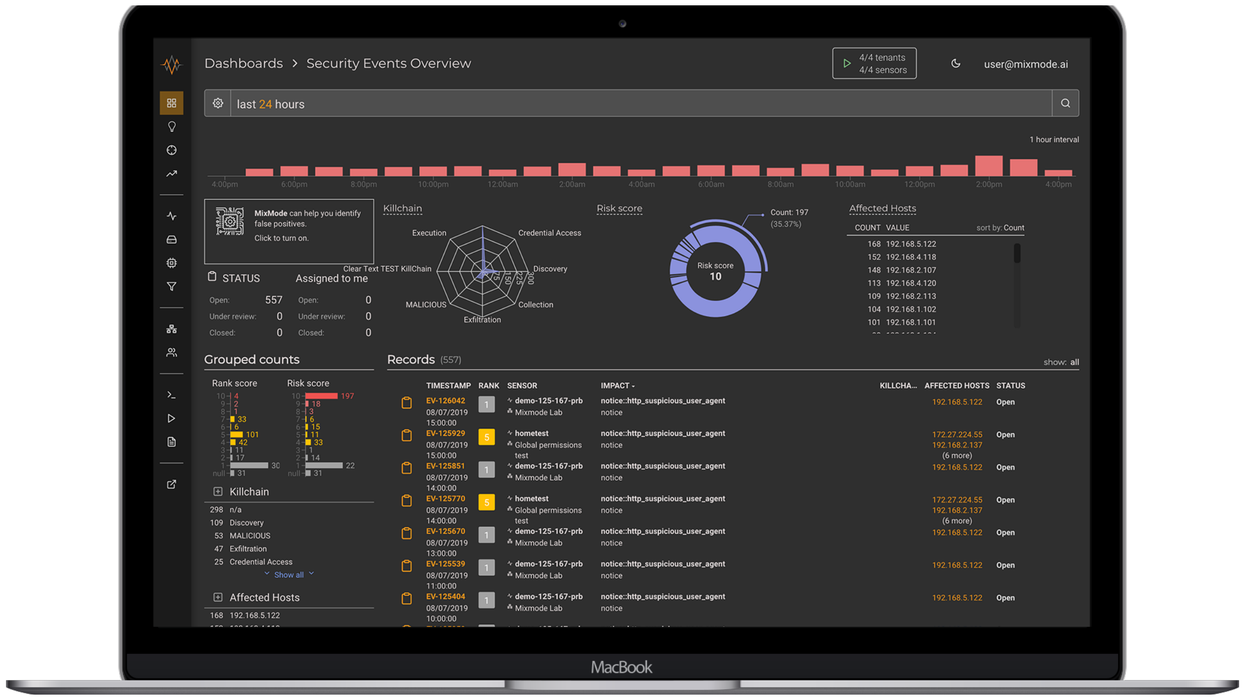
The combination of our context-aware AI and our full-packet forensic capability gives you the full picture you need to make decisions about security events from your SIEM, endpoint or firewall.

Zero Day Protection

MixMode's unsupervised learning give you access to pattern and anomaly detection that is based on your own network's behavior – not training data. The result: insight into potential zero day threats at the earliest possible moment.

Next-Gen Security

Next-generation security will be constructed around detection based on end-user usage patterns. Why settle for static training data when our AI autonomously learns and adapts to your network.



MixMode™

*according to the Ponemon Institute.

Additional Resources

Below is list of articles, videos and papers used in the creation of this eBook:

Launchbury, John, *A DARPA Perspective on Artificial Intelligence.*
Retrieved from: https://www.darpa.mil/attachments/AIFull.pdf
Viewable at: https://www.youtube.com/watch?v=-O01G3tSYpU

Tzezana, Roey (March 28, 2017). *Artificial Intelligence Tech Will Arrive in Three Waves.*
Retrieved from: https://futurism.com/artificial-intelligence-tech-will-arrive-in-three-waves

Jones, Scott (August 27, 2018). *Third Wave AI: The Coming Revolution in Artificial Intelligence.*
Retrieved from: https://medium.com/@scott_jones/third-wave-ai-the-coming-revolution-in-artificial-intelligence-1ffd4784b79e

Voss, Peter (September 24, 2017). *The Third Wave of AI.*
Retrieved from: https://becominghuman.ai/the-third-wave-of-ai-1579ea97210b

Krause, Reinhardt (November 30, 2018). *AI Companies Race To Get Upper Hand In Cybersecurity — Before Hackers Do.*
Retrieved from: https://www.investors.com/news/technology/ai-companies-artificial-intelligence-cybersecurity/

Chalaka, Ravi (February 3, 2018). *Third Wave of Artificial Intelligence (AI).*
Retrieved from: https://www.linkedin.com/pulse/third-wave-artificial-intelligence-ai-ravi-chalaka/

McAfee Labs (November 29, 2018). *McAfee Labs 2019 Threats Predictions Report.*
Retrieved from: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/

MixMode™