SOLUTION BRIEF

Artificial Intelligence Empowers Cybersecurity Insight

Human-Machine Teaming Solutions Using Artificial Intelligence, Deep Learning, and Machine Learning

The fast-and-furious magnitude of the information threat landscape is almost beyond human comprehension. Threat intelligence services respond to billions of threat queries every day and have hundreds of millions of samples in databases. The ever-increasing number of attacks intensified by speed and complexity can overpower experienced and efficient human security professionals.

Highlights

- Expand analytic capabilities to sift through increasing quantities and complexity of data and present actionable intelligence.
- Machine-generated attack analytics at the fingertips of security analysts.
- Customize and maximize enterprise's defenses without increasing staff size and expertise.
- Recognize patterns and behaviors that cause security breaches via Machine Learning algorithms.
- Improve signal-to-noise ratio for threat indicators.
- Provide advanced malware behavior analysis through deep neural networks.
- Incorporate existing investments including native and third-party controls.

Connect With Us

Analytics and human-machine teaming are the solution. While automation has long played a marginal role in the security process, increasing IT complexity, faster attack rates, and the shortage of staff talent are making analytic technologies a mandatory component of rigorous cybersecurity plans. Teaming the automated intelligence with human strategic insight provides higher security results.

By using human-machine teaming (Artificial Intelligence, Deep Learning, Machine Learning), advanced analytic capabilities are expanded to sift through enormous quantities of data and present actionable intelligence. Human-machine teaming as well as a layered approach to security can further help to detect, protect, and correct the most simple or complex of breaches, providing a complete solution for an enterprise's needs.

Intelligence gathered on threats and attacks can't alone solve an enterprise's cybersecurity challenges. Human insight gained by using intelligence allows security teams to customize and maximize an enterprise's defenses for optimum protection without increasing staff size and expertise. Intelligence lets you respond to your environment. Insights empower you to change it.

Artificial Intelligence Analytics

Using reason and logic to inspire insight

Artificial Intelligence (AI) mimics the human brain in considering value judgements and outcomes to determine good or bad, right or wrong. These same processes can elevate cybersecurity by adding complexity to Deep Learning, appending reason, suggested actions, and problem solving.

- Artificial Intelligence uses reason and logic to understand its ecosystem. AI utilizes several complex analytics, including Deep Learning and Natural Language Processing (NLP). While Machine Learning and Deep Learning can span descriptive and prescriptive analytics, AI's strength is providing more mature predictive and prescriptive analytics.
- AI relies on data from which it can be trained. AI can only learn how to handle different types of situations based on the data it is provided. As with any security process, it is imperative to identify the use case and determine the problem that needs solving.
- Cognitive computing can raise alerts and initiate appropriate action to contain threats.
- AI can be used for multiple purposes by vendors, including improved threat detection.

Key Benefits

McAfee® MVISION EDR

- Machine Learning's ability to periodically "learn" and become smarter can elevate your department's descriptive, diagnostic, predictive, and prescriptive abilities.
- Helps security teams get ahead of modern threats with AI-guided investigations that surface relevant risks and automate and remove the manual labor of gathering and analyzing evidence.
- If suspicious emails are found to be malicious, can quickly determine which machines across the organization may be impacted.
- Utilizes AI to rapidly classify threats, enabling organizations to prioritize their most critical issues.
- Uses integrated AI that helps to improve the signal-to-noise ratio for threat indicators.

Up-level existing SOC resources

The intelligence and insight of human-machine teaming makes for more efficient and sustainable endpoint security. Security teams alone cannot keep up with the volume of threats and machines alone cannot issue insightful responses.

- Advanced analytics expand detection and make better sense of alerts. AI-guided investigations and automation inform even novice analysts on how to analyze at a higher level, accelerating response time and freeing more senior analysts to focus their experienced skills on the hunt.
- AI-guided investigation reduces the expertise and resources needed to carry out investigations and increases the speed and efficiency with which analysts can verify the risk of the incident and root cause. Each analyst can be more efficient.

Figure 1. If suspicious emails or threats are detected, AI-guided investigation can locate and respond to thousands of internal and external endpoints.

Key Benefits

McAfee® MVISION Cloud

- Leverages Machine Learning to build behavior models that detect active account compromise and insider threats and apply signatures and sandboxing to identify malware in the cloud and stop threats.
- User and Entity Behavior Analytics (UEBA) automatically builds a self-learning model based on multiple heuristics and Machine Learning to identify patterns of activity indicative of user threats across multiple cloud services, and malicious behavior including insiders stealing sensitive data.
- AI-Driven Activity Mapper leverages artificial intelligence to understand apps and map user actions to a uniform set of activities, enabling standardized monitoring and controls across apps.

Better Results Faster with Machine Learning

Leveraging algorithms to detect patterns and behaviors

Machine Learning leverages automation to learn and adapt over time as new data comes in. It moves security analytics from diagnostic and descriptive to predictive and prescriptive, leading to faster and more accurate detection. Security teams can leverage Machine Learning algorithms to recognize patterns to detect behaviors that cause security breaches far more quickly than humans. As a result, Machine Learning allows endpoint security to continually evolve to stop new attack tactics. Machine Learning advantages:

- Can identify hidden malware. Pattern recognition can detect threat behaviors that lead to security breaches, whether known or unknown.
- Keeps security teams better informed so they can make better decisions.
- Helps chief security officers (CSOs) to get the most out of their staff and product assets by freeing security analysts from mundane tasks and helping even junior-level team members to become more efficient and effective.
- Helps keep up with adversaries introducing new techniques. Automating the discovery of new attack tactics and strategies helps security teams keep up with creative problem solving, while providing intelligence for your security team to promote insight for a strengthened response.
- Becomes more accurate as more data is available. The evolution of improved performance and capacity enhancements enable Machine Learning to learn and increase accuracy in cybersecurity functions.
- Helps IT teams analyze faults. When endpoint security cannot prevent damage from an attack, Machine Learning accumulates relevant data elements into one place, placing it at the fingertips of security analysts when needed.

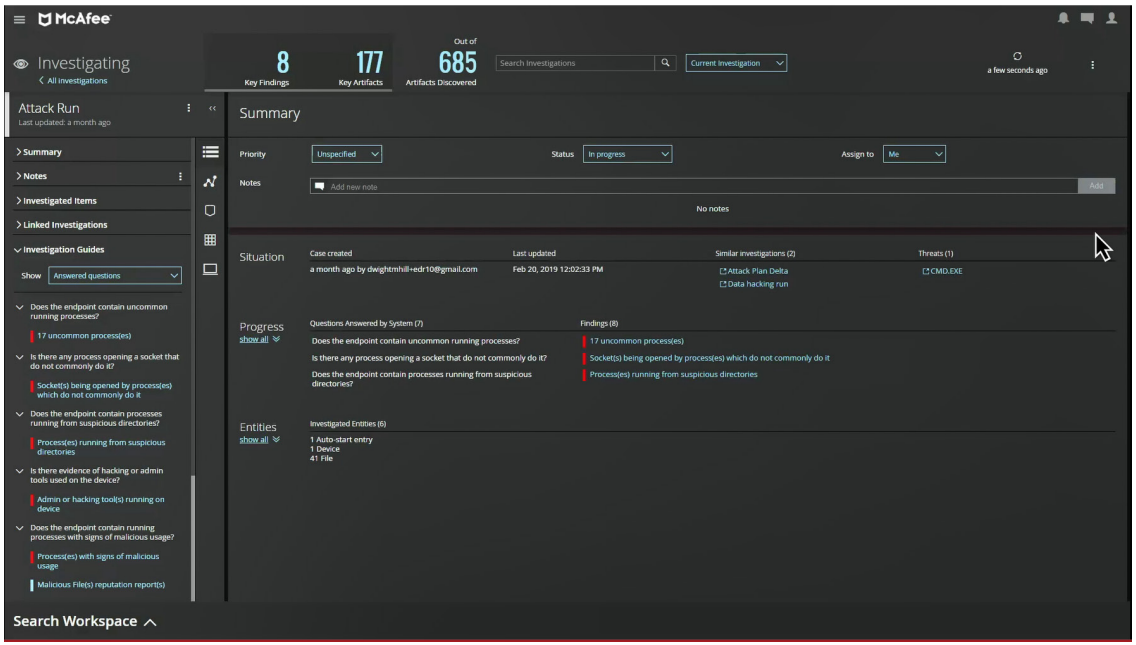

Figure 2. Artificial Intelligence-guided investigations automate and remove manual labor of gathering and analyzing evidence.

Deep Learning builds on Machine Learning

Deep Learning gives a cybersecurity defense system the ability to automatically learn through billions of combinations and observations, reducing the dependency on human resources. Deep Learning assists with defense decision making while building on Machine Learning to detect, protect, and correct against old and new threats. Deep Learning reflects multi-faceted security behaviors in its multiple complex algorithms, while also identifying outliers and unique relationships.

- Deep Learning is effective because the more it sees, the more it knows. Deep Learning's methodologies employ neural network algorithms to reach conclusions by looking at what happened in the past, applying reason, and by paying attention to current and predictive data.
- Deep Learning's algorithms are likely to be as complex as the situation. Deep Learning can be descriptive, diagnostic, predictive, and prescriptive as well.
- Deep Learning methodologies may work with symbolic and conceptual information for complex decision-making. It can be directed to mitigate threats based on analyzing patterns of activity and defining which activities appear normal and expected, as opposed to which appear to be anomalies.
- The effectiveness and efficiency of Deep Learning's algorithm is dependent on effective data sets.

Learn More

For more on the advantages of using Artificial Intelligence, Deep Learning, and Machine Learning in cybersecurity, read the McAfee white paper: Introduction to Artificial Intelligence and Machine Learning.

Forrester Spotlight: Empower Security Analysts Through Guided EDR Investigation report

SANS: Why Traditional EDR Is Not Working—and What to Do About It white paper

SANS: Why Traditional EDR Is Not Working—and What to Do About It webcast

Additional Resources

Watch the AI-Guided Investigations with MVISION EDR video

McAfee MVISION Cloud
Request a Demo

McAfee Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com