Proactive Companies Strengthen Cyber Security with AI

As organizations rely more heavily on digital technologies, they also face more frequent and sophisticated cyberattacks. To protect critical company assets and preserve business reputation, organizations increasingly seek ways to strengthen cyber security with AI. When used wisely and combined with human oversight, AI proves indispensable in today's digital environment.

AI-enhanced cyber security tools offer several advantages over traditional cyber security. By processing data at scale and utilizing machine learning, for instance, they improve threat detection. They also augment authentication and data loss prevention (DLP). Consequently, leading cyber security providers harness the power of AI to deliver world-class solutions.

Improve Threat Detection and Remediation

AI can analyze vast amounts of data from various sources, such as endpoints, networks, cloud services, identity systems, and applications. Then, using machine learning, it can then spot anomalies in that data that indicate possible malicious activity. AI can also learn from new data and adapt to changing threats, making it more effective than traditional rule-based systems.

For example, Microsoft Defender for Endpoint uses AI to detect advanced attacks like ransomware, fileless malware, zero-day exploits, and supply chain compromises. Using AI, Defender will prioritize alerts based on severity and context. It can even automate response actions such as isolating devices or blocking processes.

Strengthen Authentication and DLP

Organizations gather and store sensitive information including customer information, financial data, protected health information (PHI) and trade secrets. Keeping that information safe from unauthorized access or loss proves vitally important in preserving customer trust, staying competitive and maintaining regulatory compliance.

AI plays a key role in zero trust security, which requires continuous identification of all users and devices. For instance, AI enables adaptive authentication, adjusting the level of verification based on the context and risk of each request. Using AI, organizations can define and enforce granular security policies based on device health, encryption, password strength and more.

Additionally, products like Microsoft Purview use AI to enhance DLP by automating the classification of sensitive data. Organizations can then use sensitive data labels to enforce automated policies for data sharing, encryption, and retention.

Benefits of AI-enhanced Cyber Security Solutions

Automating cyber security with AI delivers several key benefits for organizations, including:

- Reducing human error – AI automates repetitive and tedious tasks prone to human fatigue and oversight, such as monitoring network traffic and analyzing logs. It can also analyze large and diverse data sets quickly to identify patterns that humans might not recognize.
- Improve efficiency and reduce costs – AI gathers and analyzes data continuously, enabling dynamic incident detection and response. With AI, security teams can often address potential

problems before damage occurs. And because AI handles the routine, time-consuming tasks, humans can focus on strategic activities.

- Discover unknown threats – AI can rapidly detect anomalies that might indicate vulnerabilities that software providers have not yet identified or patched. Additionally, using machine learning, AI solutions learn and improve from feedback such as false positives, false negatives, and new threat information.

Partner with eMazzanti to Strengthen Cyber Security with AI

AI is changing the cyber security space, offering cutting edge tools for preventing, detecting, and responding to security incidents. But it does not represent a silver bullet. Security teams must choose their tools wisely and implement them carefully. And they need to recognize both the possibilities and the limitations of AI technology.

For instance, while machine learning can take threat detection to new heights, machine learning tools depend on quality data to produce accurate results. Information governance thus goes hand in hand with security efforts. And even the most sophisticated tools require the oversight of humans who know how and when to use them.

The cyber security experts at eMazzanti Technologies combine a wealth of expertise with cyber security solutions that leverage AI. For instance, eCare Secure Route uses big data analytics and machine learning to automate protection against known and unknown threats. With this technology it can discover, and even predict, attacks before they launch.

Our security consultants will work with your organization to identify and implement the right tools for your business needs.