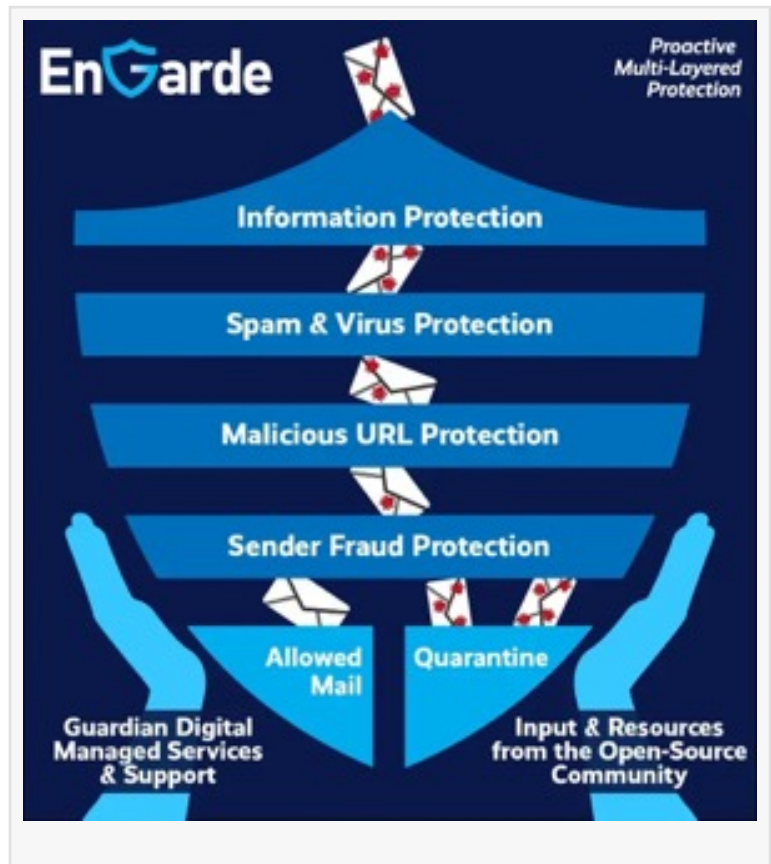


Guardian Digital Defends Email Against Adversarial AI Attack Tools with Defensive AI, Open Source Tools

NEW JERSEY, UNITED STATES, May 1, 2023 /EINPresswire.com/ -- [Guardian Digital](#), the open source email security solutions company, reaffirms its solution protects against hostile AI attacks deployed by threat actors with AI-powered email threat protection and open source. The tool analyzes the hacker's behaviors to determine if they have a specific pattern, as well as removes false positives, as it is one of the most difficult tasks for security analysts to distinguish between noise and signal when working with large datasets. The timing of the attack and the way hackers behave inside systems are all included so that AI-powered technology can detect and respond to attacks with greater accuracy.



As cyberattacks grow increasingly complex and difficult to detect, email security solutions are leaning heavily on artificial intelligence (AI) to keep organizations safe from advanced threats. Unfortunately, the same capability found in AI tools, such as ChatGPT, can also be used for malicious purposes resulting in a heightened threat from AI powered threat actors. Guardian Digital addresses these concerns with [EnGarde Cloud Email Security](#) solution that uses AI-powered auto-learn capabilities to adapt to evolving threats, upgrading its protection in real-time to safeguard against known and unknown threats. AI possesses a deep understanding of each user and device in an organization's system with an evolving understanding of what is considered normal to detect subtle deviations which could be the warning signs of an emerging attack.

The Threat of AI-Powered Threat Actors

The use of AI-based tools in cyber threats has the potential to revolutionize the way they are created and executed. AI models can generate text and speech that sounds like human speech,

which can be used to automate phishing emails and social engineering attacks. Generative AI in cybersecurity allows threat actors to develop more convincing and sophisticated attacks. For example, a generative AI model trained on a large database of phishing emails could generate new, highly convincing emails that are more difficult to detect.

The potential impact of AI-powered threat actors on individuals, organizations, and society as a whole is significant. As AI and machine learning technologies advance, cyber attackers will be able to execute attacks with greater speed and efficiency, which could lead to widespread data breaches, financial losses, and even physical harm. AI-enhanced disinformation operations could also have a profound impact on democracy and human rights.

Threat actors can use AI to scale up cyberattacks, evade security controls, and find new vulnerabilities in email security systems. Machine learning is also used for malware analysis, and next-generation AI is leveraged to create malware that can bypass traditional security measures.

It is important to develop countermeasures to protect against AI-based cyber threats. These could include incorporating AI into security systems to detect and respond to attacks, developing regulations to limit the use of AI in cyberattacks, and educating individuals and organizations on how to recognize and prevent AI-powered attacks.

EnGarde's Multi-Layered Security and Advanced Threat Protection

It is crucial to address these threats promptly, fortunately, the same technology is available for defense. [Using AI and cybersecurity together](#) can improve defenses against these attacks.

- EnGarde offers proactive, multi-layered security systems that accelerate detection, containment, and response to cyber threats, easing the burden on businesses and allowing more productivity.
- EnGarde leverages the inherent security benefits of open-source architecture to provide superior protection against cyber threats, fostering transparency, reliability, and longevity in the development of solutions.
- EnGarde utilizes Machine Learning to improve email security by identifying malicious emails that traditional security methods may miss, as well as to develop defense responses, and quickly identify, prioritize, and remediate new attacks.
- EnGarde leverages AI in global threat intelligence to prevent AI-driven attacks by detecting and mitigating potential threats before they cause harm.
- The AI algorithms can analyze large volumes of data and identify patterns and anomalies that could signal an attack. By integrating AI with human expertise, organizations can create a more effective security system that can quickly respond to emerging threats.
- EnGarde offers fully managed services, securing business email with around-the-clock monitoring and maintenance by a team of experts, dedicated to understanding the evolving risks and applying specific real-time guidance to each individual business.

About Guardian Digital

Guardian Digital, Inc. builds enterprise email solutions with an intense focus on security and unrivaled customer support, designed to ease information technology overhead for its customers. Since its inception in 1999, Guardian Digital has pioneered the open-source architecture security-as-a-service email protection model to block today and tomorrow's sophisticated threats to email integrity. Guardian Digital continues to innovate the email security marketplace using technology unavailable from any other vendor. Its EnGarde Cloud Email Security leverages the benefits of open-source development, contemporary cloud technologies, and decades of combined experience protecting enterprises. Guardian Digital is dedicated to its customers and their safety is the very foundation of what the company offers and builds on in regard to business email protection.

Connect with Guardian Digital on: [Twitter](#) | [LinkedIn](#)

Guardian Digital is a registered trademark or tradename of Guardian Digital, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

Media Contact

Company Name: Guardian Digital Inc

Contact Person: Justice Levine

Email: jlevine@guardiandigital.com

Phone: 1-866-435-5469

State: New Jersey

Country: United States

Website: <https://guardiandigital.com/>

Justice Levine

Guardian Digital, Inc

+1 866-435-5469

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/630760825>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.