Adaptive Email Security Best Practices: Why AI Alone Is Not Enough

concentrix | IRONSCALES

Introduction: The Email Security Challenge

In today's world, the reliance on technology has never been greater—and so have the threats against it. Nearly every organization now relies on advanced AI-powered email security solutions. These tools have become a critical line of defense against increasingly sophisticated cyber threats, such as phishing and business email compromise (BEC) attacks.

Artificial intelligence (AI) and machine learning (ML) are vital components of this defense system, analyzing massive datasets, detecting anomalies, and shielding users from cybercriminals. However, even the most advanced technologies aren't foolproof. While AI can detect patterns, it sometimes falls short in deciphering human deception and the evolving strategies used by attackers. This is where the invaluable partnership between human insight and AI technologies comes into play, creating a robust defense strategy.

This e-book explores how combining AI and ML with human intelligence forms the cornerstone of a strong email security strategy. Through real-world examples and in-depth analysis, we explain the strengths and limitations of AI, the role of human expertise, and how solutions are utilizing this partnership to safeguard organizations.

The Role of AI and ML in Email Security

Email remains one of the most vulnerable points of entry for cyber attacks. BEC attacks alone caused over $50 billion in global damages in 2022,[1] underscoring the critical need for AI-driven defenses.

AI uses algorithms to analyze vast amounts of data, quickly identifying patterns and predicting potential threats. Meanwhile, ML enhances AI's capabilities by allowing systems to learn from past events and improve over time. This combination provides unmatched speed and accuracy in detecting anomalies within email content.

How ML Models Work

ML models are built on variables and features extracted from data inputs, such as the time an email was sent, the sender's domain, and even the sentiment of the message. These features are analyzed by algorithms to detect suspicious activity, such as phishing links or unusual sender patterns.

However, these models face challenges. For example, as cybercriminals evolve and create more sophisticated attacks, AI and ML need to continuously adapt. Despite their abilities, false positives and negatives can occur—cases where legitimate emails are flagged or, conversely, threats go undetected.

[1] "Business Email Compromise: The $50 Billion Scam," FBI Public Service Announcement I-060923-PSA, June 9, 2023.

The Value of Human Insights

AI and ML cannot replace human intuition, which is often essential for detecting context-sensitive anomalies. Humans can perceive subtleties in communication, such as suspicious intent or tone, that AI might miss.

Human-in-the-loop models enhance AI by providing real-time feedback. As security analysts review and flag suspicious emails, their feedback improves the AI's future performance. This creates a feedback loop, making the system increasingly accurate over time.

Challenges of AI and ML in Cybersecurity

While AI and machine learning represent transformative advancements in cybersecurity, they are not without challenges. Cybercriminals are evolving at an unprecedented pace, adopting sophisticated techniques to outmaneuver even the most advanced AI-based systems. By leveraging their own AI-driven tools, attackers can craft more convincing phishing emails and bypass security filters that rely solely on static algorithms.

Moreover, AI-based security solutions often face limitations due to biases and gaps in the training data. For example, regional nuances, cultural contexts, and industry-specific jargon can present challenges for AI models, making them less effective in detecting malicious intent cloaked in tailored communications. False positives and negatives can still occur, disrupting business processes or allowing threats to slip through unnoticed. Overcoming these limitations requires continuous retraining, adaptation, and, crucially, the integration of human expertise to interpret and refine AI outputs.

Cybercriminals are evolving at an unprecedented pace, adopting sophisticated techniques to outmaneuver even the most advanced AI-based systems.

Crowdsourcing allows for shared threat intelligence, enabling practitioners across different sectors to learn from each other's experiences.

Leveraging a Crowdsourced Network for Enriched Defense

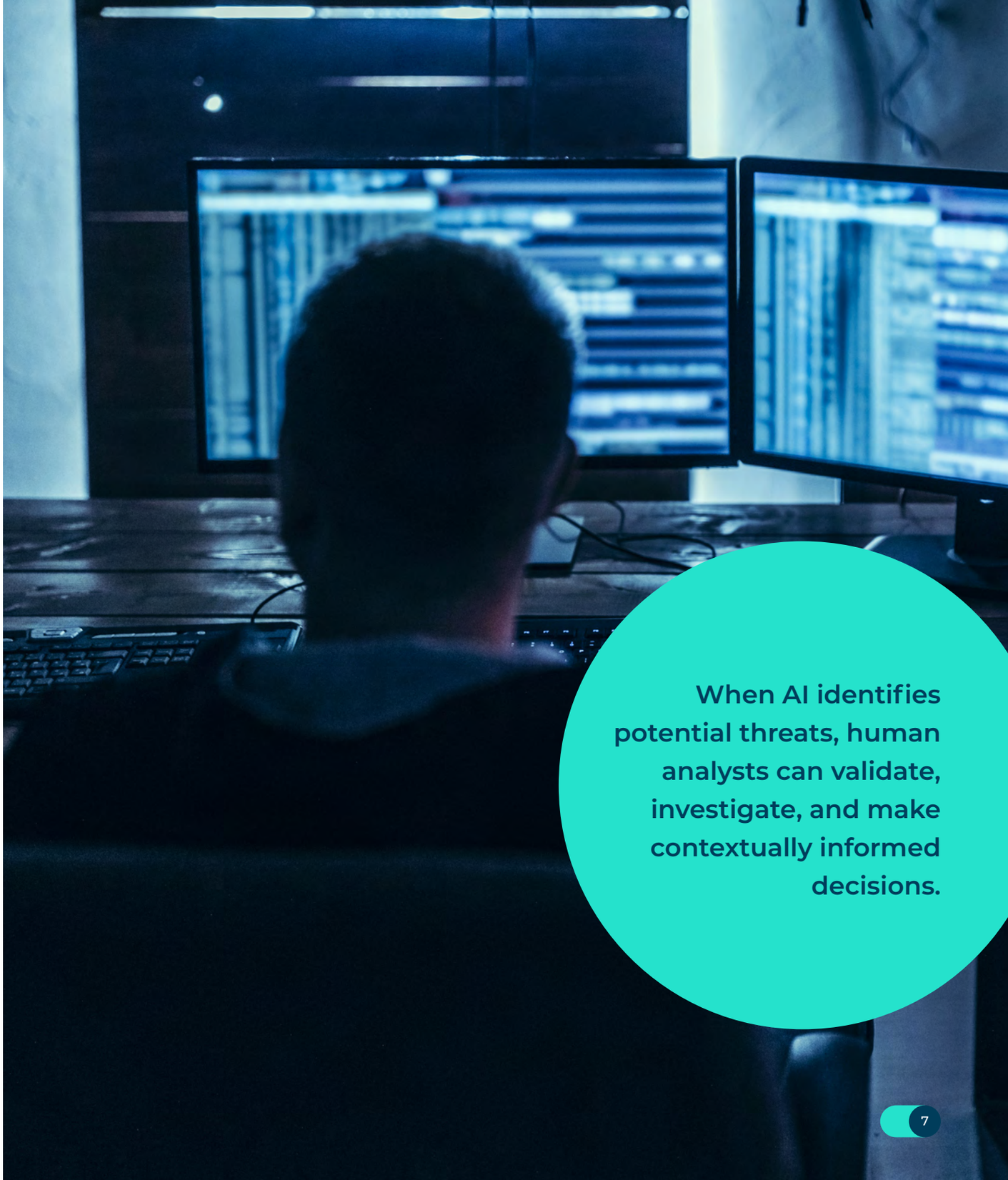
To counter these ever-shifting threats, next-generation security platforms are turning to human-driven insights to enhance AI. By tapping into crowdsourced networks composed of thousands of security practitioners worldwide, organizations can aggregate a diverse range of expertise, experiences, and perspectives. This broad intelligence base helps enrich AI models, enabling systems to adapt to emerging threats with greater speed and accuracy. Real-world observations from this network of human analysts provide invaluable feedback, bridging gaps in AI detection capabilities and fine-tuning responses to sophisticated attacks.

Crowdsourcing allows for shared threat intelligence, enabling practitioners across different sectors to learn from each other's experiences. This collaboration makes it possible to respond rapidly to emerging attack vectors and significantly improves resilience by building upon the collective knowledge of a global security community. Ultimately, this dynamic approach strengthens AI-driven defenses and ensures that adaptive systems remain relevant against evolving adversaries.

AI and Human Synergy in Real-Time Action

The combination of adaptive AI and human intelligence can effectively combat email-based threats. Leveraging adaptive AI, the system autonomously intercepts nearly 100% of malicious emails, while human analysts step in for nuanced decision-making, reinforcing the system's defenses.

By incorporating real-time human oversight, security systems achieve greater precision. When AI identifies potential threats, human analysts can validate, investigate, and make contextually informed decisions. This symbiotic relationship creates a feedback loop: human insights refine the algorithms, making them more robust over time, while AI enhances the efficiency and reach of human analysis.



When AI identifies potential threats, human analysts can validate, investigate, and make contextually informed decisions.

Looking Ahead: AI and Human Expertise in Future Cybersecurity

As cyber threats become more sophisticated with the rise of generative AI (GenAI), the need for advanced defenses has never been more pressing. Attackers are already using GenAI to generate highly targeted and convincing phishing attacks. As a result, AI defenses must stay one step ahead by learning to anticipate and respond to future attack methods.

The strategy of integrating adaptive AI with human insight represents the future of email security. By blending the efficiency of machine learning with human intuition, email security platforms offer a dynamic and adaptable defense against even the most complex cyber threats.

Next-generation solutions must evolve by incorporating predictive AI models that can anticipate new attack vectors based on emerging trends and patterns. This forward-looking approach can identify potential risks before they materialize. Equally important is the continuous engagement of human practitioners who provide ethical oversight, conduct threat hunting, and apply ethical hacking techniques to expose system vulnerabilities.

Conclusion: The Future of Cybersecurity

In an ever-evolving digital landscape, the symbiotic relationship between AI and human expertise will define the effectiveness of future cybersecurity defenses. As attackers harness AI to launch more sophisticated attacks, defenders must combine technological innovation with human intuition to stay ahead. Next generation email security platforms demonstrate how this synergy is the key to securing the digital communication channels of the future.

The path forward is clear: combining cutting-edge AI technologies with strategic human oversight is not just important—it's an absolute necessity.

About Concentrix CyberProtect

Modern Defense for Comprehensive Threat Protection

We partner with leading cybersecurity technology providers to design, build, and run next-generation security solutions. Powered by a unified AI-driven platform with advanced intelligence and automation, our solutions ensure global resilience against evolving cyber threats. Delivered as a managed service, we simplify the transition to a more advanced, easy-to-adopt service model for organizations seeking to transform and scale their security operations.

What we do:

- Modernize and transform security operations to defend against ever-evolving cyber threats.
- Leverage AI and ML to pinpoint priorities across digital ecosystems, reducing response times from days to minutes.
- Simplify and automate operations, improving process and talent efficiencies to optimize costs.

About IRONSCALES

IRONSCALES is the leader in AI-powered email security protecting over 15,000 global organizations from advanced phishing threats. As the pioneer of adaptive AI, we detect and remediate attacks like business email compromise (BEC), account takeovers (ATO), and zero-days that other solutions miss. By combining the power of AI and continuous human insights, we safeguard inboxes, unburden IT teams, and turn employees into a vital part of cyber defense across enterprises and managed service providers. IRONSCALES is headquartered in Atlanta, Georgia.

To learn more, visit **www.ironscales.com** or follow us on X **@IRONSCALES**.

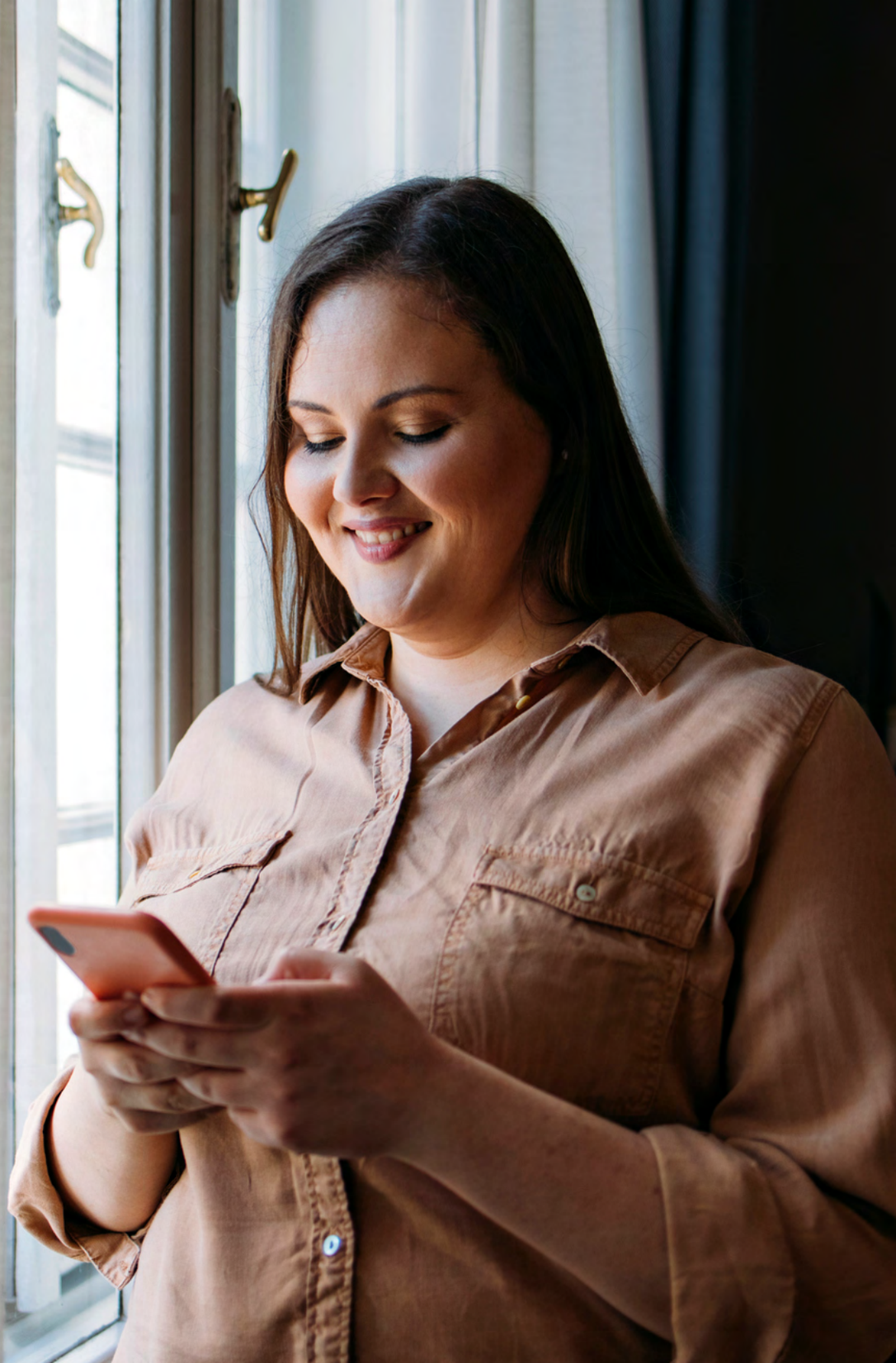
About Concentrix

Concentrix is a global technology and services leader that powers the world's best brands, today and into the future. We design, build, and run fully integrated, end-to-end solutions to support your entire enterprise, at speed and scale.

Human-centered. Tech-powered. Intelligence-fueled. Experience the power of Concentrix.

+1 800-747-0583 | concentrix.com

Learn More



© 2024 Concentrix Corporation. All rights reserved.

concentrix | IRONSCALES