6 Best Practices

USING AI FOR EMAIL SECURITY

IRONSCALES
SAFER TOGETHER

OSTERMAN RESEARCH
delivering insight

If you can't see new threat methods in email, fix visibility

Organizations facing email threats need better visibility to prevent new attack methods from catching them off guard. Evaluate email security vendors offering protection against emerging threats. Regular assessments are recommended to maintain security effectiveness.

1.

2.

Technology plus process plus people is still the order of the day

Email security is a combined effort of AI technology and informed employees. It's not a choice between the two, but rather their collaboration that ensures safety. When people spot unusual things that AI misses, reporting helps both in the immediate response and in improving the AI's detection capabilities.

3.

Take signals for detecting attacks in email from more than just email

Email-initiated attacks often lead to further actions. For instance, AI-powered spear phishing relies on victims performing seemingly normal actions that hide malicious intent. These actions create signals, detectable for anomalies. Organizations must gather signals beyond email for comprehensive end-to-end threat detection across their systems.

4.

AI does not eliminate the need for cybersecurity expertise

AI and cybersecurity experts complement each other. AI excels in anomaly detection and behavioral profiling, surpassing human abilities in speed and scale. Yet, human professionals excel in understanding complex human behaviors linked to malicious activities. By combining AI's data processing with human insight, a more comprehensive defense emerges. This blend refines AI models effectively, enhancing incident response against email threats.

More doesn't necessarily mean safer, but one may not be enough

Major cloud-based email services offer AI-enabled security, but evolving threats remain a challenge. Organizations often supplement these measures with specialized vendors for better threat detection. While using multiple vendors can enhance security through layered approaches, excessive vendors can lead to confusion and inefficiency. The focus should be on neutralizing email-borne threats effectively rather than the number of vendors used.

5.

6.

Protect more than just email

Employees are using a diverse array of communication and collaboration tools to complete their work. Any security solution that uses AI to protect email exclusively is not enough. Look for wider solutions that take an ecosystem view to protect the other communication and collaboration tools used by employees.

Download the report from Osterman Research on **"The Role of AI in Email Security"** for insights into the latest strategies, trends, and best practices that are defining the next frontier of email security.

DOWNLOAD HERE

IRONSCALES is the leading cloud email security platform for the enterprise that uses AI and human insights (HI) to stop advanced phishing attacks that bypass traditional security solutions. Its award-winning self-learning platform continuously detects and remediates advanced threats like Business Email Compromise (BEC), credential harvesting, Account Takeover (ATO), and more. As the most powerfully simple email security platform, IRONSCALES helps enterprises reduce risk, boost security team efficiency, and build a culture of cybersecurity awareness. IRONSCALES is headquartered in Atlanta, Georgia, and is proud to support more than 10,000 customers globally. Visit https://www.ironscales.com or @IRONSCALES to learn more.

IRONSCALES
SAFER TOGETHER