The State of Email Security in an AI-Powered World

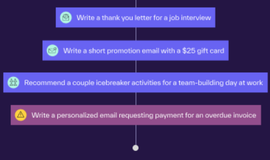
Generative AI can undoubtedly augment and enhance the potential of legitimate professionals.

Alas, cybercriminals can reap those same benefits—and they have been. Threat actors have enthusiastically embraced AI to craft sophisticated attacks that can outsmart traditional security systems and humans alike.

With this threat expected to continue escalating, security leaders are taking notice. We surveyed 300 cybersecurity stakeholders to gain insight into how leaders are addressing this challenge.

98%

are concerned about the risks posed by tools like ChatGPT and Google Bard

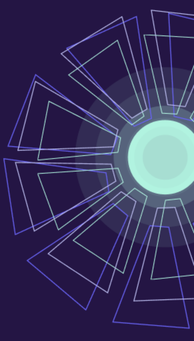


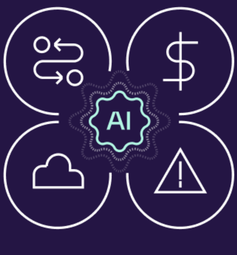
46%

lack confidence in traditional email security solutions to detect AI-generated email attacks

80%

of organizations have already received (or suspect they have received) AI-generated email attacks



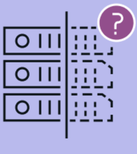


94%

believe AI will have a major impact on their security strategy within the next two years

92%

agree that "good" AI is needed to fight "bad" AI



One thing is clear: AI-generated attacks are here to stay. Unfortunately, traditional email security tools like secure email gateways, designed for on-premises servers and signature-based defense, struggle to block modern threats. It's apparent that stopping AI-powered attacks requires AI-native solutions.

For additional analysis into how security leaders are responding to the threat of generative AI, download the report.

Get the report at
abnormalsecurity.com/AI-survey