Barracuda
Your journey, secured.

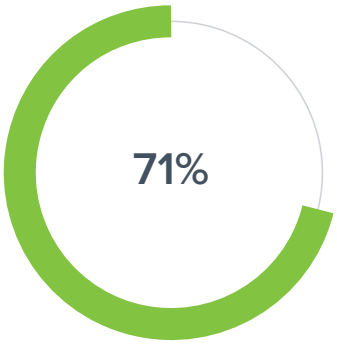
Barracuda AI-powered Email Protection for Microsoft 365

AI/ML to protect Microsoft 365 users from generative AI-based attacks.

The tech world has been buzzing with both the possibilities — and threats — that generative artificial intelligence (AI) has unlocked. With generative AI models growing and improving rapidly, there is almost unlimited potential to apply them across industries. But this great potential also comes with risk. Generative AI has fueled the scale and the sophistication of many recent attacks. However, the best defense against these newfound threats still relies on core security practices, including email protection.

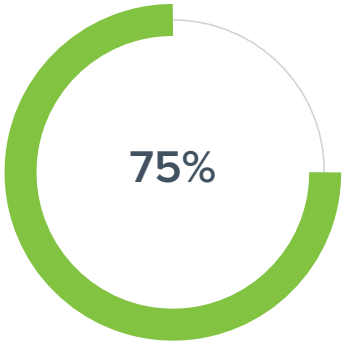
What is generative AI?

A category of AI techniques and models, generative AI generates content autonomously without direct human input, including text, image, and audio.



71% of IT decision-makers anticipate new security threats to their data from generative AI.[1]

Email as an attack vector is not new — it has only become more sophisticated and widespread. As email threats scale in numbers and technology, defenses need to stay ahead of them.



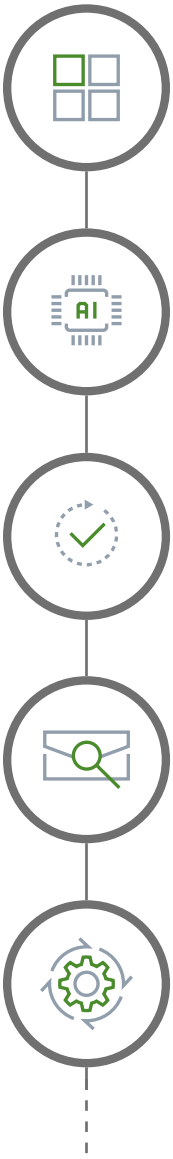
75% of organizations were hit with a successful email attack in 2022.[2]

Barracuda AI-powered email security since 2017

Barracuda has been using AI across its email security solution since 2017 to deliver comprehensive protection against all 13 types of email threats.[3] These are some of the ways Barracuda uses AI to enhance email security.

[1] *Salesforce,* Top Generative AI Statistics for 2023
[2] *Barracuda,* 2023 Emails Security Trends Report
[3] *Barracuda,* 13 Email Threat Types

Transform your email security with Barracuda AI



Microsoft 365 integration

Fast deployment with no MX records changes required, providing immediate access to a large volume of historical email data.

Sophisticated AI models

Email data is used to train Barracuda's AI models to recognize patterns and behaviors associated with different types of emails, both benign and malicious.

Real-time analysis

Barracuda AI relies on content analysis, anomaly detection, pattern recognition, and natural language processing to scrutinize all aspects of the email for malicious intent.

Threat remediation

Barracuda AI continuously monitors incoming messages for signs of threats and takes automated remediation actions to alert or delete malicious emails.

Continuous learning

Barracuda AI continually learns and adapts to new threats. As new data becomes available, its models and heuristics are automatically updated to improve detection accuracy.

AI-enabled Email Protection solutions

Barracuda Impersonation Protection

AI-powered email security against phishing, impersonation, and account takeover attacks. Fast to deploy and easy to use while delivering high detection efficacy.

Email Threat Scanner

Free AI-powered tool that 16,000 organizations already used to identify over 12 million advanced latent threats hiding inside their users' mailboxes.

Barracuda
Your journey, secured.