

# Barracuda Total Email Protection

Comprehensive security against advanced email-borne threats

Secure email gateways are no longer sufficient to defend against today's sophisticated social-engineering attacks. These attacks bypass traditional security and end up costing organizations time, money, and brand equity.

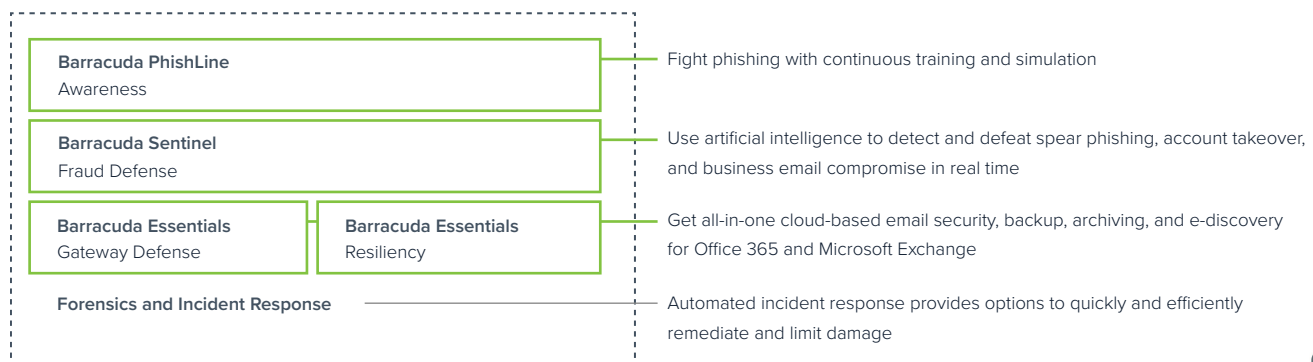
Barracuda Total Email Protection is the most effective solution to prevent targeted social-engineering attacks. Its multi-layered approach combines a secure email gateway, AI-powered fraud protection, and advanced security awareness training. This results in comprehensive protection against business email compromise, account takeover, and CEO fraud.

## Barracuda Advantage

- Complete multi-level defense that combines AI-based email security, compliance, business continuity, and user security training
- AI learns your communication patterns to detect personalized fraud in real time
- Unique API-based architecture stops threats inside your mailbox that traditional gateways cannot
- Uses vast, real-time global threat information network to optimize detection

## Product Spotlight

- API-based integration with Office 365
- Real-time AI-powered anti-phishing protection
- Brand protection using DMARC reporting and enforcement
- Tamper-proof email archiving for compliance and e-discovery
- Advanced, automated security awareness training
- Simple setup and management, with zero impact on network performance



Multi-Layered Email Protection

## 1. Protect your business from targeted email attacks

Modern attacks are rapidly growing in volume and sophistication. With 91 percent of hacks starting with a targeted email attack, you need a solution that is able to detect and prevent attacks before they cause harm.

Barracuda Essentials is a cloud-based security solution designed to protect against spam, phishing, malware, ransomware, and other targeted email threats. Essentials combines heuristic, behavioral, and sandboxing technologies to detect advanced, zero-day attacks.

## 2. Transform users from a vulnerability into a robust defensive layer

Some attacks will get by your security and land in users' inboxes. What happens next depends on how well trained and aware the targeted user is.

Barracuda PhishLine transforms users from potential attack vectors into a powerful layer of defense. Customized simulations test and train users to recognize social engineering attacks. Content is updated daily to reflect the most recent threats.

## 3. Prevent account takeover and social engineering attacks

Socially engineered spear-phishing attacks are growing fast, with total losses estimated at more than \$5 billion. These highly targeted attacks are designed to impersonate a trusted third party to trick employees into disclosing valuable information or transferring funds directly to hackers.

Barracuda Sentinel is a leading AI solution for real-time defense against socially engineered attacks, account takeover, and other cyber fraud. It uses artificial intelligence to learn each user's unique communication pattern, to identify malicious intent and flag fraud attempts.

## 4. Build resiliency and mitigate compliance risk

You need data protection that boosts resiliency, minimizes downtime, and simplifies recovery from ransomware and accidental data loss.

Barracuda Essentials ensures compliance and business continuity with advanced archiving and backup services, protecting against accidental or malicious deletion of emails and data.

## 5. Automate incident response and get access to threat insights

Many organizations struggle with slow, manual, and inefficient email security incident response processes, which often results in attacks spreading even further.

Barracuda Forensics and Incident Response automates incident response and provides remediation options to quickly and efficiently address attacks. Admins can easily send alerts, quarantine malicious emails, and use threat insights to stop the spread of malicious threats.

