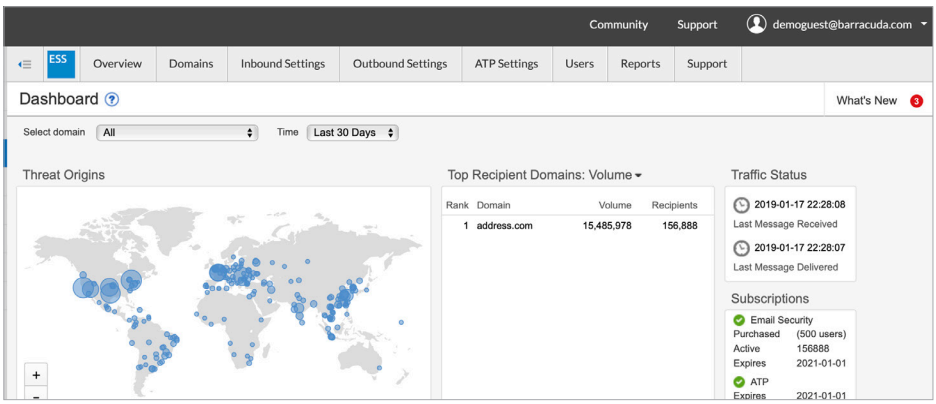
Barracuda
Total Email Protection



DETAILS

Vendor Barracuda

Price Starting at $2.63 per month, per user

Contact barracuda.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths Protects against all forms of traditional email-borne threats and includes cloud backups, security awareness training and incident response.

Weaknesses None that we found.

Verdict Total Email Protection guards on-premise and cloud-based email solutions with multi-layered email protection that can detect threats more effectively that traditional email gateways. The intuitive interface makes deployment simple and the bundled features combine to create a comprehensive email security solution.

Barracuda
Your journey, secured.

+1 877 295 5342

info@barracuda.com

Contact Sales: https://www.barracuda.com/contact/salesrep

support@barracuda.

Barracuda Total Email Protection is a multi-layered product that integrates with any SMTP service and protects on-premises and cloud email using virus scanning, spam scoring, real-time intent analysis, URL link protection, reputation checks and advanced threat detection.

This inbox defense goes beyond the traditional gateway, using AI to guard against social engineering, leveraging Office 365 APIs for unprecedented access to internal emails, offering the ability to expect rule changes, and obtaining historical information. This helps to prevent advanced, targeted attacks like account takeovers. Barracuda lays claim as the first vendor to provide a solution capable of stopping these attacks automatically and it can detect them even when an attacker is just doing reconnaissance.

Inbox defense layer's capabilities center around AI to stop targeted spearphishing attacks. Barracuda's AI collects information for a year to learn how people behave and transmit information to establish baseline behavior communication patterns. This dashboard displays an overview and allows users to filter attacks that can be exported to a CSV file. The AI is simple to use. Once it's up, it learns an environment and begins blocking emails much like a human analyst would.

Barracuda uses AI to look for suspicious sign-ons based on user history to protect against account takeovers and incorporates signals to identify unusual geographic locations. Users can create inbox rules to receive automatic alerts that can then be acted on.

Forensics and incident response show anything that's blocked and help identify targeted users. It also offers visibility into users who have interacted with malicious messages to kickstart additional training.

After an incident is created, the solution outlines step-by-step remediation. Internal cleanup removes malicious emails from users' mailboxes to prevent further takeovers. External notification mitigates reputation and brand risk by letting the parties know they received a malicious email. Block access prevents further use of the compromised account by the attack. This is all done by leveraging Office 365 APIs.

A database collects every message in an ESS Log of all emails sent and received by every account in an organization, giving administrators control of email security and a dashboard view of the organization that allows a deeper dive and more granular look into any of the setting policies.

Reports identify trends over time, highlight employees who are targeted most often, and identify impersonated senders, services impersonated, top fraud sending domains, popular fraud subjects, and types of fraud.

Pricing starts at $2.63 per month, per user. PhishLine can be purchased separately and includes voice, USB and more. Barracuda offers Standard 24/7 phone-based support as well as Premium Support (includes a dedicated Technical Account manager) and Concierge Support (for white-gloved service).

— Katelyn Dunn
Tested by Matthew McMurray