Barracuda Total Email Protection

Comprehensive security against advanced email-borne threats

Secure email gateways on their own are no longer sufficient to defend against all email threat types. Barracuda Total Email Protection is the most comprehensive protection against all email threat types, from spam and malware to business email compromise and account takeover. Its multi-layered approach combines a secure email gateway, AI-powered fraud protection, user security awareness training, and automated incident response.

Detect and block all 13 email threat types

Barracuda Total Email Protection uses advanced techniques to detect known spam and malware, while built-in Advanced Threat Protection uses payload analysis and sandboxing to discover zero-day malware. Link protection redirects suspicious and typosquatted URLs to prevent recipients from downloading malware inadvertently.

API-based inbox defense uses artificial intelligence to learn each user's unique communication pattern, identify malicious intent, and flag socially engineered fraud attempts and account-takeover attacks.

Strengthen defenses against spear phishing

Barracuda Total Email Protection employs a unique API-based architecture that lets its AI engine study historical email and learn users' unique communication patterns. It can then identify anomalies in message metadata and content, to find and block socially engineered attacks in real time.

Advanced, highly engaging security awareness training and phishing simulation engages and motivates your employees while training them to understand the latest phishing techniques, recognize subtle phishing clues, and prevent email fraud, data loss, and brand damage.

Respond to email attacks faster and more accurately

Automated incident response provides remediation options to address threats faster and more efficiently than is possible with manual response processes. Admins can quickly identify the scope of the attack and remove malicious messages directly from all impacted users' inboxes. Automatic remediation automatically identifies and removes email messages that contain malicious URLs or attachments directly from user's inboxes post-delivery.

Barracuda Total Email Protection

Barracuda Total Email Protection delivers a complete email protection platform in a single solution that is easy to buy, implement, and use. Avoid the integration chores, uncertain support, and risk that come with building your own solution using point products.

Technical Specs

Email Security (Gateway)

- Cloud-based protection against spam, malware, viruses, phishing and other email-borne threats
- Advanced Threat Protection using full-system emulation sandbox
- Agentless email encryption
- Link and typosquatting protection

Web-based management

- Managed via Barracuda Cloud Control
- Web-based management portal
- LDAP and multi-factor authentication
- Centrally managed security policies
- Reports accessible from any location
- Mobile applications

Continuity

- Failover to cloud-based email service
- Up to 96 hours of email continuity
- Emergency mailbox to send, receive, read, and respond to email

Secure Cloud Data Centers

- AES 256-bit encryption at rest and in transit
- Public key cryptography (RSA 1024)
- Isolated customer metadata databases
- Data stored in-country (based on colo)
- SAE 16 or SOC audited data centers

Cloud Archiving

- Archive directly from Office 365 to cloud-based archive
- PST management for legacy email
- Granular retention policies
- Full text search with multiple operators
- Legal hold

Cloud-to-cloud backup

- Backup and recovery for Exchange Online, SharePoint Online, OneDrive, and Teams for Business
- Centralized administration
- Custom retention policies
- Granular scheduling and restores
- Automated or manual backups
- Multi-selection restores
- Granular recovery of SharePoint items
- Restore back to Exchange Online or OneDrive for Business, or download files locally

API-base Inbox Defense

- Direct connectivity to Office 365
- Fast, easy set-up (less than 5 minutes)

AI for Real-Time Protection

- Stops spear-phishing attacks, business email compromise (BEC), extortion, and other socially engineered attacks
- Artificial Intelligence to detect and stop email attacks
- Automatic message quarantining
- Alerts to administrators and users

Account takeover protection

- Detects and alerts account takeover activity
- Notifies external users and deletes compromised email
- Blocks attackers' access to compromised account
- Provides visibility into inbox rule changes and suspicious sign-ins

Domain fraud protection

- DMARC authentication, reporting and analysis
- Intuitive wizard to help set up DMARC authentication
- Prevent domain spoofing and brand hijacking

Reporting

- Threat environment analytics
- Attacks detected over time
- Insights into impersonation and BEC attacks

Security awareness training

Multi-Vector Threat Simulation

- Email, SMS, voice, and physical media
- Real-world threat templates
- Advanced interactions: landing pages, attachments, credential forms, and more

Education

- SCORM-compliant courseware
- Microlearning videos
- Quizzes and risk assessment surveys
- Posters and infographics

Reporting and Analytics

- Collects over 16,000 data points
- Detailed trend analytics
- Customizable reports and dashboards

Incident Response

- Phish reporting button for multiple email clients
- SIEM integration

Administrative Features

- Multi-factor authentication
- Active Directory integration
- 25+ languages supported

Incident response

Identification

- Outlook Add-in and one-click threat reporting.
- Threat hunting

Investigation

- Advanced search with context and relevance
- Review users who interacted with malicious emails
- Identify high-risk users
- Automate incident response workflow

Response

- Block future emails coming from specific regions
- Delete emails directly from user inboxes
- Automatic post-delivery remediation
- Send alerts automatically to all impacted users

Barracuda
Your journey, secured.