Barracuda Email Protection

Incident Response

No email defense technology can protect against increasingly advanced email threats 100 percent of the time. Some advanced social engineering attacks like business email compromise will reach users' mailboxes. And when they do, you need to respond quickly and accurately to minimize the scope and severity of damage.

Barracuda lets you respond to threats quickly and effectively, by automating investigative workflows and enabling direct removal of malicious emails.

Automate your entire incident response process.

The timing and effectiveness of your response are critical when your organization is under attack. Barracuda automatically removes malicious emails from users' inboxes, post-delivery. Search all delivered mail, create incidents, and delete emails from user inboxes with just a few clicks. Create and enable custom response workflows to automate manual processes. Remediate threats within minutes, instead of hours or days.

Limit damage from email attacks.

Manual intervention can waste valuable time during attacks, allowing threats to spread and damage to escalate. Barracuda gives you immediate insight into users who have interacted with, forwarded, or replied to malicious messages, helping you contain threats faster. Incident Response also enhances your web security by blocking malicious links for your entire organization.

Prevent future attacks with real-time forensic analysis and community threat intelligence.

Barracuda analyzes the source of inbound messages and identifies anomalies, giving you the insight needed to prevent future attacks. It also leverages community intelligence to alert of potential threats identified by other Barracuda customers. Continuous remediation ensures your users won't be susceptible to new instances of threats you've previously remediated.

Key features and benefits

Threat hunting

Threat reporting by employees

- Outlook Add-in provides one-click threat reporting
- Enable your users to act as the strongest line of defense

Threat identification with Barracuda Insights

- Use Barracuda Insights to discover and identify threats
- Identify anomalies in delivered email.
- Get geo-IP threat insights

Locate potential incidents in Office 365 mailboxes:

- Related Threats – Threats based on an incident you already created
- Post-Delivery Threats – Based on Barracuda's (community) intelligence on currently circulating threats that might already be present in your inbox

Uncovering malicious emails and preventing attack spread

- Identify malicious emails based on geo-reporting
- Block future emails coming from specific regions

Remediation

Advanced search with context and relevance

- Search by user and incident

User behavior and compromised accounts

- Review users who clicked on malicious links or forwarded or replied to malicious emails
- Identify high-risk users that may require security awareness training

Create incidents

- Search through delivered mail and create incidents

Malicious email deletion

- Delete emails directly from user inboxes
- Remediate threats within minutes

Automation

Automatic remediation

- Automatically remove all messages that contain malicious URLs and attachments post-delivery

Automatic User Alerts

- Send alerts automatically to all users who received malicious email

Domain-based phishing protection

- Detect and automatically block access to malicious domains and URLs in phishing emails
- Seamlessly leverage APIs to share info with Barracuda Content Shield

Continuous remediation

- Delete copies of malicious emails that arrive after the initial remediation

Automated workflows

- Create and enable custom response playbooks

API integration

- Export event data to SOAR/SIEM/XDR platform

Incident Response is included as part of Barracuda Email Protection Premium and Premium Plus. Find the plan that's right for you.

CAPABILITIES	ADVANCED	PREMIUM	PREMIUM PLUS
Spam and Malware Protection	✓	✓	✓
Attachment Protection	✓	✓	✓
Link Protection	✓	✓	✓
Email Continuity	✓	✓	✓
Email Encryption	✓	✓	✓
Data Loss Prevention	✓	✓	✓
Phishing and Impersonation Protection	✓	✓	✓
Account Takeover Protection	✓	✓	✓
Automatic Remediation	✓	✓	✓
Domain Fraud Protection		✓	✓
DNS Filtering		✓	✓
Threat Hunting and Response		✓	✓
Automated Workflows		✓	✓
SIEM/SOAR/XDR Integration		✓	✓
Cloud Archiving			✓
Cloud-to-Cloud Backup			✓
Data Inspector			✓
Attack Simulation			✓
Security Awareness Training			✓

Barracuda
Your journey, secured.