Barracuda®
Your journey, secured.

Barracuda Incident Response - MSP

Email is the number one attack vector, and threats are becoming increasingly sophisticated. Advanced social engineering attacks, such as business email compromise, are designed to bypass traditional email defense technologies. Protect your customers from these attacks with automated incident response to reduce the scope and amount of damage they can cause.

Automate email attack detection and response

Using Barracuda Incident Response's automated response workflow, you can automatically remove malicious emails from customers' user inboxes, even after the email is delivered to their inbox. It searches all delivered emails, creates incidents, and deletes emails from inboxes with just a few clicks, allowing you to remediate threats within minutes, instead of hours or days.

Reduce the damage an email attack can cause

Today's sophisticated email attacks comes in many forms, some of them immediately detonate while others silently spread through your customers' network to maximize the impact of the attack, leaving you with little time to stop the attack. With Barracuda Incident Response, you gain immediate insight into customers' users who have interacted with, forwarded, or replied to malicious messages, letting you contain threats faster.

Real-time analysis and community threat intelligence

Barracuda Incident Response analyzes the source of inbound messages and identifies anomalies, giving you the insights you need to prevent future attacks. It also leverages community intelligence to alert of potential threats identified by other Barracuda customers.

Expand your managed email security service offering

Easily expand your managed email security service offering to include automated detection and remediation. Barracuda Incident Response is an easy-to-deploy, easy-to-manage solution that connects directly with Office 365 through an API-based architecture. It creates zero impact on network performance, maintaining your customers' users experience.

Gateway Defense and Resiliency	API-Based Inbox Defense	Incident Response
Cloud Backup and Archiving	AI for Social Engineering	Automation
Email Continuity	Brand Protection DMARC Reporting	Post Delivery Remediation
Encryption and DLP	Account Takeover	Threat Hunting
In/Outbound Security		

Barracuda **Total Email Protection**™

Total Email Protection

As part of the Barracuda Total Email Protection solution for MSPs, Barracuda Incident Response provides rich investigative tools and an automated approach to attack remediation.
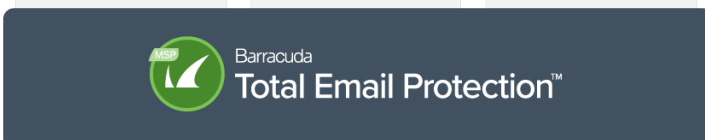
Key features and benefits

Threat hunting

Threat reporting by employees

- Outlook Add-in provides one-click threat reporting
- Enable end-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
- Locate related threats based on existing incidents

Prevent email attack spread

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

Remediation

Advanced search with content and relevance

- Search by user and incident

User behavior and compromised accounts

- Review activities associated with the malicious email
- Identify high-risk users who may need additional training

Create incidents and remediate

- Upon discovering emal threats, it creates the incident and delete the malicious emails directly from user inboxes

Automation

Automatic remediation

- Messages that contain malicious URLs and attachments are automatically removed post-delivery

Automatic user alerts

- Alerts are automatically sent to all users who received the 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

Automated workflows

- Create and enable custom response playbooks

API integration

- Export event data to SOAR/SIEM/XDR platform