Barracuda Email Protection

Compare plans

CAPABILITIES	ADVANCED	PREMIUM	PREMIUM PLUS
Spam and Malware Protection Identify and block spam, viruses, and malware delivered via email messages. Using virus scanning, spam scoring, real-time intent analysis, URL link protection, reputation checks, and other techniques, Barracuda scans email messages and files.	✓	✓	✓
Attachment Protection Barracuda combines behavioral, heuristic, and sandboxing technologies to protect against zero-hour and targeted attacks. A sandbox environment is used to detonate and observe behavior of suspicious attachments.	✓	✓	✓
Link Protection Link Protection automatically rewrites URLs so that Barracuda can sandbox the request at click time to block malicious links.	✓	✓	✓
Email Continuity In the event of a mail server outage or loss of connectivity, an emergency mailbox lets users continue to send and receive emails, staying productive until your primary servers are back online.	✓	✓	✓
Email Encryption Secures your mail by encrypting it during transport to the Barracuda Message Center, encrypting it at rest for storage in the cloud, and providing secure retrieval by your recipients through HTTPS web access. Create a policy to automatically encrypt emails based on their sender, content, and other criteria.	✓	✓	✓
Data Loss Prevention Create and enforce content policies to prevent sensitive data, including credit card numbers, Social Security numbers, HIPAA data, customer lists, and other private information, from being sent by email. Policies can automatically encrypt, quarantine, or block certain outbound emails based on their content, sender, or recipient.	✓	✓	✓
Phishing and Impersonation Protection Automatically detect and prevent impersonation, business email compromise, and other targeted attacks. Barracuda's AI engine learns each organization's unique communication patterns and leverages these patterns to identify anomalies and prevent socially engineered attacks in real time.	✓	✓	✓
Account Takeover Protection Stop phishing attacks used to harvest credentials for account takeover. AI detects anomalous email behavior and alerts IT, then finds and removes all fraud emails sent from compromised accounts.	✓	✓	✓
Automatic Remediation All user-reported messages are automatically scanned for malicious URLs or attachments. When a threat is detected, all matching emails are automatically moved from users' mailboxes into their junk folders.	✓	✓	✓
Domain Fraud Protection Prevent email domain fraud with DMARC reporting and analysis. Barracuda provides granular visibility and analysis of DMARC reports and helps you minimize false positives, protect legitimate email, and prevent spoofing.		✓	✓

CAPABILITIES	ADVANCED	PREMIUM	PREMIUM PLUS
DNS Filtering Protect users from accessing malicious web content with advanced DNS and URL filtering.		✓	✓
Threat Hunting and Response Quickly identify and efficiently remediate post-delivery threats by automating investigative workflows and enabling direct removal of malicious emails.		✓	✓
Automated Workflows Build custom playbooks to completely automate your incident response process. Admins at any technical level can create a workflow by defining a trigger, determining conditions, and assigning the desired actions through a simple user interface.		✓	✓
SIEM/SOAR/XDR Integration Orchestrate incident response cross-product with RESTful API (beta) and syslog integrations. Remotely administer and configure incident response capabilities and store your event data for tracking, analysis, and troubleshooting.		✓	✓
Cloud Archiving A cloud-based, indexed archive allows for granular retention policies, extensive search, role-based auditing/permissions, legal hold, and export. Easily comply with e-discovery requests and regulatory or policy-retention requirements.			✓
Cloud-to-Cloud Backup Get data protection and cloud backup for Office 365 data, including Exchange Online mailboxes, SharePoint Online, OneDrive for Business, and Teams. Fast point-in-time recovery in the event of accidental or malicious deletion.			✓
Data Inspector Automatically scan your OneDrive for Business and SharePoint data for sensitive information and malicious files containing malware. Use it to develop policies that comply with GDPR, CCPA, and other data privacy regulations.			✓
Attack Simulation Simulated phishing attacks are constantly updated to reflect the most recent and most common threats. Simulations are not limited to email, but also include voice, SMS, and portable-media (USB stick) attacks.			✓
Security Awareness Training Get access to advanced, automated education technology that includes simulation-based training, continuous testing, powerful reporting for administrators, and active incident-response awareness.			✓

Barracuda®
Your journey, secured.