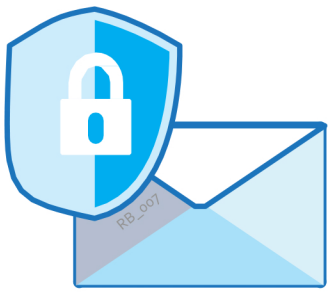
Barracuda Essentials for Office 365

Enhanced Security for Office 365 Environments

Advanced, multilayered email security

Our Barracuda Essentials for Office 365 service bundle includes Barracuda Email Security Service and Advanced Threat Detection (ATD). These give you an easy, comprehensive, and cost-effective solution to protect against a broad range of email-based threats.



Key Solution Advantages

Office 365's standard security features leave you vulnerable to phishing, zero-day exploits, and other email-borne attacks. Barracuda Essentials for Office 365 protects you against:

- Spam
- Email-borne viruses
- Email-based
- Phishing emails
- Unsecured emails
- Denial of Service (DoS) attacks

Advanced Threat Detection

Barracuda Essentials for Office 365 includes Advanced Threat Detection, a vital security layer that scans email attachments in most commonly used file formats and compares them against a cryptographic hash database.

ADT isolates and detonates files of unknown status in a sandbox environment within the Barracuda Cloud to observe their behavior. The result is pushed into the Barracuda Real Time System to provide protection for all you and other customers.

Emails found to contain malicious content are quarantined. If no malicious content is found, regular mail processing rules apply.

Real-Time Security Monitoring

- Continuous monitoring and blocking of the latest Internet threats via Barracuda Central
- Quarantines, exception lists, and blocked sender lists configurable per user or per organization

Multilayered Security Features

Virus Protection
Email and file scanning using three layers of polymorphous scanning technologies

Spam Protection
Barracuda Central-enabled screening for known spammers and malware domains

Anti-Phishing
Anti-fraud intelligence, sender spoofing detection, and domain name validation

Link Protection
Intelligent detection of malicious URLs

Typosquatting Detection
Active URL screening against fraudulent lookalikes of genuine sites

Denial of Service Attack Prevention
Protection against malware designed to cripple or disable networks

Email Spooling
Up to 96 hours of spooling to ensure email delivery in case of server or connection failures

Automated Email Encryption
Simplified key management using 256-bit AES encryption and SMTP over TLS

Outbound Filtering
Filtering against botnet spam and outbound attacks originating inside the network

Data Loss Prevention
Policy-based screening of credit card numbers. SSNs. and other sensitive content

GMGCommunications (954) 709-8345 gg@gmgcommunications1.com