



Enhanced Security for Office 365 Environments

Advanced, multilayered email security

Barracuda Essentials for Office 365 includes Barracuda Email Security Service and Advanced Threat Protection (ATP). These help give you an easy, comprehensive, and cost-effective solution to protect your SMB customers against a broad range of email-based threats.

You can use Barracuda Essentials to customize your Office 365 offering, or offer it to SMBs already using Microsoft's cloud-based productivity suite.



Multilayered Security Features

Key Solution Advantages

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

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

Advanced Threat Protection

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

Files of unknown status are detonated in a sandbox environment within the Barracuda Cloud to observe its behavior, and the result is pushed into the Barracuda Real Time System to provide protection for all other customers.

Emails found to contain malicious content are quarantined and administrators and users can be notified. If no malicious content is found, regular mail processing rules apply.

Centralized Management of Email Security

- Global visibility of all installed devices
- Centrally managed policies and configurations
- 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

Barracuda MSP provides data protection solutions for small businesses, delivered exclusively through the IT channel.

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