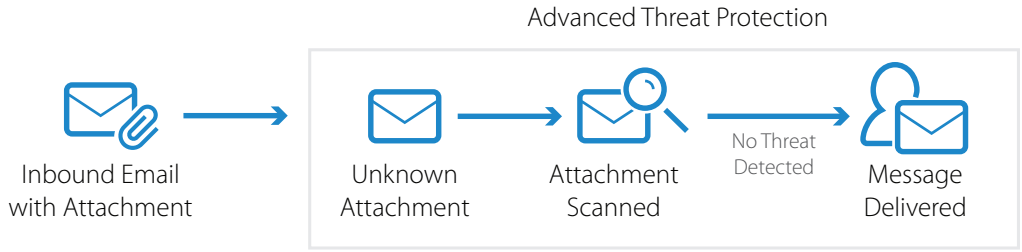
Solution Brief

Advanced Threat Protection (ATP) for Email Security Gateway

IT security threats are constantly evolving and improving, especially as attackers compete to create new ways to exploit and discover new vulnerabilities. For this reason, it simply isn't enough to depend on a single strategy or technology layer to protect your networks, data, and users. Instead, a security solution that will remain relevant and effective over time must be built on an agile, versatile platform that evolves and incorporates new scanning technology, modules, and strategies designed to detect rapidly evolving threats. Barracuda has built simple and easy-to use email security solutions that protect our customers from new and emerging threats, without having to manage the complexities of multiple products and solutions.

Barracuda Advanced Threat Protection

Continuing to execute on this strategy, Barracuda provides an Advanced Threat Protection (ATP) layer to the Barracuda Email Security Gateway (ESG). This service analyzes inbound email attachments in a separate, secured cloud environment, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Gateway virus scanning features.



To increase effectiveness and performance, Barracuda's Advanced Threat Protection uses micro-services to create a multilayered scanning infrastructure that blocks known and unknown threats.

LAYER 1	LAYER 2	LAYER 3
Connection and Intent Analysis (ESG)	Static Analysis (ESG)	Dynamic Analysis (ATP)
• Emails are filtered through multiple defense layers to verify authenticity of envelope and sender information, blocking inappropriate emails before delivery. • Real-Time Protection immediately blocks the latest spam, virus, phishing, and other malware attacks. • Managed by 24/7 security operations center that works to continuously monitor, identify, and block the latest threats.	• Machine learning server farm learns from high volume and highly diverse threat data to understand threat patterns. • Uses vector machine algorithm to deliver fast and accurate verdicts. • Taught with 50 million+ endpoints in the field ingesting good and bad files + millions of files everyday. • Catalogs previous zero-day and zero-hour threats caught by Layer 3.	• Analyzes email attachments in separate, secured cloud environment • Uses full-system emulated sandbox for remote analysis and detonation of advanced threats designed to evade detection. • Analyzes attachments and files for advanced malware, zero-hour exploits, and targeted attacks not detected by Layers 1 or 2. • Scans 900+ artifact attributes in less than one second.
Captures 3% of Email Threats	Captures 96% of Email Threats	Captures 1% of Email Threats

Barracuda Cloud Protection Layer

Barracuda Advanced Threat Protection is delivered as part of the Cloud Protection Layer (CPL) feature of the Barracuda Email Security Gateway. CPL blocks threats before they reach your network, prevents phishing and zero day attacks, and provides email continuity. Once email passes through the Cloud Protection Layer, the Barracuda Email Security Gateway filters email via more granular policies, further recipient verification, quarantining, and other features you configure on the appliance or virtual machine.

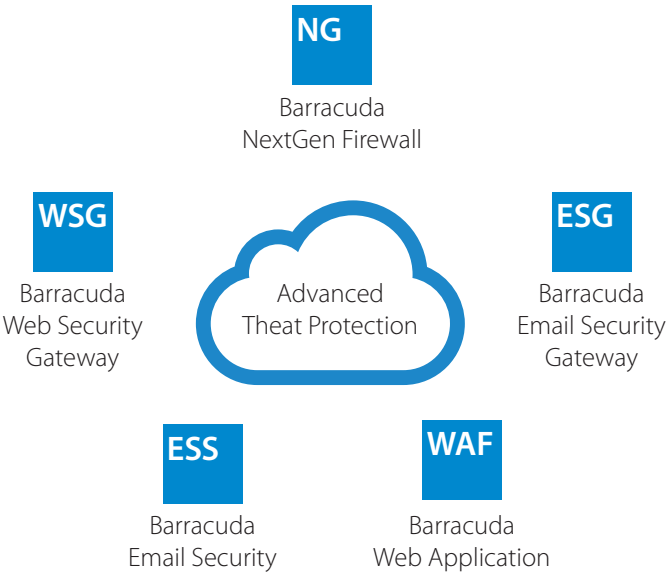
The Cloud Protection Layer receives inbound email on behalf of the organization, insulating your organization's mail server from receiving direct connections and associated threats. In addition to Advanced Threat Protection, here are some of the benefits of using the Cloud Protection Layer together with your Barracuda Email Security Gateway:

- **Link Protection** – Rewrites a deceptive URL in an email message to a safe Barracuda URL, and delivers that message to the user.
- **Typo-squatting Protection** – Checks for common typos in the URL domain name in an email message and, if found, rewrites the URL to the correct domain name so that the user visits the intended website.
- **End User Security Training** - Users that click on malicious links are taken to a landing page where they can take training exercises to understand what they did wrong and how to avoid repeating this mistake moving forward.
- **Email Burst Handling** – Email surge suppression during peak traffic and spam spikes, which offloads a significant volume of spam email from your Barracuda Email Security Gateway to be filtered via the cloud.
- **Immediate Response** – Automatic updates in real time, leveraging threat intelligence from Barracuda Labs and Barracuda Central to continuously stay ahead of quickly morphing threats.

Summary

Barracuda Advanced Threat Protection provides comprehensive real-time protection against all known and unknown advanced threats. The service shares threat intelligence across all Barracuda security products ensuring that customers' networks, users, data, and web applications are dynamically protected from the rapidly evolving threat landscape.

For example, an email borne, zero-hour threat is detected and immediately neutralized by Barracuda Advanced Threat Protection running on Essentials for Office 365. With the threat now known, Barracuda Advanced Threat Protection distributes the signature across all deployed Barracuda devices around the world. Should the same threat then show up in a file downloaded from a website, then a Barracuda NextGen Firewall or Web Security Gateway will already know about the threat and block the download.



Barracuda is the only company to integrate this level of threat intelligence and protection across an entire portfolio of security products. Whether using one or multiple products, customers benefit from the collective volume and diversity Barracuda's global threat intelligence network.