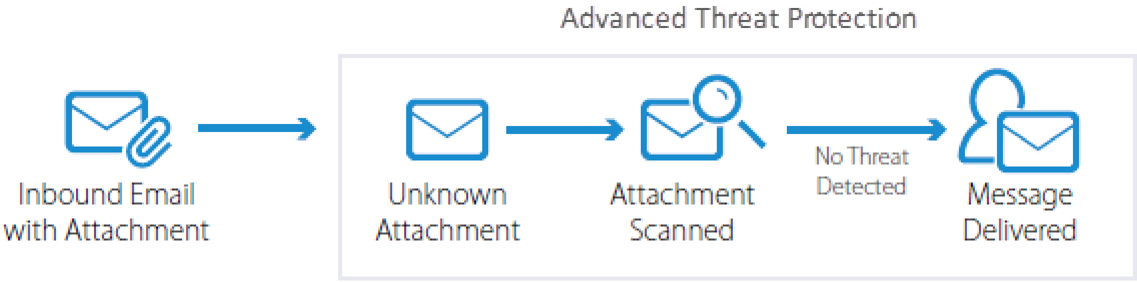
Advanced Threat Protection

https://campus.barracuda.com/doc/54264986/

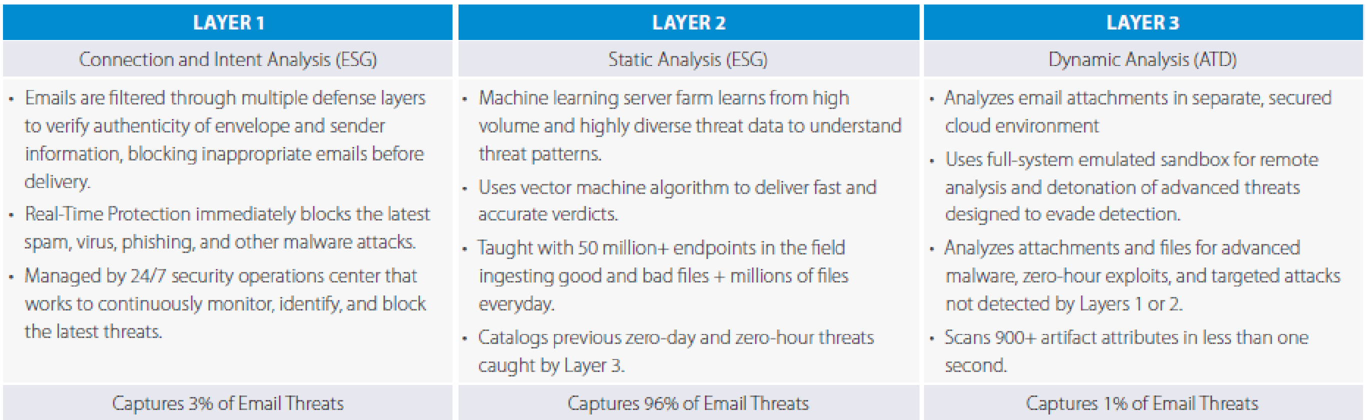
Advanced Threat Protection (ATP) offers cloud-based protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Gateway virus scanning features.The Barracuda Email Security Gateway provides access to the Barracuda Cloud Protection Layer (CPL) with an active ATP subscription. For information about setting up the Cloud Protection Layer, see Cloud Protection Layer and How to Set Up Your Cloud Protection Layer.

ATP analyzes inbound email attachments with most MIME types and publicly accessible direct download links in a separate, secured cloud sandbox, 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.



When ATP determines an attachment contains a threat and blocks the message, review the ATP Report before determining whether to deliver the message. See How to Use Advanced Threat Protection Reports for more information.

To increase effectiveness and performance, Barracuda’s ATP 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 (ATD)
• 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

ATP Options

In CPL, configure how and when attachments are scanned on the **ATP SETTINGS** tab:

- **Deliver First, Then Scan** – When selected, the ATP service attempts to scan the mail in real time. If the ATP scan completes in real time and a virus is detected, the message is blocked and is not delivered. If the ATP scan does not complete in real time, the message is delivered; if the ATP service determines the attachment to be suspicious or virus-infected upon completion, the recipient is notified, and if **Notify Admin** is set to **Yes**, an email alert is sent to the specified admin address.

  > This option does not delay email processing, however, the email recipient can potentially open an infected attachment.

- **Scan First, Then Deliver** – When selected, the ATP service scans messages with attachments before delivery. If a virus is detected in an attachment, the message is blocked, otherwise, the message is delivered to the recipient.

  > This option provides more security and prevents the email recipient from opening infected attachments. Note that messages with attachments may be temporarily deferred while queued for scanning. These messages appear in the Message log and **Pending Scan** displays in the **Reason** column. The mail server retries until the scan is complete and no virus is detected in the attachment, at which point the message is delivered.

- **No** – When selected, ATP is disabled.

ATP Exemptions

When ATP is set to either **Deliver First, then Scan** or **Scan First, then Deliver**, you can exempt sender email addresses, sender domains, recipient email addresses, recipient domains, or sender IP addresses from ATP scanning in the **ATP Exemptions** section on the **ATP SETTINGS** tab of CPL.

> Attachments from exempted entries are not sent to the ATP cloud. Note that these exemptions apply to *ATP scanning only* and do not apply to Barracuda Email Security Gateway virus scanning.

Scanned File Types

Table 1 lists example file types scanned by the ATP service.

Table 1.

MIME Type	File Extension
application/pdf	**.pdf**
application/msword	**.doc**
application/vnd.ms-powerpoint	**.ppt**
application/vnd.ms-excel	**.xls**
application/x-msaccess	**.mdb**
application/vnd.openxmlformats-officedocument.presentationml.presentation	**.pptx**
application/x-dosexec	**.exe**
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	**.xlsx**
application/vnd.microsoft.portable-executable	**.exe**
application/x-executable	**.exe**
application/vnd.ms-cab-compressed	**.cab**
text/x-msdos-batch	**.bat**
application/rtf	**.rtf**
application/vnd.android.package-archive	**.apk**
application/zip	**.zip**
application/x-tar	**.tar**
application/java-archive	**.jar**
application/javascript	**.js**
application/vnd.openxmlformats-officedocument.wordprocessingml.document	**.docx**

Administrator Notification

When **Deliver First, Then Scan** is selected, select **Yes** for **Notify Admin** to notify the administrator when a virus is detected by the ATP service in a scanned attachment. The email notification includes the sender, recipient, attachment type, and detected virus. Enter the admin email address in the **ATP Notification Email** field address. Infected attachments are listed in the **ATP Log**.

User Notification

If the ATP service determines an attachment is suspicious or virus-infected, the recipient is notified, and the Message Log displays the action as **Advanced Threat Protection**. Additionally, the Message Log displays:

Envelop From: no-reply@barracudanetworks.com

ATP Exemptions

When ATP is set to either **Deliver First, then Scan** or **Scan First, then Deliver**, you can exempt sender email addresses, sender domains, recipient email addresses, recipient domains, or sender IP addresses from ATP scanning. Attachments from exempted entries are not sent to the ATP cloud. Note that these exemptions apply to *ATP scanning only* and do not apply to Barracuda Email Security Gateway virus scanning.

Message Log

Messages blocked or deferred by the ATP service are listed in the CPL **Message Log** with the following codes listed in the **Reason** column:

- **Advanced Threat Protection** – Message is blocked by the ATP service due to an infected attachment.
- **Pending Scan** (**Scan First, Then Deliver** enabled) **–** Message is deferred while the attachment is scanned. The mail server retries until the scan is complete. Once complete, if no virus is detected, the message is delivered.
- **ATP Service Unavailable** – Message is deferred because the ATP service is temporarily unavailable. The message is retried and, when the scan is complete and if no virus is detected, the message is delivered.

View ATP Statistics

The **DASHBOARD** page in CPL displays statistics of scanned attachments determined to be infected by the ATP service.

Figures