

Overview

<https://campus.barracuda.com/doc/87196656/>

Take a look at the new [Barracuda Email Protection plans](#).

Barracuda Total Email Protection combines Barracuda Networks' complete email protection portfolio in a single bundle that is easy to buy, implement, and use.

Barracuda Networks offers additional bundles, described in this table:

	Total Email Protection	Total Email Security	Essentials Complete	Essentials Compliance	Essentials Security
Barracuda Email Security Service	✓	✓	✓	✓	✓
Barracuda Cloud Archiving Service	✓		✓	✓	
Barracuda Cloud-to-Cloud Backup	✓		✓		
Barracuda Forensics & Incident Response	✓				
Barracuda PhishLine	✓				
Barracuda Sentinel	✓	✓			

Be sure to read about [License Definitions](#) for the Barracuda Email Protection portfolio.

The following Barracuda Networks solutions are included in Barracuda Total Email Protection and other bundles. Follow the links for documentation and activation information for each of the solutions.

Barracuda Essentials

[Barracuda Essentials](#) provides the most complete, simple, and affordable solution for protecting business emails and data in Office 365, Microsoft Exchange, and Google Workspace. It combines our award-winning email security, as well as a tamper-proof email archive to ensure compliance and simplify litigation searches. For Office 365, Barracuda Networks also offers full cloud-to-cloud backup and recovery of all your emails and files.

The three components of Barracuda Essentials include:

- **Barracuda Email Security Service** – Security service protecting both inbound and outbound email against the latest spam, viruses, worms, phishing and denial of service attacks.
- **Barracuda Cloud Archiving Service** – Journal mail directly from Office 365 to the Barracuda Cloud to optimize email storage, meet regulatory compliance and e-discovery requirements, and provide anytime/anywhere access to old emails.
- **Barracuda Cloud-to-Cloud Backup** – Protects Exchange Online, OneDrive for Business, and SharePoint Online data by backing it up directly to Barracuda Cloud Storage.

Learn how to [activate Barracuda Essentials](#).

Learn how to [activate Barracuda Cloud Archiving Service](#) as a standalone product.

Learn how to [activate Barracuda Cloud-to-Cloud Backup](#) as a standalone product.

If purchased as part of a bundle, Barracuda Cloud Archiving Service and Barracuda Cloud-to-Cloud Backup are activated with Barracuda Essentials above.

Barracuda Forensics & Incident Response

[Barracuda Forensics & Incident Response](#) enables your IT team to identify, track, and resolve email attacks like phishing or ransomware which originate outside your organization. Search by subject and/or sender for any allowed email reported as malicious and take immediate action. Remediation options include blocking a sender or a sender's domain in Email Gateway Defense, deleting messages from a user's inbox, and sending an incident summary to the user. If a user clicks on a fraudulent email link, Barracuda Forensics & Incident Response helps you identify these user accounts as potential security concerns and determine what actions to take.

Learn how to [activate Barracuda Forensics & Incident Response](#).

Barracuda PhishLine

[Barracuda PhishLine](#) uses advanced training and simulation to both measure your vulnerability to phishing emails and to teach users how to avoid becoming victims of data theft, malware, and ransomware. Your users need to be trained to easily recognize malicious emails, especially as hackers become more sophisticated and prevalent.

Here are just a few of the things you can do with Barracuda PhishLine to thwart social engineering attacks:

- Create your own training campaigns, working with hundreds of included email lure templates, landing pages, and domains.
- Simulate social engineering attacks across four vectors: email, voice, SMS, and portable media
- Customize the templates to personalize them for your organization.
- Create a phish reporting button your users can use to report possible threats.
- Analyze results with advanced metrics and reporting.

Learn how to [activate Barracuda PhishLine](#).

Barracuda Sentinel

[Barracuda Sentinel](#) is a comprehensive artificial intelligence (AI) solution for real-time spear phishing and cyber fraud defense. It is delivered as a cloud service. Barracuda Sentinel utilizes artificial intelligence to protect people, businesses, and brands from spear phishing, impersonation attempts, business email compromise (BEC), and cyber fraud.

The three main components of Barracuda Sentinel include:

- A multi-layer AI engine that detects and blocks spear phishing attacks in real time and identifies which employees are at highest risk of spear phishing
- Domain Fraud Protection that delivers visibility and analysis of DMARC reports, which prevent phishing and brand hijacking and ensure deliverability of legitimate email traffic
- Ability to detect account takeover attempts and block email attacks launched from compromised accounts.

Learn how to [activate Barracuda Sentinel](#).

Figures

1. checkmarkIcon.png
2. checkmarkIcon.png
3. checkmarkIcon.png
4. checkmarkIcon.png
5. checkmarkIcon.png
6. checkmarkIcon.png
7. checkmarkIcon.png
8. checkmarkIcon.png
9. checkmarkIcon.png
10. checkmarkIcon.png
11. checkmarkIcon.png
12. checkmarkIcon.png
13. checkmarkIcon.png
14. checkmarkIcon.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.