Barracuda CARES Act and ARPA Product Justification Document

Barracuda Products can provide complete protection for remote workers or learners. The CARES Act definition is broad so other Barracuda products might also quality. Customers are responsible for applying for this funding, but this document can help them justify buying Barracuda products under the US CARES Act.

Total Email Protection

Barracuda Total Email Protection combines Barracuda's complete email protection portfolio + O365 Backup and Cloud Archiving in a single bundle that is easy to buy, implement, and use.

Bundle description: https://www.barracuda.com/products/essentials/editions

Total Email Protection	Includes Barracuda Essentials, PhishLine, Sentinel, Forensics, Cloud Archiving and Cloud-to-Cloud Backup (see product features listed below)

Barracuda Total Email Protection in relation to COVID-19 response and planning:

Barracuda Total Email Protection (TEP) is an integrated bundle of everything needed to protect your organization from email malware attacks with multiple, integrated layers of security. This is more important than ever as malware attacks have increased due to the pandemic as attackers take advantage of the disruption caused by the pandemic.

TEP includes Barracuda Essentials, Sentinel, PhishLine and Forensics and Incident Response for integrated, multilayered security.

- Barracuda Essentials and Sentinel protect from internal and external email attacks.
- PhishLine trains people to be an added line of defense – even with remote personal accounts.
- Forensics and Incident Response can track down and shut down attacks in minutes and minimize damage

- Cloud-to-Cloud Backup offers SaaS based backup for Microsoft Office 365 Exchange Online, SharePoint, OneDrive for Business and Teams.

Essentials

Barracuda Essentials quickly filters and sanitizes every email before it is delivered to your mail server to protect you from email-borne threats.

Essentials	• Stops spam and malware with inbound mail filtering • Outbound filtering stops attacks originating from inside your network • Includes Barracuda Advanced Threat Protection, a cloud-based service that defends against malware/ransomware • Data loss protection and email encryption keeps sensitive data from leaving your organization • Content policies can automatically encrypt, quarantine, or even block certain outbound emails based on their content, sender, or recipient • Cloud-based Email Archiving with search and e-discovery for compliance (included with Essentials Compliance, Essentials Complete, Total Email Protection bundles) • Cloud-to-Cloud Backup (included with Essentials Complete) to back up your Office 365 environment

Barracuda Essentials in relation to COVID-19 response and planning:

Employees, especially when distracted, are more susceptible to accidently sending sensitive information to the wrong people. Setting up appropriate outbound filtering, data loss prevention and encryption policies will protect them from such errors. Barracuda Essentials will keep sensitive data from leaving your organization, while content policies can automatically encrypt, quarantine or even block certain outbound emails based on their content, sender, or recipient.

Cloud-to-Cloud Backup

Barracuda Cloud-to-Cloud Backup offers SaaS based backup for Microsoft Office 365 Exchange Online, SharePoint, OneDrive for Business and Teams.

Cloud-to-Cloud Backup	• Unlimited storage and retention for Exchange Online, SharePoint, OneDrive for Business, Teams, and Groups data • Find and recover files, folders, and mailboxes and restore to the same account/location or to a different account/location • Granular restore for Email, SharePoint, and OneDrive • Protects against accidental data deletion or overwrite • Ability to restore after corruption, malware, or ransomware • 5 minutes from signup to running your first backup

Cloud-to-Cloud backup in relation to COVID-19 response and planning:

Now that more of your users are remote, there is potential risks in how they save their data. It is important that your IT team plan these changes and review them with your uses. People who would normally save to a network drive on a file server will now either need to be connected via VPN or be using something like Microsoft OneDrive for Business.

If you are using Office 365 you should be following Microsoft best practices by backing up with Barracuda Cloud-to-Cloud Backup, so that your IT team can ensure that business data can be protected according to new organizational policies.

Barracuda Cloud-to-Cloud Backup seamlessly protects Office 365 data. Every email, OneDrive file and SharePoint document is backed up with no storage or retention limits. IT can easily recover data lost due to malware, ransomware, or deletion — whether accidental or malicious.

- Largest cause of data loss is accidental deletion of data by users
- Working remote there is no way to access or recover the data if it hasn't been backed up to a central location

- New cyber-threats are targeting users during this crisis
    - Independent copy of data is stored to another location
    - Granular restore of SharePoint and OneDrive
    - Ability to restore data lost due to corruption, malware attack or deletion

Your users are accessing and saving data from a variety of platforms and applications, which increases the risk of accidental deletion and falling victim to cyber-attacks. Centralized remote management is critical in this environment of distributed data.

- CCB provides a browser-based management console to manage data access, retention policies, backups, and restores.
    - Optimize security with granular, role-based access controls
    - Cross-restore data to other users, mailboxes, folders or sites

Cloud Archiving

Barracuda Cloud Archiving Service provides a completely cloud-based SaaS solution for email archiving and compliance.

Cloud Archiving	• Reduce email storage requirements • Boost user productivity with mobile or desktop access to any email ever sent or received • Granular retention policies • Set up in less than an hour • Unlimited storage per user • Search and e-discovery for compliance • Retention and Litigation Hold • Export of Archived Data

Cloud Archiving in relation to COVID-19 response and planning:

The rapid migration to remote work has increased the strain on IT resources, making it difficult to allocate time for compliance audits and eDiscovery.

- Barracuda Cloud Archiving Service's indexed archive provides iterative, multi-level search and tagging capabilities to support complex audit and discovery exercises. This drastically cuts the time and effort required to respond to discovery requests, freeing up IT resources to focus on more strategic initiatives.

As users adapt to working from home, they face increased distractions which can lead to accidental email and file deletion.

- With Barracuda Cloud Archiving Service, data is archived outside your operational email environment in a dedicated tamper-proof repository, ensuring it will be retained securely for as long as your need it without risk of corruption or deletion.
- "Ensure that measures taken extend beyond pure IT security and include a focus on compliance and cyber-physical systems where necessary". – Gartner, *"Be Resilient: Prepare to Treat Cyber Risk Following the Coronavirus (COVID-19) Outbreak by Focusing on These 7 Areas"*
- Barracuda Cloud Archiving Service provides everything an organization needs to comply with government regulations, including tools to assist with litigation support, storage and knowledge management and regulatory compliance.

Forensics and Incident Response

Barracuda Forensics and Incident Response (FIR) reduces the cost and impact of email attacks by responding to attacks and stopping the damage in minutes.

Forensics and Incident Response	• Report suspicious messages • Real-time reporting and forensics • Identify users who interacted with suspicious email • Automated incident response • Send alerts to users • Remove email from users' inboxes

Forensics and Incident Response in relation to COVID-19 response and planning:

- 1 in 7 senior decision makers said their organization has already experienced at least one cyberattack since the start of the COVID-19 pandemic, according to a new report by Alliant Cybersecurity.
- Furthermore, more than one in five (22%) said their organization transitioned to remote work without having a clear policy to mitigate or prevent cybersecurity

threats, the report said. Additionally, 17% said their organization is at an increased risk for a cyberattack and 12% said they would not know how to respond to one.

  - Barracuda Forensics and Incident Response automates these processes to ensure that IT can quickly identify the nature and scope of the attack, immediately eliminate malicious emails, and carry out remediation actions rapidly to halt the attack’s progress and minimize damages.

- 80% of organizations report taking over 6 hours to respond to email attacks. During that time, threats are free to spread throughout the network, causing mounting damage and increasing costs.
  - FIR offers your IT team the ability to identify, track, and resolve email attacks that originate outside your organization, such as a phishing or ransomware attack. This is done in a matter of minutes rather than hours
  - This action can be performed from a remote setting in your admins interface, further supporting work at home endeavors
  - Slow, inefficient manual incident response processes can allow the COVID-19 email attacks to spread further. With FIR, IT can do proactive threat hunting and use intelligence to block future emails from malicious actors, and identify the most vulnerable remote users.

PhishLine

Barracuda PhishLine is a complete training system to teach people to recognize and respond to security risks.

PhishLine	• Realistic email phishing campaigns with customizable email lure templates, domains and landing pages • Patented multi-vector campaigns that include email, SMS, voicemail and USB media • Vast library of educational content • Risk-based surveys • Phish reporting plug-in • Incident response dashboards • Full report writer with over 16,000 data points

PhishLine in relation to COVID-19 response and planning:

PhishLine leverages that extensive threat intelligence to create real-world simulation and training content aligned with all identified 13 email threat types. Users will learn to spot Business Email Compromise, Impersonation attacks and other top email threats.

With PhishLine, administrators can simulate multi-vector phishing attacks through email, text (smishing) and voice (vishing). PhishLine captures thousands of data points to give your organization deeper and more useful insights into exactly where risks exist so you can precisely target your awareness programs.

- "Communicate key security awareness messages to ensure the organization's workforce remains vigilant and alert to phishing and other socially engineered cyberattacks that could compromise operational continuity, data security and privacy when working remotely." -Gartner, "Be Resilient: Prepare to Treat Cyber Risk Following the Coronavirus (COVID-19) Outbreak by Focusing on These 7 Areas"
    - PhishLine enables organizations to launch continuous phishing simulation and training campaigns for their users with training videos ranging from a wide range of topics, including how to spot social engineering attacks and how to safely work from home.
- In a single 24-hour period, Microsoft detected a massive phishing campaign using 2,300 different web pages attached to messages and disguised as COVID-19 financial compensation information that actually lead to a fake Office 365 sign-in page to capture credentials
    - PhishLine's "Real World" threat simulation content category replicates actual spear phishing attacks captured by Barracuda email protection solutions. This allows organizations to expose their users to the latest attack techniques (including those related to COVID-19) in a safe environment, to identify phishing risks, target training campaigns and lets users practice secure email behavior.
- "Provide clear guidance on who to contact and the information they need to collect should they
  experience a suspected compromise. Make sure any communications also provide locations to any security awareness training relating to phishing, smishing, other socially engineered forms of cyberattacks…" – *Gartner, "Be Resilient"*

- PhishLine comes with Phish Report button that plugs directly into outlook. This enables your users to report suspicious emails with the click of a button, right from within their email client.

Sentinel

Barracuda Sentinel detects threats that traditional email security systems can't. It integrates directly with Microsoft Office 365 APIs to detect attacks coming from both internal and external sources.

Sentinel	• AI based email protection • Spear phishing prevention • Account takeover protection • Prevent BEC and CEO fraud • Real-Time remediation • DMARC reporting and visualization • Quick and Easy setup • Works with any email gateway • Flexible API-based deployment

Sentinel in relation to COVID-19 response and planning:

Many remote users are facing a variety of distractions during this crisis. This time of distraction creates a perfect storm for email scammers to attack.

There are several active COVID-19 scams that involve ransomware, phishing, and other types of attacks. The success of these attacks is based on the victim believing that the email is a legitimate status update from the company or from world health care leaders.

- Spear Phishing attacks are increasing exponentially since the start of the COVID-19 outbreak. About 32% of breaches involve phishing, and many phishing attacks include malicious links to fake websites, trending now with COVID related messages or impersonations from credible sources such as the CDC. About 4% of recipients in any given phishing campaign click on the malicious link.

    - Barracuda Sentinel has advanced API-based protection that is effective in detecting such attacks coming from both internal and external sources. It uses artificial intelligence to detect signs of malicious intent and deception with every email and does not require IT administration.

- Reported losses in 2019 due to phishing reached almost $58 million. While only 57% of organizations have URL protection in place, according to a recent survey.
    - With Sentinel, the API can enable a historical, internal view of actual URLs used by an organization. Abnormal or impersonating URLs, which signal phishing attacks, can be blocked.

- With email scamming, cybercriminals use fraudulent schemes to defraud victims or steal their identity by tricking them into disclosing personal information
    - A recent phishing campaign disguised as COVID-19 financial compensation led recipients to a fake O365 login page, allowing hackers to capture their credentials
    - Scamming accounts for 39% of all spear-phishing attacks. The FBI has recorded millions of dollars in reported losses as a result of these scams
    - Barracuda Sentinel API-based inbox defense against scamming uses historical email communications to determine what normal email communications look like for each employee. When criminals send scamming emails to their victims that fall outside of normal and expected communication, it’s flagged and removed by inbox defense

- Spear phishing is a highly personalized form of email phishing attack. Cybercriminals research their targets and craft carefully designed messages. Attackers are impersonating established entities like the World Health Organization (WHO), Centers for Disease Control and Prevention (CDC), and the Department of Health to get into inboxes.
    - Impacts of these attacks include malware infection of end points and network, direct monetary losses through wire transfers, and reputational damage. In many cases, spear-phishing attacks lead to the theft of credentials and email account takeover.
    - API-based inbox defense uses access to historical email communication data to build a communication identity graph, a statistical model that is specific to each user in the organization. This identity graph is then used to detect unusual communication patterns that fall outside of its statistical model, which in turn predicts and blocks spear-phishing attacks that make it past the gateway.

- Attackers attempt to impersonate a domain by using techniques such as typo-squatting, replacing one or more letters in a legitimate email domain with a similar letter or adding a hard-to-notice letter to the legitimate email domain. In preparation for the attack, cybercriminals register or buy the impersonating domain.
    - Barracuda researchers have seen a sharp rise in domain-impersonation attacks used to facilitate conversation hijacking. An analysis of about 500,000 monthly email attacks shows a 400% increase in domain-impersonation attacks used for conversation hijacking
    - An API-based inbox defense uses past email communications to get data on domains used by the organization, their partners, and customers. Inbox defense associates specific conversations, requests, and individuals with specific email domains. So, when a vendor sends an unusual request from the wrong domain, inbox defense detects and blocks it.

- In BEC attacks, scammers impersonate an employee in the organization in order to defraud the company, its employees, customers, or partners. In most cases, attackers focus their efforts on employees with access to the company's finances or personal information, tricking individuals into performing wire transfers or disclosing sensitive information. These attacks use social-engineering tactics and compromised accounts, and they often include no attachments or links
    - Working from home leaves your company more vulnerable as you are unable to walk over to an individual and confirm if they sent an email
    - In your ETS scan results we discovered x impersonated senders within your organization.
    - BEC makes up only 7% of spear-phishing attacks, it caused more than $1.7 billion in losses in 2019 alone, according to the FBI. Gmail accounts are used to launch 47 percent of business email compromise attacks.
        - Payroll scams account for 8% of BEC attacks, but they are on the rise, growing more than 800% recently.
    - API-based inbox defense is a more effective protection against BEC attacks
- Conversation hijacking, cybercriminals insert themselves into existing business conversations or initiate new conversations based on information they've gathered from compromised email accounts to steal money or personal information.
    - In one well-publicized case, the Shark Tank's Barbara Corcoran lost nearly $400,000 due to a phishing scam. Scammers tricked her bookkeeper using email-domain impersonation, sending a bill that appeared to come from her assistant. But Corcoran's assistant never sent the invoice; the fake bill came from an email that closely resembled her address. By the time

Commented [AH1]: Recommend running ETS scan. If the customer does not run the scan, please remove this.

    Corcoran’s team realized something was wrong, the money had already been transferred to the scammers.
    - Your ETS scan results have shown that your team may have already fell victim to one of these attacks which could have gone unnoticed on DATE. A message was received from A. Arnold with a sender domain aanorldlaw.com that appears to be impersonating the domain anorldlaw.com

Commented [AH2]: Use an actual ETS example here. Name used here is just an example.

    - With Sentinel when an email conversation is hijacked and a trusted partner is impersonated by cybercriminals, inbox defense blocks the attack.
- With lateral phishing, attackers use recently hijacked accounts to send phishing emails to unsuspecting recipients, such as close contacts in the company and partners at external organizations, to spread the attack more broadly. Because these attacks come from a legitimate email account and appear to be from a trusted colleague or partner, they tend to have a high success rate.
    - In a recent study, researchers found that 1 in 7 organizations has experienced a lateral phishing attack. More than 55% of these attacks target recipients with some work or personal connection to the hijacked account
        - Gateways can’t remediate attacks post-delivery, either. Once email is delivered to the inbox, it stays there. APIs for inbox defense provide visibility into internal communications. They can detect internal threats, such as lateral phishing, and remediate them post-delivery
- A recent analysis of account-takeover attacks found that 29% of organizations had their Microsoft Office 365 accounts compromised by hackers in one month. More than 1.5 million malicious and spam emails were sent from the hacked Office 365 accounts in that 30-day period.
    - An API-based inbox defense connects directly with users’ inboxes, monitoring for suspicious changes to inbox rules, unusual login activity, and malicious messages sent from already-compromised accounts. Inbox defense detects account takeover before it’s used to conduct fraud and remediates an attack by locking malicious users out of the compromised account
- Spear Phishing attacks are increasing exponentially since the start of the COVID-19 outbreak. All these attacks are ones we have seen in the past, they are simply finding a new way in through workers fear of COVID and need for information surrounding it.
    - Remote working brings new security risks and productivity challenges. Cybercriminals can take advantage of distracted employee email behavior.

- Barracuda Sentinel has advanced API-based protection that is effective in detecting such attacks coming from both internal and external sources. It uses artificial intelligence to detect signs of malicious intent and deception with every email and does not require IT administration.