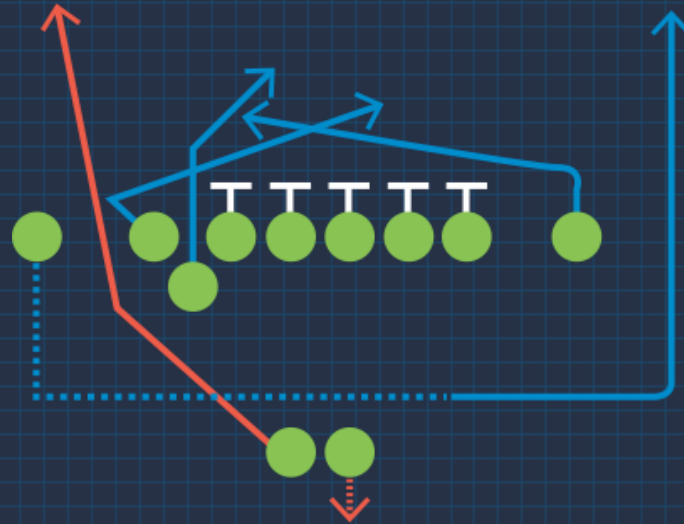


EMAIL PROTECTION

PARTNER SALES PLAYBOOK



Secure Your Office 365 Journey



Contents

- ★ Market Overview
- ★ Solution Overview
- ★ Discovery and Qualification
- ★ Top Plays and Landing Zones
- ★ Competitive Scouting Report
- ★ Resource Index



Market Overview

6.3B

Email protection
market

Email Security

2.3B+

Total addressable market

21%

Expected growth

Incident Response

2.5B

Total addressable market

16%

Expected growth

Cloud Backup

2.5B

Total addressable market

25%

Expected growth

Security Awareness

600M

Total addressable market

42%

Expected growth

Notes:

Cloud email security solutions are emerging as strong complements to Office 365.

Gartner says 30% of enterprises will have an automated solution by 2023.

Microsoft is recommending third-party backup solutions on top of Office 365.

By 2022 60% of enterprise organizations will have comprehensive SAT programs with at least one FTE.

Mega Trends



Office 365 is
mainstream

79%

Of organizations are on Office 365



Native security is
not enough

37%

Of business say security is the biggest blocker for
Office 365 migration



Broadening of
threats

91%

of breaches begin with email

Notes:

Hackers actively target Office 365 users

*Microsoft brand most used in
impersonation attacks*

*Move to cloud raises security
concerns*

*40% of Office 365 users reported
compromised credentials*

*Targeted attacks get through
traditional security*

Email #1 threat vector

13 email threat types

*Cost of avg data breach
is \$3.92 million*

Analysts recommend additional security

“... many times some malicious emails are actually missed by MSDO*, organizations should strongly consider integrating third-party solutions to strengthen their email security capabilities. Aside from traditional gateway solutions, security and risk management leaders should evaluate API-based solutions to act as an additional layer of protection.”

— Gartner, “Determine If Email Security in Office 365 Meets Your Organization’s Needs”

*Microsoft Defender for Office 365

Comprehensive, integrated security



THREAT
PREVENTION



DETECTION
AND RESPONSE



DATA PROTECTION
AND COMPLIANCE



Barracuda

Email Protection™

Value Proposition

For IT organizations that need to protect their businesses, brands, and people against the most advanced email-borne threats, **Barracuda Email Protection™** is a comprehensive, easy-to-use solution that delivers gateway defense, API-based inbox defense, incident response, data protection and compliance capabilities.

Unlike traditional email security vendors, Barracuda offers the most complete, industry-leading prevention, detection, and response capabilities leveraging AI, to enable email protection beyond the gateway for over 38,000+ businesses across the globe.

```
graph TD; A[Prevent Threats] --> B[Detect and Respond]; B --> C[Secure Data and Ensure Compliance];
```

Prevent Threats

Detect and Respond

Secure Data and Ensure
Compliance

Email Protection Plans

CAPABILITIES	ADVANCED	PREMIUM	PREMIUM PLUS
Spam and Malware Protection	✓	✓	✓
Attachment Protection	✓	✓	✓
Link Protection	✓	✓	✓
Email Continuity	✓	✓	✓
Email Encryption	✓	✓	✓
Data Loss Prevention	✓	✓	✓
Phishing and Impersonation Protection	✓	✓	✓
Account Takeover Protection	✓	✓	✓
Automatic Remediation	✓	✓	✓
Domain Fraud Protection		✓	✓
DNS Filtering		✓	✓
Threat Hunting and Response		✓	✓
Automated Workflows		✓	✓
SIEM/SOAR/XDR Integration		✓	✓
Cloud Archiving			✓
Cloud-to-Cloud Backup			✓
Data Inspector			✓
Attack Simulation			✓
Security Awareness Training			✓

Customer Pain Points

Threat Prevention

- Spam, viruses and zero-day attacks
- Growing number of phishing and account takeover, domain spoofing and brand impersonation
- No protection from domain spoofing

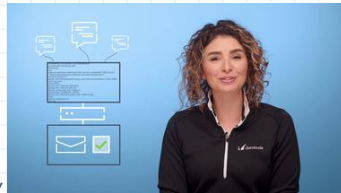
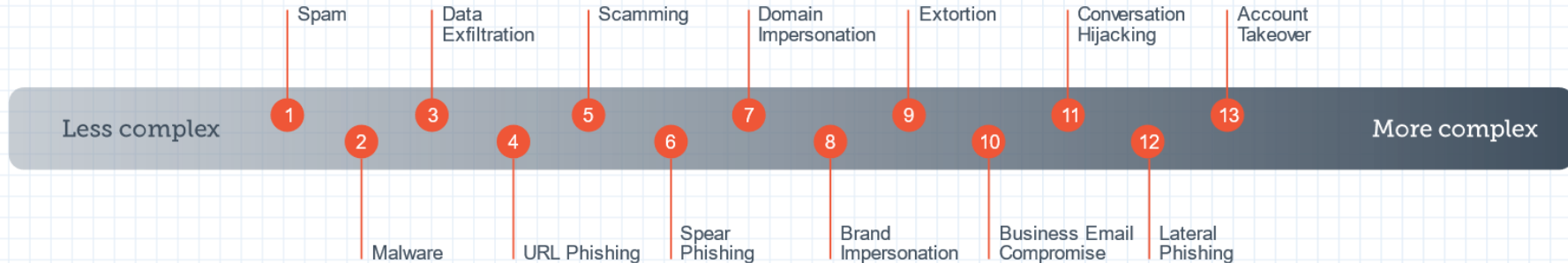
Post-delivery detection and response

- Users falling for spear phishing attacks
- Insufficient incident response that takes too much time
- Malicious links spread through email, Slack/Teams, or other communication tools

Compliance and Data Protection

- Need to comply with email retention mandates, eDiscovery requests and litigation holds
- Need to backup Office 365 data
- Ensure sensitive data is secure and not corrupted
- Has security awareness training compliance mandate

The 13 Email Threat Types



Target Personas



Economic: CISO, CIO

Senior executive that identifies needs and opportunities for technology solution investment and manages cybersecurity risk.

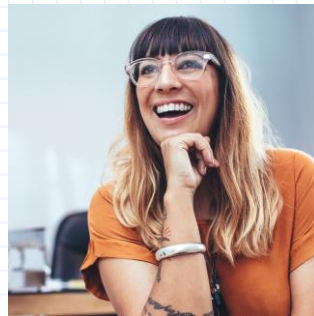
- Experiencing increased spear phishing and BEC attacks
- Needs confirmation of overall effectiveness blocking threats and email attacks, usability and performance of the solution.



Technical: IT Director

Manages IT projects and takes responsibility for the outcomes.

- Recognizes increasing risks from email threats, and wants to migrate them on an ongoing basis
- Ensures chosen solution is good technical fit for organization and IT infrastructure. (current and proposed)



Functional: IT Admin

Owns day-to-day responsibility for security and compliance for the organization.

- Needs to provide effective and practical security to defend against email threats
- Concerned about maintaining compliance within their organization.
- Wants to reduce their overall workload and make operations more efficient

The playing field

mimecast®

Mimecast is a provider of cloud-based email security, archiving, email continuity, security awareness training, web security, and more. Large market presence with over 36,000 customers, servicing SMBs, mid-size and enterprise organizations.

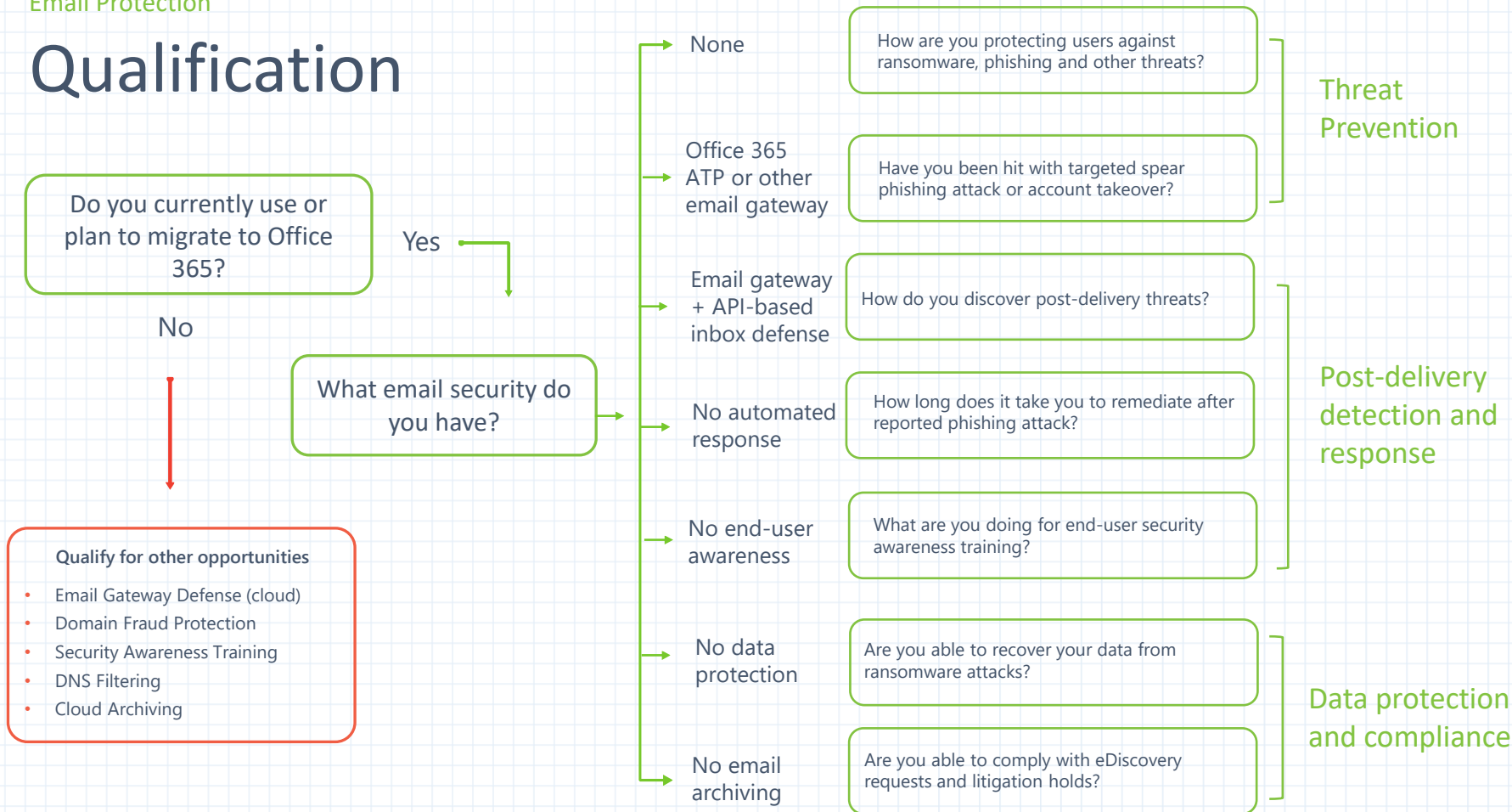
proofpoint®

Proofpoint provides an integrated suite of products for email security, advanced threat protection, cloud app security, archiving, compliance, information protection, digital risk protection, and training. Large customer base, focus of enterprise accounts, high price point.

 **Microsoft**

Microsoft provides email security as part of their Office 365 subscription. Their offering includes email security, archiving, spear phishing simulation and post-delivery remediation. Very large install base with organizations of all sizes.

Qualification



Identify the problem

1. Email threats get through existing security
2. Ineffective post-delivery detection and response
3. Lack of data protection and need to demonstrate compliance

Explore and Pitch: Threat Prevention



Explore: Threat Prevention



Customer use cases

- Malicious inbound email
- Increased number of social engineering attacks
- No protection against account takeover
- Domain spoofing and brand impersonation
- Users access malicious websites



Discovery questions

- How do you protect yourself against malicious links and zero-day malware?
- Do you get spear phishing or other targeted attacks in your inboxes?
- How would you discover and recover from account takeover?
- Are you concerned about your domain being spoofed in phishing attack?
- How do you keep links from malicious websites spreading throughout your organization/.

Advanced

Premium

The Play



Pitch Advanced to prevent threats

Barracuda Email Protection

Advanced is a comprehensive, easy-to-use solution that delivers gateway defense, phishing and impersonation protection and post-delivery remediation



Position Premium for post-delivery detection and response



























- How are you protecting your brand from impersonation?
- Can you prevent your users from accessing malicious websites?
- How do you remediate email threats post-delivery?



Expand to Premium Plus to protect data and ensure compliance

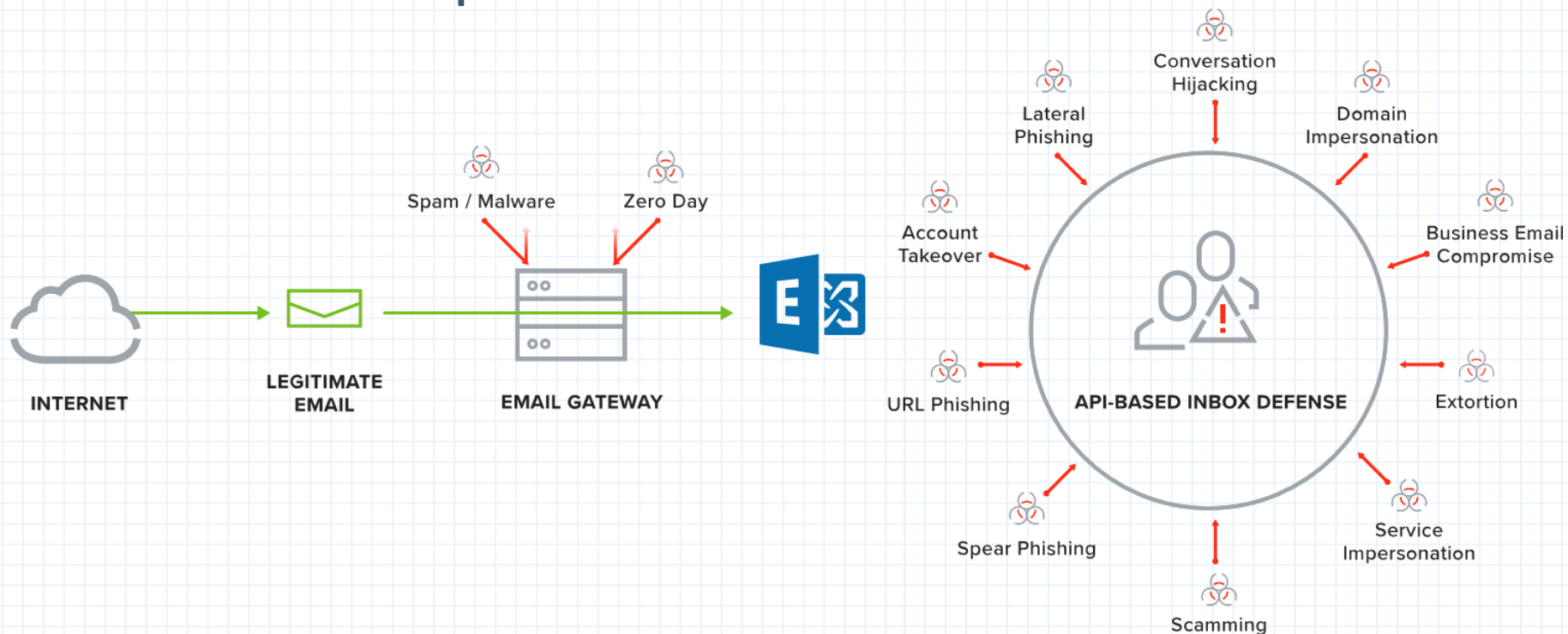
- Are you currently training your staff to recognize spear phishing attacks?
- How do you access and recover data lost, corrupted, or accidentally deleted in users' OneDrive?
- Do you have a compliance requirement to archive emails?

Barracuda's threat prevention

THREAT TYPES	EMAIL GATEWAY ONLY SOLUTIONS	BARRACUDA
Spam		
Malware		
Data Exfiltration		
URL Phishing		
Scamming		
Spear Phishing		
Domain Impersonation		
Service Impersonation		
Extortion		
Business Email Compromise		
Conversation Hacking		
Lateral Phishing		
Account Takeover		



Two forms of prevention



Use email security to protect web users

Web-based threats can arrive via email, and spread throughout your network through Slack, Teams and other collaboration platforms.

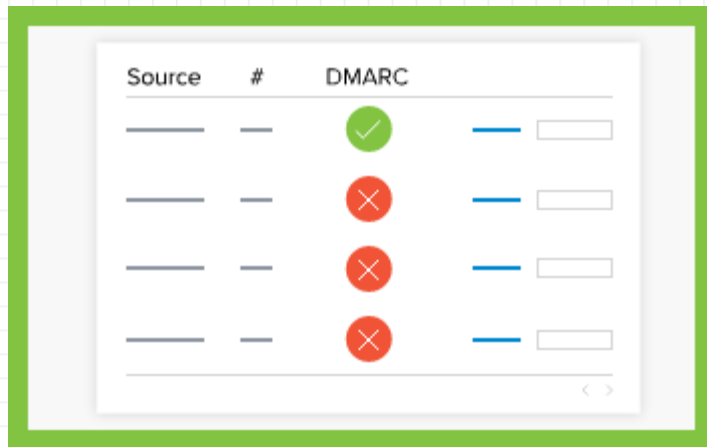
Block users from accessing malicious or inappropriate websites with DNS filtering



Tip: Block malicious websites as part of your incident response workflow

Protect your brand and domains from fraud

- ✓ Automate DMARC reporting and visualization to help accurately set up enforcement policies
- ✓ Prevent third parties from maliciously spoofing your email domain
- ✓ Improve your own email deliverability by ensuring that it passes email authentication



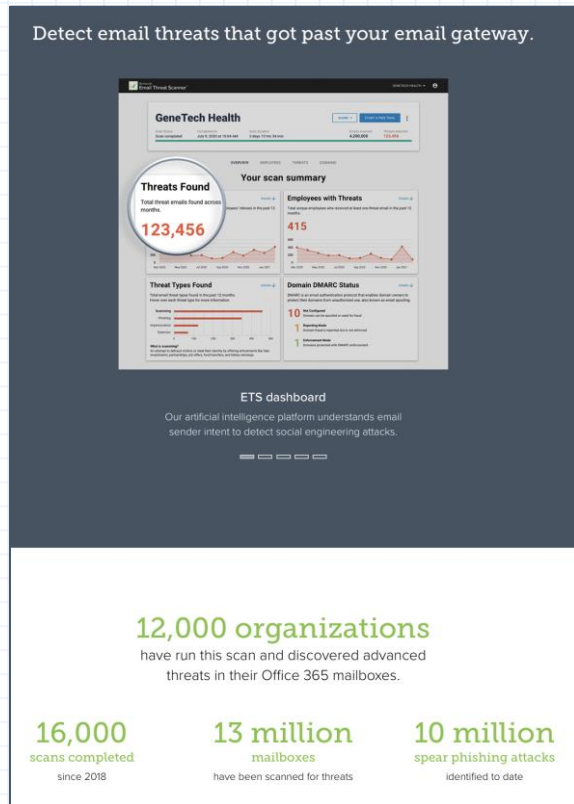
The image shows a screenshot of a DMARC report visualization interface. It features a table with three columns: 'Source', '#', and 'DMARC'. The first row shows a green checkmark in the DMARC column, indicating a successful authentication. The subsequent three rows show red 'X' marks in the DMARC column, indicating failed authentication attempts. To the right of the DMARC column, there are blue lines and input boxes, likely representing the percentage of emails that passed or failed authentication. The interface is framed by a green border.

Source	#	DMARC
—	—	✓
—	—	✗
—	—	✗
—	—	✗

Play Call: Email Threat Scan

- A free tool that scans a customer's Office 365 tenant and discover hidden threats
- Provides detailed report of all threats found regardless of the customer's email gateway
- Highlights gaps in customer's existing email security solution
- Identifies existing security and compliance threats

98% of organizations with Office 365 harbor malicious emails inside their mailboxes.



Explore and Pitch: Detection and Response



Explore Landing Zone: Detection and Response



Customer use cases

- Post delivery threats go undetected
- Incident response takes too long, is inefficient and inconsistent
- Users do not report email attacks
- Security awareness training content is outdated
- Limited IT resources



Discovery questions

- How do you discover post-delivery email threats?
- How long does it take you to respond to email security incidents?
- Do you have a well-defined automated incident response?
- How do you train your users to recognize email attacks?
- Do your users report suspicious email messages?

Premium

Premium Plus

The Play



Pitch Premium

Barracuda Email Protection Premium is a comprehensive, easy-to-use solution that delivers gateway defense, API-based inbox defense, incident response, and web security.



Position Premium Plus

- Are you currently training your staff to recognize spear phishing attacks?
- How do you access and recover data lost, corrupted, or accidentally deleted in users' OneDrive?
- Do you have a compliance requirement to archive emails?



Proactively identify threats post-delivery

Search for any delivered message

- Search by sender email, sender name, email subject, attachment name
- See affected users, clicks, opens, replies, forwards

Get alerted of potential threats

- Based on community-sourced threat intelligence
- Based on previously remediated threats

See sender geographies and live email stats

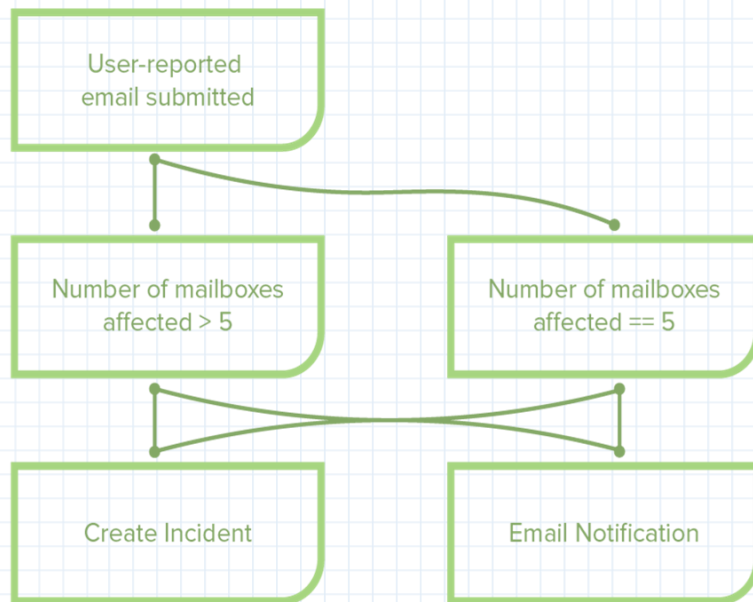
- Geo-IP map helps to identify suspicious senders
- See regional inbound email statistics



Automate response to post-delivery threats

Create custom workflows to completely automate response

- ✓ Preserve IT resources
- ✓ Eliminate duplicate effort
- ✓ Ensure consistent response



Integrations for better security

Integrate email data with external platforms

Integration benefits:

- Centralized view of threat data across security portfolio
- Streamline processes and operations
- Improves IT productivity – reduce alert fatigue, faster incident response, connected systems
- Make smarter security decisions for risk resilience

SIEM/SOAR/XDR



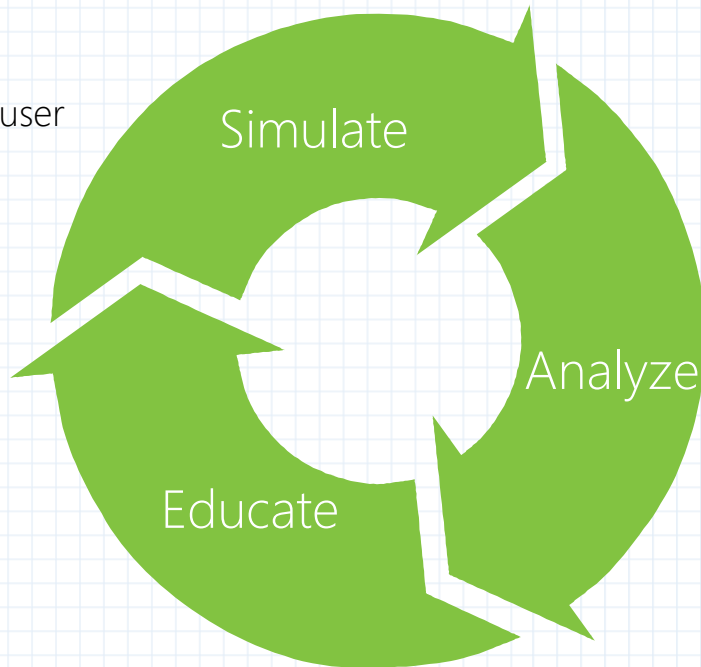
Security Awareness Training

Simulate

Real-world threat simulation to assess user awareness

Educate

Extensive library of training content tailored for different learning styles and abilities.



Analyze

Detailed reporting metrics to determine threat risk and inform the next campaign

Explore and Pitch: Data Security and Compliance



Explore Landing Zone: Data Security and Compliance



Customer challenges

- Data-loss and non-compliance
- Inappropriate web-browsing
- Complex e-discovery response
- Lack of data back and difficulty in recovery of lost data
- Inappropriately stored sensitive data



Discovery questions

- How much control do you have/need over your employees' web browsing?
- How do you demonstrate compliance and retention of your emails?
- What solution are you using to back up your Office 365 data?
- How will you access and recover lost data?
- How are you meeting data compliance and data privacy regulations ?

Premium

Premium
Plus

The Play



Pitch Premium Plus

Barracuda Email Protection Premium Plus is a comprehensive, easy-to-use solution that delivers gateway defense, API-based inbox defense, incident response, data protection, and compliance capabilities.



Explore other opportunities

- How do ensure secure connectivity to other offices and the cloud?
- Do you have remote users? How are you ensuring they securely access business applications?
- What is your cloud firewall solution?



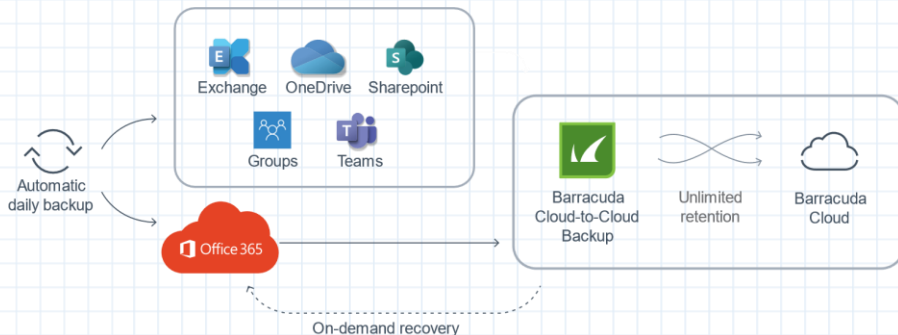
Position Data Protection for Office 365

Microsoft recommends using a third party for data protection

"We strive to keep the services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve your content or data that you've stored. We recommend that you regularly backup your content and data that you store on the services or store using third-party apps."

Microsoft Services Agreement, Section 6B

Unlimited storage and retention with Barracuda



Barracuda offers **unlimited storage and retention** for Office 365 Exchange Online, SharePoint, OneDrive for Business, Teams and Groups, delivered as a SaaS solution.

Cloud Archiving

Securely retain and easily find every email, for as long as needed.

- Retain an unmodified copy of each new message when it's sent or retrieved.
- Streamline e-discovery with multi-level search capabilities
- Ensure regulatory compliance with granular retention policies.



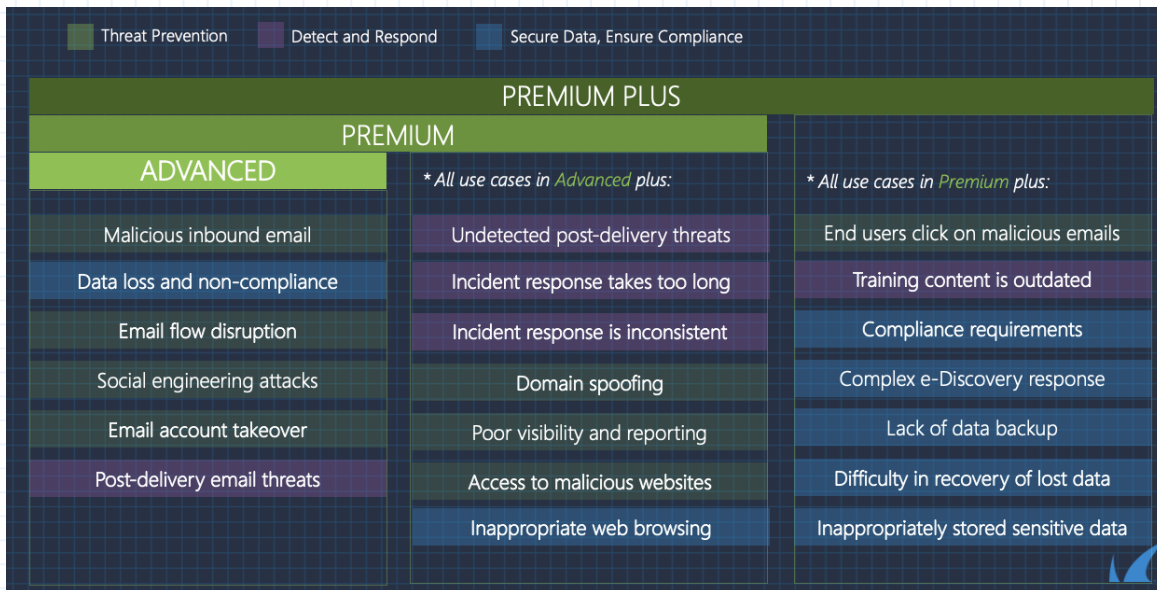
Identify sensitive info and malicious files

Automated detection of sensitive data and malware in OneDrive and SharePoint.

- Easy verification of findings using redacted previews
- Over 130 built-in classifiers + support for custom classifiers
- Automated notifications to admins and end-users



Customer use case navigator



Refer to use case navigator for more in-depth discovery

Identify specific pain-points and position the right email protection plan for customers

Customer use cases navigator

- Prevent Threats
- Detect and Respond
- Secure Data, Ensure Compliance

PREMIUM PLUS		
PREMIUM		
ADVANCED	<i>* All use cases in Advanced plus:</i>	<i>* All use cases in Premium plus:</i>
Malicious inbound email	Undetected post-delivery threats	End users click on malicious emails
Data loss and non-compliance	Incident response takes too long	Training content is outdated
Email flow disruption	Incident response is inconsistent	Compliance requirements
Social engineering attacks	Domain spoofing	Complex e-Discovery response
Email account takeover	Poor visibility and reporting	Lack of data backup
Post-delivery email threats	Access to malicious websites	Difficulty in recovery of lost data
	Inappropriate web browsing	Inappropriately stored sensitive data



Competition



Competitive Comparison: Mimecast

Key strike points:

- Mimecast's API-based phishing protection does not remove messages from inboxes. Provides alert banners only
- Incident response capabilities are limited to automatic remediation
- Mimecast does not offer - account takeover protection, cloud backup, Data Inspector capabilities

	MIMECAST						BARRACUDA
	Email Security Plans			Cyber Resilience Plans			
	Perimeter Defense	Comprehensive Defense	Pervasive Defense	Cyber Resilience Foundations	Cyber Resilience Plus	Cyber Resilience Pro	Email Protection
ADVANCED							
Spam and Malware Protection	✓	✓	✓	✓	✓	✓	✓
Attachment Protection	✓	✓	✓	✓	✓	✓	✓
Link Protection	✓	✓	✓	✓	✓	✓	✓
Email Continuity	-	-	-	✓	✓	✓	✓
Email Encryption	-	-	-	-	-	✓	✓
Data Loss Prevention	✓	✓	✓	✓	✓	✓	✓
Phishing and Impersonation Protection (AI)	Add-on (no remediation)	Add-on (no remediation)	Add-on (no remediation)	Add-on (no remediation)	Add-on (no remediation)	Add-on (no remediation)	✓
Account Takeover Protection	-	-	-	-	-	-	✓
Automatic Remediation	✓	✓	✓	✓	✓	✓	✓
PREMIUM							
Threat Hunting and Response	-	-	-	-	-	-	✓
SIEM/SOAR/XDR Integrations	✓	✓	✓	✓	✓	✓	✓
Automated workflows	-	-	-	-	-	-	✓
Domain Fraud Protection (DMARC)	-	-	✓	-	-	-	✓
DNS filtering	-	-	-	-	-	✓	✓
PREMIUM PLUS							
Cloud Archiving	-	-	-	-	✓	✓	✓
Office 365 backup	-	-	-	-	-	-	✓
Data Inspector	-	-	-	-	-	-	✓
Attack Simulation	-	✓	✓	✓	✓	✓	✓
Security Awareness Training	-	✓	✓	✓	✓	✓	✓

Competitive comparison: Proofpoint

Key strike points:

- No API-based protection against phishing attacks
- Account takeover protection will require purchase of a separate product (CAB)
- No data protection or Data Inspector capabilities

Capability	PROOFPOINT					BARRACUDA
	P1	P1+	P2	P2+	P3	Email Protection
ADVANCED						
Spam and Malware Protection	✓	✓	✓	✓	✓	✓
Attachment Protection	✓	✓	✓	✓	✓	✓
Link Protection	✓	✓	✓	✓	✓	✓
Email Continuity	-	-	✓	✓	✓	✓
Email Encryption	Basic	✓	✓	✓	✓	✓
Data Loss Prevention	Basic	✓	✓	✓	✓	✓
Phishing and Impersonation Protection (AI)	-	-	Partial	Partial	Partial	✓
Account Takeover Protection	-	-	CAD	CAD	CAD	✓
Automatic Remediation	✓	✓	✓	✓	✓	✓
PREMIUM						
Threat Hunting and Response	✓	✓	✓	✓	✓	✓
SEIM/SOAR/XDR Integrations	✓	✓	✓	✓	✓	✓
Automated workflows	✓	✓	✓	✓	✓	✓
Domain Fraud Protection (DMARC)	-	✓	✓	✓	✓	✓
DNS filtering	-	-	-	-	-	✓
PREMIUM PLUS						
Cloud Archiving	-	-	-	-	✓	✓
Office 365 backup	-	-	-	-	-	✓
Data Inspector	-	-	-	-	-	✓
Attack Simulation	✓	✓	✓	✓	✓	✓
Security Awareness Training	✓	✓	✓	✓	✓	✓

Competitive comparison: Microsoft

Key strike points:

- Built-in native security is not enough to protect against email threats
- Significant gaps in data protection and business continuity
- Impersonation protection is limited to 350 users

	Microsoft			Barracuda
Capability	Microsoft Exchange Online Protection	Microsoft Defender Plan 1	Microsoft Defender Plan 2	Barracuda
ADVANCED				
Spam and Malware Protection	✓	✓	✓	✓
Attachment Protection	-	✓	✓	✓
Link Protection	-	✓	✓	✓
Email Continuity	-	-	-	✓
Email Encryption	✓	✓	✓	✓
Data Loss Prevention	✓	✓	✓	✓
Phishing and Impersonation Protection (AI)	-	✓	✓	✓
Account Takeover Protection	-	-	-	✓
Automatic Remediation	-	✓	✓	✓
PREMIUM				
Threat Hunting and Response	-	-	✓	✓
Automated Workflows	-	-	-	✓
SIEM/SOAR/XDR Integrations	-	-	✓	✓
Domain Fraud Protection (DMARC)	-	-	-	✓
DNS filtering	-	-	-	✓
PREMIUM PLUS				
Cloud Archiving	-	✓	✓	✓
Cloud-to-Cloud Backup	-	-	-	✓
Data Inspector	-	-	-	✓
Attack Simulation	-	-	-	✓
Security Awareness Training	-	✓	✓	✓

Microsoft Defender Plan 1 and 2 are included with E5 or available at an additional cost for all other Office 365 plans.

Our Right to Play



“Barracuda solutions offer a lot of value. They make it easy to protect our organization against email threats like account takeover and to deal with incidents effectively. Barracuda helped tighten up our email security posture.” – Salvation Army



Resource Index



Email Protection Resources



Use case navigator [COMING SOON!]

Product info, in-depth use cases, qualification guidance, competitive differentiators



Sales Toolkit

Product info, use cases, competitive differentiators



Overview Deck

Solution value proposition



Data Sheet

Comprehensive overview



FAQ