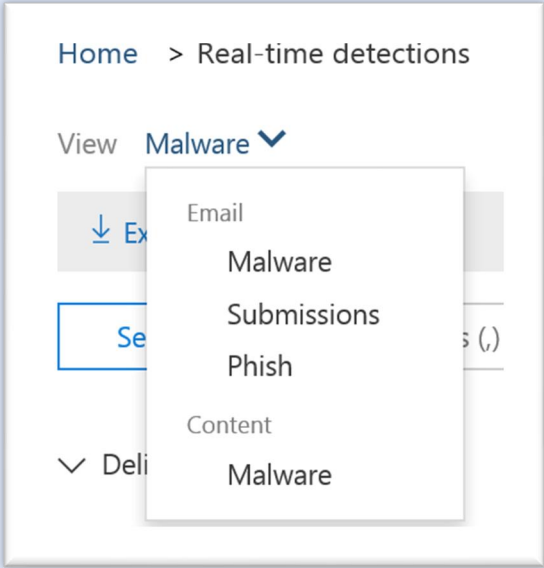
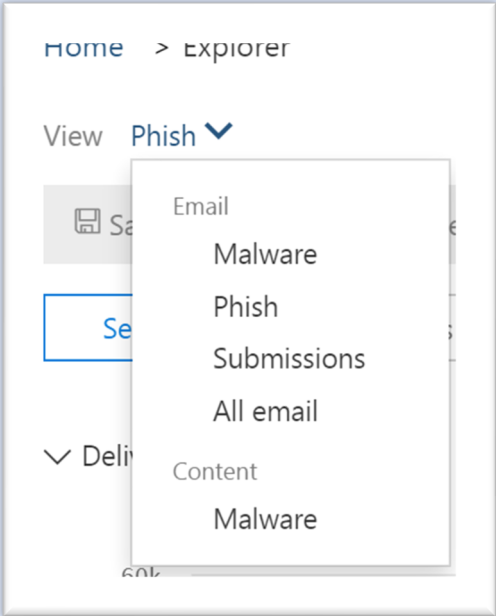


# Office 365 Advanced Threat Protection (Office 365 ATP) Plans

This document illustrates capabilities and UI feature differences for Office 365 ATP Plan 1 and Plan 2.

NOTE: New features are continually in progress and are being added to Office 365 ATP. This document compares features in Office 365 ATP Plan 1 and Plan 2 as of the time of this document creation. For the most current information, use the following resources:

- [Office 365 ATP plans and pricing](#)
- [Microsoft 365 roadmap: Office 365 features](#)

Category	Feature	Plan 1	Plan 2
Threat Protection Capabilities	ATP Safe Attachments	Yes	Yes
	ATP Safe Links	Yes	Yes
	ATP anti-phishing	Yes	Yes
Threat Investigation	Toolset	Real-time detections	Threat Explorer
		<b>Email:</b> Malware, Submissions, Phish, <b>Content:</b> Malware	<b>Email:</b> Malware, Submissions, Phish, All email. <b>Content:</b> Malware
	Search Criteria Available		

Search Filter - Malware

Home > Real-time detections

View Malware

Export

Sender

Use commas (,)

Basic

- Sender
- Recipients
- Sender domain
- Subject
- Attachment filename
- Malware family
- Delivery action
- Detection technology
- Delivery location

Advanced

- Internet Message ID
- Network Message ID
- Sender IP
- Attachment SHA256
- Cluster ID
- Alert Policy ID

Home > Explorer

View Malware

Save query | Save query

Sender

Use commas (,)

Basic

- Sender
- Recipients
- Sender domain
- Subject
- Attachment filename
- Malware family
- Delivery action
- Detection technology
- Delivery location

Advanced

- Internet Message ID
- Network Message ID
- Sender IP
- Attachment SHA256
- Cluster ID
- Alert Policy ID

Search Filter - Phish

[Home](#) > [Real-time detection](#)

View

Phish

Export

Sender

Use comma

Email

Sender

Recipients

Sender domain

Subject

Attachment filename

Delivery action

Detection technology

Delivery location

Advanced

Internet Message ID

Network Message ID

Sender IP

Attachment SHA256

Cluster ID

Alert Policy ID

Campaign ID

URLs

URL domain

Click verdict

[Home](#) > [Explorer](#)

View

Phish

Save query

Save c

Sender

Use comm

Email

Sender

Recipients

Sender domain

Subject

Attachment filename

Delivery action

Detection technology

Delivery location

Advanced

Internet Message ID

Network Message ID

Sender IP

Attachment SHA256

Cluster ID

Alert Policy ID

Campaign ID

URLs

URL domain

URL domain and path

URL

URL path

Click verdict

Search Filter - Content  
Malware

[Home](#) > [Real-time detection](#)

View [Malware](#) ▼

↓ Export ▼

Filename ▼

Use comma

File

Filename

Workload

Site

Users

File owner

Last modified by

Malware

SHA256

Malware family

Detection technology

[Home](#) > [Explorer](#)

View [Malware](#) ▼

↓ Export ▼

Filename ▼

Use comma

File

Filename

Workload

Site

Users

File owner

Last modified by

Malware

SHA256

Malware family

Detection technology

		No	Yes
	Search Filter - All Email		<div>Home &gt; Explorer</div> <div>View All email</div> <div>Save query   Save q</div> <div>Sender Use comma</div> <div><div>Basic</div><div>Sender</div><div>Recipients</div><div>Sender domain</div><div>Subject</div><div>Attachment filename</div><div>Malware family</div><div>Delivery action</div><div>Detection technology</div><div>Delivery location</div><div>Advanced</div><div>Internet Message ID</div><div>Network Message ID</div><div>Sender IP</div><div>Attachment SHA256</div><div>Cluster ID</div><div>Alert Policy ID</div><div>Campaign ID</div><div>URLs</div><div>URL domain</div><div>URL domain and path</div><div>URL</div><div>URL path</div><div>Click verdict</div></div>

Sub Filter - Malware

Home > Real-time detections

View Malware ▾

⬇ Export ▾

Sender ▾ Use commas

Delivery action  
Detection technology

Home > Explorer

View Malware ▾

Save query | Save

Sender ▾ Use co

Malware family

Malware family

Sender domain

Sender IP

Delivery action

Detection technology

	<b>Sub Filter - Phish</b>	<div data-bbox="913 266 1426 948"><div>Home &gt; Real-time detections</div><div>View Phish ▾</div><div>↓ Export ▾</div><div>Sender ▾ Use commas</div><div><div>Sender domain</div><div>Sender IP</div><div>Delivery action</div><div>URL domain</div><div>Detection technology</div></div></div>	<div data-bbox="1756 204 2165 1170"><div>Home &gt; Explorer</div><div>View Phish ▾</div><div>Save query   Save query as</div><div>Sender ▾ Use commas</div><div><div>Delivery action ▾</div><div>Sender domain</div><div>Sender IP</div><div>Delivery action</div><div>Full URL</div><div>URL domain</div><div>URL domain and path</div><div>Detection technology</div></div></div>
	<b>Advanced Queries/Filter</b>	No	Yes <div data-bbox="1778 1338 2137 1516"><div>Advanced filter</div></div>
	<b>Ability to Save Queries</b>	No	Yes <div data-bbox="1605 1634 2332 1719"><div>Save query   Save query as   Saved query settings  </div></div>



	Result View - Malware	Only Email	Top Malware Family, Emails and Email Origin
	Result View - Phish	Emails, URL clicks, URLs	Email, URL clicks, URLs, Top Campaign

Email

+ Actions ▾

Top malware families

Email

Email origin

Email

URL clicks

URLs

+ Actions ▾

<input type="checkbox"/>	Email date ▾	Subject	Recipient	Sender
<input type="checkbox"/>	12/31/19 1:32 PM	Please approve	menanh@m365h7300	Tom hanl

Email

URL clicks

URLs

Email origin

Top Campaign (Preview)

+ Actions ▾

<input type="checkbox"/>	Email date ▾	Subject	Recipient	Sender
<input type="checkbox"/>	31/12/2019 2:1...	sicher, dass Sie bereit si...	emilyb@m365x246949....	PhillipWood@lithoexp

Threat Remediation	Threat remediation Action	Only Submission	Move and Delete, Track and Notify and Submission.
		<div><div>EmailURL click</div><div>+ Actions ▾</div><div><div>Start new submission</div><div>Report clean</div><div>Report phishing</div><div>Report malware</div><div>Report spam</div></div></div>	<div><div>EmailURL clicks</div><div>+ Actions ▾</div><div><div>Move &amp; delete</div><div>Move to junk folder</div><div>Move to deleted items</div><div>Soft delete</div><div>Hard delete</div><div>Move to inbox</div><div>Track &amp; notify</div><div>Trigger investigation</div><div>Add to remediation</div><div>Contact recipients</div></div></div> <div><div>Track &amp; notify</div><div>Trigger investigation</div><div>Add to remediation</div><div>Contact recipients</div><div>Start new submission</div><div>Report clean</div><div>Report phishing</div><div>Report malware</div><div>Report spam</div></div>

	Action Center	No	Yes																																				
			<div><div>Home &gt; Review</div><div><div>Action Center</div><div><div><div><div></div></div></div><div>Track phishing and malware campaigns aimed at your users and take appropriate action.</div></div></div></div>																																				
	Campaign View	No	Yes																																				
			<div><div><div>campaign</div><div>sample subject</div><div>type</div><div>campaign subtype</div><div>sup. campaign (review)</div></div><div><div>note: This feature is in <b>preview</b> and is subject to change. Also, campaigns include a specific subset of messages, and are only filterable by date. <a href="#">Learn more</a></div><table><tr><th>name</th><th>Sample Subject</th><th>Type</th><th>Subtype</th><th>Recipients</th><th>Delivered</th></tr><tr><td><a href="#">vish.F832FADC</a></td><td>FAB Email Profile Modification</td><td>Phish</td><td>Unknown</td><td>1</td><td>0</td></tr><tr><td><a href="#">vish.C95A7B8E</a></td><td>1,000,000 EURO</td><td>Phish</td><td>ATP-Unknown</td><td>41</td><td>0</td></tr><tr><td><a href="#">vish.BFC2C586</a></td><td>Info on Your Mailbox Storage Usage</td><td>Phish</td><td>Unknown</td><td>5</td><td>0</td></tr><tr><td><a href="#">vish.BCCED095</a></td><td>Get a full range of bright feelings. Buy Viagra Super Force.</td><td>Phish</td><td>Unknown</td><td>8120</td><td>0</td></tr><tr><td><a href="#">vish.3E3EE1FE</a></td><td>LINEにご登録のアカウント（名前・パスワード、その他個人情報）の磁部 10:33...</td><td>Phish</td><td>Unknown</td><td>3</td><td>0</td></tr></table></div></div>	name	Sample Subject	Type	Subtype	Recipients	Delivered	<a href="#">vish.F832FADC</a>	FAB Email Profile Modification	Phish	Unknown	1	0	<a href="#">vish.C95A7B8E</a>	1,000,000 EURO	Phish	ATP-Unknown	41	0	<a href="#">vish.BFC2C586</a>	Info on Your Mailbox Storage Usage	Phish	Unknown	5	0	<a href="#">vish.BCCED095</a>	Get a full range of bright feelings. Buy Viagra Super Force.	Phish	Unknown	8120	0	<a href="#">vish.3E3EE1FE</a>	LINEにご登録のアカウント（名前・パスワード、その他個人情報）の磁部 10:33...	Phish	Unknown	3	0
name	Sample Subject	Type	Subtype	Recipients	Delivered																																		
<a href="#">vish.F832FADC</a>	FAB Email Profile Modification	Phish	Unknown	1	0																																		
<a href="#">vish.C95A7B8E</a>	1,000,000 EURO	Phish	ATP-Unknown	41	0																																		
<a href="#">vish.BFC2C586</a>	Info on Your Mailbox Storage Usage	Phish	Unknown	5	0																																		
<a href="#">vish.BCCED095</a>	Get a full range of bright feelings. Buy Viagra Super Force.	Phish	Unknown	8120	0																																		
<a href="#">vish.3E3EE1FE</a>	LINEにご登録のアカウント（名前・パスワード、その他個人情報）の磁部 10:33...	Phish	Unknown	3	0																																		

	Top Users Impacted	No	Yes
			<div>Top targeted users</div> <div><div>EM</div><div>emilyb@m365x246949.onmicrosoft.com</div><div>30322 attempts</div></div>

Automated Investigation and Remediation	Automated Investigation and Remediation	No	Yes
	Integration with MDATP for Threat signal sharing with Endpoints	No	Yes
Office 365 Alerts	A potentially malicious URL click was detected	No	Yes
	Email messages containing malware removed after delivery	No	Yes
	Email messages containing phish URLs removed after delivery	No	Yes
	Malware campaign detected after delivery.	No	Yes
	Malware campaign detected and blocked	No	Yes
	Malware campaign detected in SharePoint and OneDrive	No	Yes
	Phish delivered due to tenant or user override	No	Yes
	Unusual external user file activity	No	Yes
	Unusual volume of external file sharing	No	Yes
	Unusual volume of file deletion	No	Yes
	Unusual increase in email reported as phish	No	Yes
	User impersonation phish delivered to inbox/folder	No	Yes

Attack Simulator			
	Spear Phishing Simulation	No	Yes
	Spear Phishing (Attachment) Simulation	No	Yes
	Brute Force Attack Simulation	No	Yes
	Password Spray Attack Simulation	No	Yes
Threat Tracker	Trending Campaigns	No	Yes
	Noteworthy Campaign	No	Yes
	Tracking saved Queries	No	Yes