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](https://products.office.com/en-us/exchange/advance-threat-protection#office-ProductsCompare-785zwzq)
* [Microsoft 365 roadmap: Office 365 features](https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=O365)

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
|  | **Search Criteria Available** | **Email:** Malware, Submissions, Phish,  **Content:** Malware  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1AB3C77A.tmp | **Email**: Malware, Submissions, Phish, All email.  **Content**: Malware  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D527ED98.tmp |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | **Search Filter - Malware** | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B217DF66.tmp | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2E748864.tmp |
|  | **Search Filter - Phish** | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5DEB6012.tmp | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\38F249F0.tmp |
|  | **Search Filter - Content Malware** | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\671E757E.tmp | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AFE3E3C.tmp |
|  | **Search Filter - All Email** | No | Yes  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F1203148.tmp |
|  | **Sub Filter - Malware** | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FFCFCE96.tmp | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3956AF14.tmp |
|  | **Sub Filter - Phish** | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\199E2A42.tmp | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\ED2303A0.tmp |
|  | **Advanced Queries/Filter** | No | Yes  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4C844AAE.tmp |
|  | **Ability to Save Queries** | No | Yes  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6553AEC.tmp |
|  | **Result View - Malware** | C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E72A1BDA.tmp Only Email | Top Malware Family, Emails and Email Origin    C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6A9820F8.tmp |
|  | **Result View - Phish** | Emails, URL clicks, URLs  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\88A049C6.tmp | Email, URL clicks, URLs, Top Campaign  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B9BD41C4.tmp |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Threat Remediation | **Threat remediation Action** | Only Submission    C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A08C4072.tmp | Move and Delete, Track and Notify and Submission.  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BAC8E950.tmp  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BC142BDE.tmp |
|  | **Action Center** | No | Yes  Machine generated alternative text: Home > Review  Action Center  Track phishing and  malware campaigns aimed  at your users and take  appropriate action. |
|  | **Campaign View** | No | Yes      C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F3BE239C.tmp |
|  | **Top Users Impacted** | No | Yes  C:\Users\avlot\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B8AF80A.tmp |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |