

M365 Product Marketing Group

Microsoft Office 365 ATP and Proofpoint PRO+TAP

Comparison Document (version 1.0)

© 2025 Microsoft Corporation. All rights reserved.

Microsoft Proprietary and Confidential Information

This training package content is proprietary and confidential, and is intended only for users described in the training materials. Some elements of this document are subject to change. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

This content and information is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or information included in this package is strictly prohibited. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft and the Microsoft products and services listed are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Table of Contents

Using this Comparison Document.....	4
Audience and Terminology.....	5
Audience	5
Terminology.....	5
Product Changes and Approach.....	6
Product Changes.....	6
Approach.....	6
Purpose, Added Value, and Objectives	7
Purpose and Added Value	7
Objectives	8
Quick Start.....	9
Document Structure	9
Quick Start Table.....	10
Key Fundamentals of Both Products	11
Microsoft Office 365 Advanced Threat Protection (ATP).....	12
Products and Plans.....	12
Design and Approach	13
Proofpoint PRO+TAP	14
Products and Plans.....	14
Design and Approach	15
System Requirements	16
Executive Summary.....	17
Comparison Table Summary	18
Pricing.....	18
Evaluation Experience	18
Dashboards and Reporting.....	19
Default Settings	20
Quarantine Experience.....	21
Key Product Differences	22
Pros/Cons.....	24
Office 365 ATP Plan 2.....	24
Proofpoint PRO+TAP	26
Comparisons and User Scenarios	28

About the Change in Focus for this Document	29
Pricing.....	30
Comparison Table.....	30
Office 365 ATP Plan 2.....	30
Proofpoint PRO+TAP	31
Evaluation Experience	32
Comparison Table.....	32
Evaluating Office 365 ATP Plan 2	33
Evaluating Proofpoint PRO+TAP	33
Dashboards and Reporting	43
Comparison Table.....	44
Different Dashboard and Reporting Approach	45
Dashboards and Reporting for Both Products.....	47
Dashboards and Reporting of Office 365 ATP Plan 2	57
Dashboards and Reporting of Proofpoint PRO+TAP.....	58
Default Settings	61
How the Information was Gathered	61
Comparison Table.....	62
Default Settings for Both Products	63
Default Settings of Office 365 ATP Plan 2	64
Default Settings of Proofpoint PRO+TAP	79
Quarantine Experience.....	90
Comparison Table.....	90
Quarantine Experience with Office 365 ATP Plan 2	90
Quarantine Experience with Proofpoint PRO+TAP	91
FAQ	92
References	99
Microsoft ATP References	100
Proofpoint PRO+TAP References	102
Appendix.....	104
Evaluating Proofpoint PRO+TAP	104

Using this Comparison Document

Start here to most quickly and efficiently use and apply the information in this comparison document. Briefly, this section describes this document's audience, terminology, product changes, approach, purpose and added value, and objectives, providing you with its scope and intent.

Also, at the end of this section is the [Quick Start](#) section, where you can see the [Document Structure](#) and [Quick Start Table](#), so that you can immediately get the information you need, when you need it.

Audience and Terminology

Audience

The audience for this document is internal Microsoft only. The raw content in this document might take other forms and formats and can be made available to the M365 Product Marketing Group.

Terminology

From this point forward in this document, the Microsoft product will be referred to as *Microsoft ATP* (or simply *ATP*). The Proofpoint products are *Proofpoint Email Protection (PRO)* and *Proofpoint Targeted Attack Protection (TAP)* and will be referred to as *Proofpoint PRO+TAP* (or simply *PRO+TAP*).

Product Changes and Approach

Product Changes

During the time period that this document was drafted, there were changes to the products, specifically, to the Proofpoint product. The main shift impacting this document was the shift in what products were paired with one another. Initially, the focus of this document was Proofpoint TAP, but in the final draft, you'll see multiple references to Proofpoint PRO and Proofpoint TAP (Proofpoint PRO+TAP). See both the [Terminology](#) and [Proofpoint PRO+TAP](#) sections for further details.

Approach

Sources

Content for this document was sourced from:

- Initiating an information gathering process for both products.
- Initiating an evaluation download, installation, and configuration process.
- Based on CELA, logistics, and purchase requirements. Also used available specification information to complete the information needed as described in the [Purpose](#) and [Objectives](#) sections.



Note: Products and technology change and evolve over time, and these two products are no exception. As of this writing, Microsoft had not planned any major changes to the Microsoft ATP product, though the timeline is unknown for changes in the Proofpoint TAP product.

Comparisons and User Scenarios

In the Comparisons and User Scenarios section, there are three subsections for each element of the comparison criteria:

- **Comparison Table:** A table with star ratings (0 to 5) and notes about those specific ratings.
- **Office 365 ATP Plan 2:** Detailed comparison information about the Office 365 ATP Plan 2 product.
- **Proofpoint PRO+TAP:** Detailed comparison information about the Proofpoint TAP product.

Purpose, Added Value, and Objectives

Purpose and Added Value

Supporting Materials

While the main purpose for this document is to compare the two products, a secondary purpose quickly surfaced that is equal to (and possibly even greater than) the comparisons.

The supporting materials for this document (including a recorded product demonstration, an SLA, a detailed administration guide, and much more information for both products) are a considerable library of information for the intended audience and further support the [objectives](#) of this document. All of the supporting materials are listed (and where possible, linked to) in the [References](#) section.

Comparisons

The main purpose of this document is to compare the [Office 365 ATP Plan 2](#) and [Proofpoint Targeted Attack Protection \(TAP\)](#) advanced threat protection (ATP) products.

The following categories, usage scenarios, and considerations will be compared and evaluated:

Comparison Categories and Usage Scenarios	Comparison Considerations
Pricing	○ What are the pricing plans or approaches for each product? ○ How does pricing differ between the products?
Evaluation Experience	○ How easy is it to evaluate the product? ○ There is a significant difference between the processes for evaluating each product.
Dashboards and Reporting	○ Dashboards ▪ How do the dashboards compare? ▪ What tools/reports are available for automated investigation and hunting. What does that process look like? ○ Reporting ▪ How can customers see if it's working and effective? What reports are available, how often are they delivered? ▪ What tools/reports are available for manual investigation and hunting? What does that process look like? ▪ How can users and admins report suspicious content?
Default Settings	○ How does each product's approach to advanced threat protection default settings compare? ○ How (where comparable) to the settings themselves compare?
Quarantine Experience	○ How does the quarantine experience differ between the two products?

Objectives

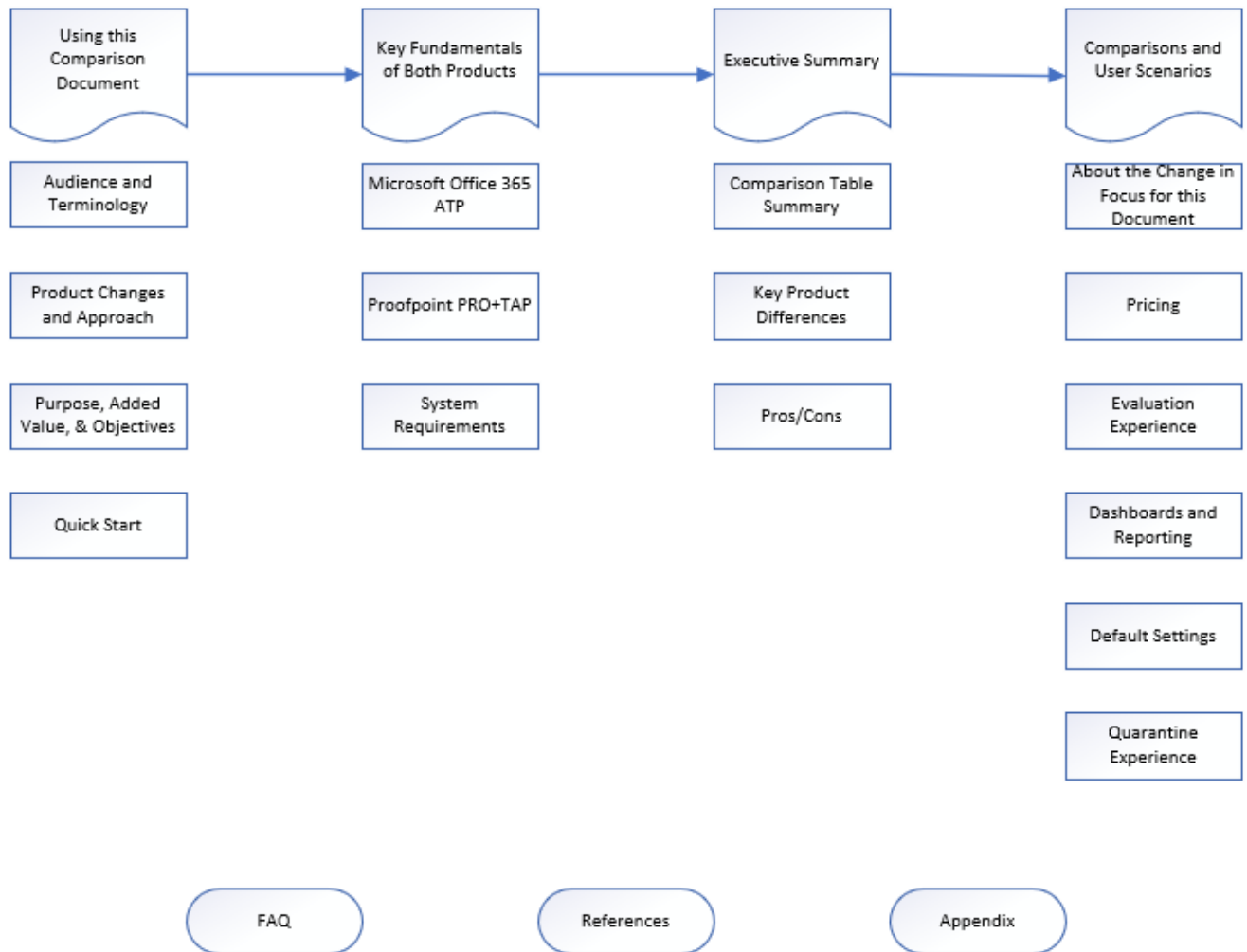
The objectives of this comparison document are:

- Provide any identified product gap information to the engineering team.
- Document information for the M365 Product Marketing Group to communicate with the customers around perceptions. (To better position ourselves.)
- Producing follow-on materials using this document as the baseline source content.
- Optionally: Best practice end-user guidance.

Quick Start

Document Structure

The following diagram shows the structure of this document, to help you understand where to go to get the information you need from it.



Quick Start Table

Use the following table to quickly go to the information you need.

Figure 1: Comparison document structure

Topic	Subtopic	Description and Notes
Using this Comparison Document	Section overview	Comparison document introduction (context and setting the stage).
	Audience and Terminology	Describes the audience and how the product names are used.
	Product Changes and Approach	About the products in motion during document development and the approach to the comparisons and evaluation.
	Purpose, Added Value, and Objectives	Purpose and intent of this document, added value beyond the comparisons and evaluations, and the objectives.
	Quick Start	Documentation structure and quick start.
Key Fundamentals of Both Products	Section overview	Introduction to the <i>Key Fundamentals of Both Products</i> .
	Microsoft ATP	Microsoft ATP product, plan, design, and approach.
	Proofpoint TAP	Proofpoint TAP product, plan, design, and approach.
	System Requirements	System requirements for both products.
Executive Summary	Section overview	Introduction to the <i>Executive Summary</i> .
	Comparison Table Summary	Compilation of all of the comparison and rating tables from each section in the <i>Comparisons and User Scenarios</i> section.
	Key Product differences	Details the important differences between the products.
	Pros/Cons	The strengths and the challenges with both products.
Comparisons and User Scenarios	Section overview	Side-by-side comparison across multiple features.
	About the Change of Focus for this Document	How the focus changed for this document, and why. Also, what was removed and what was added, as a result.
	Pricing	Pricing plans and comparison between the two products.
	Evaluation Experience	Comparing how easy or hard it is to evaluate each product.
	Dashboards and Reporting	Comparing the dashboards and reporting.
	Default Settings	Comparing each product's default settings, how easy it is to change them, and the effectiveness of the defaults.
	Quarantine Experience	Comparing how each product applies quarantining.
FAQ		Responses to frequently asked questions.
References		Sources used in developing this document and references for further information.
Appendix		Detailed imbedded email attachments used for the <i>Evaluation Experience</i> section.

Key Fundamentals of Both Products

The purpose of this section is to share product, plan, design, and approach information about both Microsoft Office 365 Advanced Threat Protection (ATP) and Proofpoint Email Protection (PRO) plus Targeted Attack Protection (TAP). This includes details about the fundamental differences and (in the case of system requirements) similarities.

Understanding that information is critical to providing the context you need to consume comparisons between ATP and PRO+TAP. There are significant differences in the approach, product design, and business model, which result in corresponding differences in the elements compared in this document (such as the evaluation process, setup experience, and performance).

Microsoft Office 365 Advanced Threat Protection (ATP)

Microsoft Office 365 Advanced Threat Protection (ATP), which is referred through the rest of this document as Microsoft ATP, is built on top of Office 365. Before describing the two plans to select from, first, here is a little bit of background about prior product offerings.

Products and Plans

Prior to Microsoft Office 365 ATP, there were two separate products:

- **The original Microsoft ATP:** Formerly, the ATP standalone product.
- **Office 365 Threat Intelligence (TI):** Formerly, the TI standalone product.

Those two products are shown in the [Feature availability across Advanced Threat Protection \(ATP\) plans](https://docs.microsoft.com/en-us/office365/advanced-threat-protection/feature-availability-across-atp-plans) page on docs.microsoft.com.

In short, there are three plans to select from:

- **Plan 1:** Original ATP
- **Plan 2:** Plan 1 plus TI
- **Plan 3:** Office 365 Enterprise E5 (includes all Office 365 ATP Plan 2 benefits and more).

Design and Approach

Plan 1 and Plan 2 are designed to be added to your existing Office 365 subscription plan. Plan 3 is the Office 365 Enterprise E5 plan, which is an Office 365 subscription that includes the Office 365 ATP Plan 2 benefits and more.

See them compared, with the corresponding features on the [Get the right Office 365 Advanced Threat Protection](#) table.

This plan used for this comparison document is the Office 365 Advanced Threat Protection (Plan 2) plan.

Proofpoint PRO+TAP

Proofpoint PRO+TAP is shorthand in this document for a combination of two third-party products among several related Proofpoint products. As described in the [Product Changes](#) and [Terminology](#) sections, those two products are Proofpoint Email Protection (PRO) and Proofpoint Targeted Attack Protection (TAP).

Products and Plans

Proofpoint products are listed on their partner sites (such as what's listed on the [AdvancedThreatWorks](#) site, a Proofpoint authorized online reseller whose page was the first (as an ad) to appear in an Internet search for **Proofpoint Products**). Comparing that list with what's listed on the Proofpoint site, on their [product line card](#), the two lists are different. What we list here is from the Proofpoint [product line card](#).

Their suite of solutions spans email, social media, web, network and cloud—including Microsoft Office 365. The Proofpoint TAP product (that is the focus of this document) is one of the Advanced Threat Protection products in the Proofpoint product suite.

Table 1: Proofpoint product table

Category	Product
Email Protection	Email Protection
	Email Fraud Defense 360
	Internal Mail Defense
	Essentials for Small Business
Advanced Threat Protection	Targeted Attack Protection in Email
	TAP Isolation Personal Browsing Defense
	TAP Isolation Personal Webmail Defense
	TAP SaaS Defense
	Threat Response
	Threat Response Auto-Pull
	Emerging Threats Intelligence
	Emerging Threats Pro Ruleset
Cloud App Security	Premium Threat Information Service
	Cloud Account Defense
Information Protection	Cloud App Security Broker
	Data Discover
	Email DLP
User Protection	Email Encryption
	Phishing Simulation and Security Awareness Training from Wombat Security
Digital Risk Protection	Digital Risk Protection
Archiving and Compliance	Enterprise Archive
	Enterprise Collaboration Archive
	E-Discovery and Analytics
	Intelligent Supervision
	Social Media Compliance

Design and Approach

As the Proofpoint suite is a third-party product, it is not built on top of the Microsoft Office 365, nor can it be added to your existing Office 365 plan. Proofpoint PRO+TAP is a gateway that is built and configured for a customer organization based on specific information provided by the customer. Examples of that customer information are:

- **Number of email users:** Need the number of email users (not the number of mailboxes).
- **Mail volume report:** Minimum of 30-day day-to-day mail volume report (can be pulled by an Office 365 administrator).

(For more information, go to [Details: Evaluating Proofpoint PRO+TAP](#) and [Details: Setting Up Office 365 ATP Plan 2](#).)

System Requirements

Both products use a Software as a Service (SaaS) model. So, there are not hardware or software requirements like there would be for desktop or mobile applications. Though neither company specifies system requirements for the typical users or for admin users, all that is needed is simply an operating system, browser, and Internet connection.

Executive Summary

This section briefly and concisely summarizes the results of the [System Requirements](#), [Comparisons and User Scenarios](#), and other information in the following subsections:

- [Comparison Table Summary](#): All of the comparison tables listed together, to see the full picture all at once.
- [Key Product Differences](#): The main product differences.
- [Pros/Cons](#): The advantages and disadvantages of both products.

Comparison Table Summary

This section lists the comparison tables from all of the sections in the [Comparisons and User Scenario](#) section ([Pricing](#), [Evaluation Experience](#), [Dashboards and Reporting](#), [Default Settings](#), and [Quarantine Experience](#)) to see the full picture at a high level.

Pricing

Table 2: Pricing comparison table

Office 365 ATP Plan 2	Proofpoint PRO+TAP	Notes
		Microsoft: Though higher, the pricing is comparable to the Proofpoint product. Microsoft does include support, but not Premier support. The benefit of the product is developed and supported by the same company, the added benefit (that would otherwise be a hidden cost) is theoretically, less back-and-forth between companies in a support scenario. But Microsoft pricing actually edges out Proofpoint for 233 or fewer users (see the next paragraphs about Proofpoint). Proofpoint: For 250 users, Proofpoint edges out Microsoft by roughly \$.33/user/month, which for a large enterprise, over a longer period of time, could make a significant difference. But there is more to the story. In the first Proofpoint pricing bracket (1–250), at 233 users, the Proofpoint and Microsoft price are the same (\$5.00/user/month). For fewer than 233 users, the Microsoft price is less than that of Proofpoint.

Evaluation Experience

Table 3: Ease of Evaluation table

Office 365 ATP Plan 2	Proofpoint PRO+TAP	Notes
		Microsoft: Microsoft Office ATP Plan 2 design and business model is quite different, and Currently, there is no evaluation mode for Office 365 ATP where it doesn't impact real users. With no Office 365 ATP evaluation mode, there is nothing to compare to the Proofpoint product. Proofpoint: Due to the Proofpoint product design and business model, their evaluation process is very detailed, requiring extensive information from the customer or client company. For details, go to Evaluating Proofpoint TAP.

Dashboards and Reporting

Table 4: Dashboards and Reporting comparison table

Office 365 ATP Plan 2	Proofpoint Targeted Attack Protection (TAP)	Notes
Ease of Access and Use 	Ease of Access and Use 	There are two main elements to this comparison: the ease of accessing and using the dashboards and reporting and the effectiveness of the dashboards and reporting. These are examined separately here and are given separate star ratings. Ease of Access and Use: • Microsoft: The Microsoft UI uses a completely different approach (see Different Dashboard and Reporting Approach) than Proofpoint, making access and use more difficult. The approach does not have the uniformity and ease of their Proofpoint counterparts, requiring the user to go to an entirely different report when with Proofpoint, it's a drill-down or different view of tab of the same report. • Proofpoint: The dashboard and reports are thoughtfully designed and organized, making deep analysis within a report just a few clicks into the dashboard. Effectiveness of dashboards and reporting: • Microsoft: While Microsoft has a longer list of reports, Proofpoint includes report data akin to Microsoft, just organized differently (see prior ratings for ease of access and use). Microsoft does provide custom reports, but they lack an Effectiveness Report and other key reports that Proofpoint includes. (See Dashboards and Reporting for Both Products.) • Proofpoint: Proofpoint is more effective as a result of both dashboards and reports design and because they provide reports and views that Microsoft does not. However, they do not include custom reporting.
Effectiveness of Dashboards and Reporting 	Effectiveness of Dashboards and Reporting 	

Default Settings

Table 5: Advanced threat protection default settings comparison table

Office 365 ATP Plan 2	Proofpoint Targeted Attack Protection (TAP)	Notes
Ease of Changing Settings 	Ease of Changing Settings 	There are two main elements to this comparison: the ease of changing settings and the effectiveness of the default settings. These are examined separately here and are given separate star ratings. Ease of Changing Settings: • Microsoft: The Microsoft policy setting UI design is very easy to reach and get to each policy, but once within each policy, the approach differs from policy to policy. There's an opportunity for Microsoft to make the UI across all of the policies much more uniform. • Proofpoint: Distributed throughout the Proofpoint product, and the difficulty in finding, enabling, or configuring the settings, makes the process much more difficult for the administrator.
Effectiveness of Default Settings 	Effectiveness of Default Settings 	Effectiveness of default settings: • Microsoft: Microsoft errs on the side of caution, putting phishing and spam emails into the Junk Email folder by default. While this is good for false positives, it does create undue exposure from true positives. Proofpoint defaults don't seem to create enough of a negative user experience for them to change their approach (read on for more about Proofpoint). • Proofpoint: The Proofpoint approach to defaults and quarantining (see the Quarantine Experience section and the quarantine settings for both products throughout that section) are more extreme than Microsoft. For example, while Microsoft puts email in the Junk Email folders (for phishing and spam), Proofpoint puts them in a Quarantine subfolder.

Quarantine Experience

Table 6: Quarantine Experience comparison table

Office 365 ATP Plan 2	Proofpoint Targeted Attack Protection (TAP)	Notes
		Microsoft: The default behavior of ATP makes it easier for a user to access false positive emails and content (emails identified as threats that are not threats). But, that ease has a downside: real threats going to the user's Junk Email folder, too. Effectiveness outweighs ease of use in this case, since the purpose of the product is to provide security. Proofpoint: The default behavior of TAP errs on the side of caution, putting all emails that are a potential threat (including false positives) in quarantine. While that makes getting harmless emails from quarantine more difficult, that does not seem to be an issue as a use case, as Proofpoint provides the user with a view and access to what is in quarantine (depending on how restrictive the security administrator makes the Quarantine settings and Spam Detection Module settings).

Key Product Differences

This section focuses on the main differences in the products.

The fundamental differences with the products, plans, design, and approach are in the [Key Fundamentals of Both Products](#) section. The focus of this section is different, in that the key product differences detailed here are the result of surfacing differences from comparing the two products.

As a result, the focus is on the comparisons and user scenarios: pricing, evaluation experience, dashboards and reporting, default settings, and quarantine experience.

Table 7: Key product differences

Comparison	Office 365 ATP Plan 2	Proofpoint PRO+TAP
Pricing	Cost tipping point: The prices for both products are comparable. For less than 233 users, Microsoft product is less expensive. Price visibility: Microsoft is transparent with their pricing, posting it clearly on their site (on the See Pricing page).	Cost tipping point: The prices for both products are comparable. For more than 233 users, the Proofpoint product is less expensive. Price visibility: Proofpoint is not transparent with their pricing. It is not available on their site and can only be estimated from one of their account executives or partners.
Evaluation Experience	Evaluation process: Microsoft does not have an evaluation process that uses journaling (to mitigate impact to a production environment). Alternative: They do have a free trial for their Office 365 E5 plan which contains Office 365 ATP Plan 2, but that would need to be either set up with the production environment or with a separate domain and multiple accounts and an Exchange infrastructure would need to be created (like a test environment).	Evaluation process: Proofpoint has an evaluation process, but it is very detailed with many steps (see Evaluating Proofpoint PRO+TAP). Requirements: It requires that they obtain information from the prospective customer (number of email users and a 30-day email volume report) and they need the customer's Exchange administrator set up the Journal Rule and associated Send Connector in the Office 365 Exchange Admin Console.
Dashboards and Reporting	What they do not have that Proofpoint does: They do have customer reports and Proofpoint does not. What they have that Proofpoint does not: Microsoft has quite a few reports, but they do not have some key reports that Proofpoint does (such as effectiveness reports and login location reports). Usability: As described in Organizing and Grouping Reports and Ease of Accessing Dashboards and Reporting, the Microsoft design and approach adds complexity and clicks for accessing the dashboard and each report.	What they do not have that Microsoft does: They do not have custom reports. What they have the Microsoft does not: Effectiveness reports and login location reports. Usability: As described in Organizing and Grouping Reports and Ease of Accessing Dashboards and Reporting, the Proofpoint design and approach simplifies access and reduces the number of clicks for accessing the dashboard and each report.

Comparison	Office 365 ATP Plan 2	Proofpoint PRO+TAP
Default Settings	Ease of Changing Settings: This is much easier with ATP than with TAP. Microsoft does have some improvement opportunities for making the settings interface within each policy more uniform across their six policy pages. Effectiveness of default settings: One major difficulty with the Microsoft default settings is that they err on the side of making it easier on the user to access false positive emails, but as a result, put true positive emails (malicious emails) into the Junk Email folder when they should be moved to quarantine.	Ease of Changing Settings: This is more difficult with TAP than with ATP. Microsoft puts their six policies and settings together in one page. Finding and changing settings for ATP is not as centralized. Effectiveness of default settings: The Proofpoint defaults err on the side of caution. They quarantine by default. How difficult it is for a user to remove an email from quarantine depends on how restrictive the security administrator makes the Quarantine settings and Spam Detection Module settings).
Quarantine Experience	Quarantine default behavior: The default behavior of ATP makes it easier for a user to access false positive emails and content (emails identified as threats that are not threats). But, that ease has a downside: real threats going to the user's Junk Email folder, too. Effectiveness outweighs ease of use in this case, since the purpose of the product is to provide security.	Quarantine default behavior: The default behavior of TAP errs on the side of caution, putting all emails that are a potential threat (including false positives) in quarantine. (See the Quarantine Experience section and the quarantine settings for both products throughout that section.) While that makes getting harmless emails from quarantine more difficult, that does not seem to be an issue as a use case, as Proofpoint provides the user with a view and access to what is in quarantine (depending on how restrictive the security administrator makes the Quarantine settings and Spam Detection Module settings).

Pros/Cons

This section ladders up all of the detailed comparisons and user scenarios, comparison tables, and key product differences, to highlight the pros and cons (strengths and challenges) of both products.

Office 365 ATP Plan 2

Pros

- **Documentation:** Critical, but not analyzed deeply in this document, is the difference in product documentation. The Microsoft product information is extensive at <https://docs.microsoft.com>, which we link to throughout this comparison document. The Microsoft site is much easier to search and to quickly find what you're looking for.
- **Pricing:** The pricing is competitive with Proofpoint PRO+TAP. Plus, Microsoft is very transparent with their pricing.
- **Dashboards and Reporting:** Microsoft includes custom reporting and Proofpoint does not.
- **Default Settings: Ease of changing settings:** The Microsoft policy setting UI design is very easy to reach and get to each policy, but once within each policy, the approach differs from policy to policy.

Cons

- **Evaluation Experience:** Microsoft does not have an evaluation process that uses journaling (to mitigate impact to a production environment).
- **Dashboards and Reporting:** While Microsoft has a longer list of reports, Proofpoint includes report data akin to Microsoft, just organized differently (see prior ratings for ease of access and use). Microsoft does provide custom reports, but they lack an *Effectiveness Report* and other key reports that Proofpoint includes. (See [Dashboards and Reporting for Both Products](#).)
 - Proofpoint gathers reports in the dashboard with a drill-down and ladder-up approach, putting a lot of useful information in a single dashboard report, with the ability to click each element for more details.
 - The Microsoft tile approach (while showing an active thumbnail of the reports, requires clicking the tile to get to the actual report.
- **Default Settings: Ease of changing settings:** There's an opportunity for Microsoft to make the UI across all of the policies much more uniform. The following are a few examples:
 - **Default ATP Anti-Phishing policy settings:** A default policy is active/enabled, but not visible. You must click **Default policy** to view the default policy. (See [Default ATP Anti-Phishing Settings](#) for details.)
 - **Default ATP Safe Attachments policy settings:** There is no hidden enabled default policy. There is no protection enabled by default. Plus, if you want to create a policy, the UI is completely different (a plus sign instead of clicking **Create**). The user must create a policy. (See [Default ATP Safe Attachments Settings](#) for details.)
 - **Default ATP Safe Links policy settings:** For this policy, there is a default policy, and it's listed for **Policies that apply to the entire organization**. There is no default policy for specific recipients. (See [Default ATP Safe Links Settings](#) for details.)
 - **Default Anti-Spam policy settings:** For this policy, there is a default policy, but not in a list of policies. (See [Default Anti-Spam Settings](#) for details.)
 - **Default DKIM policy settings:** For this policy, there is a default policy in a list, but it is empty. (See [Default DKIM \(DomainKeys Identified Mail\) Settings](#) for details.)
 - **Default Anti-Malware policy settings:** For this policy, the default policy is listed and shown as enabled in a list, and to the right, that policy's settings are shown. (See [Default Anti-Malware Settings](#) for more details.)
- **Default Settings: Effectiveness of default settings:** One major difficulty with the Microsoft default settings is that they err on the side of making it easier on the user to access false positive emails, but as a result, put true positive emails (malicious emails) into the **Junk Email** folder when they should be moved to quarantine.
- **Quarantine default behavior:** The default behavior of ATP makes it easier for a user to access false positive emails and content (emails identified as threats that are not threats). But, that ease has a downside: real threats going to the user's **Junk Email** folder, too. Effectiveness outweighs ease of use in this case, since the purpose of the product is to provide security.

Proofpoint PRO+TAP

Pros

- **Pricing:** The pricing is competitive with Proofpoint PRO+TAP.
- **Evaluation Experience:** This is listed as a *Pro* for Proofpoint, because they do have an evaluation process. Though, due to the Proofpoint product design and business model, their evaluation process is very detailed, requiring extensive information from the customer or client company. For details, go to [Evaluating Proofpoint TAP](#).
- **Dashboards and Reporting:** The dashboard and report are thoughtfully designed and organized, making deep analysis within a report just a few clicks into the dashboard. Proofpoint is more effective as a result of both dashboards and reports design and because they provide reports and views that Microsoft does not.

Proofpoint gathers reports in the dashboard with a drill-down and ladder-up approach, putting a lot of useful information in a single dashboard report, with the ability to click each element for more details.

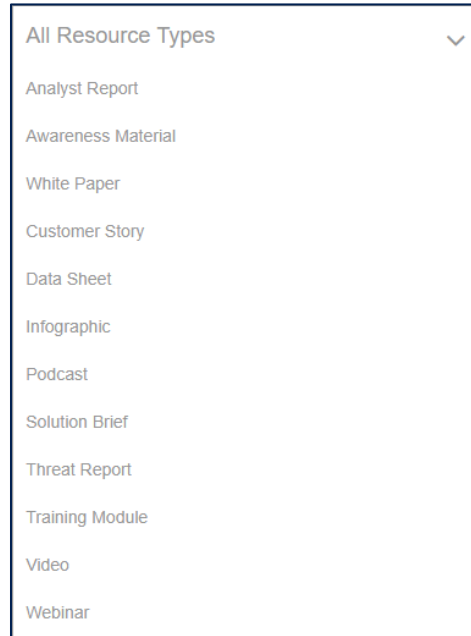
- **Default Settings: Effectiveness of default settings:** The Proofpoint defaults err on the side of caution. They quarantine by default. How difficult it is for a user to remove an email from quarantine depends on how restrictive the security administrator makes the [Quarantine](#) settings and [Spam Detection Module](#) settings).
- **Quarantine default behavior:** The default behavior of TAP errs on the side of caution, putting all emails that are a potential threat (including false positives) in quarantine. (See the [Quarantine Experience](#) section and the quarantine settings for both products throughout that section.)

While that makes getting harmless emails from quarantine more difficult, that does not seem to be an issue as a use case, as Proofpoint provides the user with a view and access to what is in quarantine (depending on how restrictive the security administrator makes the [Quarantine](#) settings and [Spam Detection Module](#) settings).

Cons

- **Documentation:** Critical, but not analyzed deeply in this document, is the difference in product documentation. Proofpoint documentation has some limitations.
 - **Communication and engagement model:** The Proofpoint communication model starts with contacting them for information or for a trial/POC product version (see [Evaluation Experience](#) for more details). While it is fairly easy and relatively quick to request information from the Proofpoint account executive, it is sometimes several days before you receive a response.
 - **Areas of their site:** Their site contains a combination of the following areas: [Resource Library](#), [Blogs](#), [Webinars](#), and their [Threat Center](#).

- **Resource Library:** Of those four, you can access product information from the [Resource Library](#) by using their search boxes, where you can perform a text search, narrow the results down by solution, and/or narrow them down by type. While the results are a variety of item types, such as the following:



- The Microsoft site is much easier to search and to quickly find what you're looking for.
- The Microsoft product information is extensive at <https://docs.microsoft.com>, which we link to throughout this comparison document.
- **Pricing:** Proofpoint is not transparent with their pricing. It is not available on their site and can only be estimated from one of their account executives or partners.
- **Dashboards and Reporting:** Proofpoint does not include custom reporting.
- **Default Settings: Ease of Changing Settings:** This is more difficult with TAP than with ATP. Microsoft puts their six policies and settings together in one page. Finding and changing settings for ATP is not as centralized.

Comparisons and User Scenarios

This section contains side-by-side comparisons of both products across the following features and user scenarios:

- Pricing
- Evaluation Experience
- Dashboards and Reporting
- Default Settings
- Quarantine Experience

About the Change in Focus for this Document

For completeness, this brief section describes the original scope and intent for this document, and how it organically changed. Originally, the document focus included *Evaluation Experience*, *Setup Experience*, *Performance*, *Default Settings*, *Dashboards*, and *Reporting*.

The factors in this organic change were:

- Needs for testing and evaluation
- Increased depth of product information discovery
- Issues with trial product availability and implementation

All of these factors led to the need to add some evaluation and comparison criteria, combine some, and remove others.

What was added:

- Pricing
- Quarantine Experience

What was combined:

- Dashboards
- Reporting

What was removed:

- Setup Experience
- Performance

Pricing

Comparison Table

Table 8: Pricing comparison table

Office 365 ATP Plan 2	Proofpoint PRO+ TAP	Notes
		Microsoft: Though higher, the pricing is comparable to the Proofpoint product. Microsoft does include support, but not Premier support. The benefit of the product is developed and supported by the same company, the added benefit (that would otherwise be a hidden cost) is theoretically, less back-and-forth between companies in a support scenario. But Microsoft pricing actually edges out Proofpoint for 233 or fewer users (see the next paragraphs about Proofpoint). Proofpoint: For 250 users, Proofpoint edges out Microsoft by roughly \$.33/user/month, which for a large enterprise, over a longer period of time, could make a significant difference. But there is more to the story. In the first Proofpoint pricing bracket (1–250), at 233 users, the Proofpoint and Microsoft price are the same (\$5.00/user/month). For fewer than 233 users, the Microsoft price is less than that of Proofpoint.

Office 365 ATP Plan 2

The pricing for all of the Microsoft products are on the [See Pricing](#) page. Specifically, the price for Office 365 ATP Plan 2 is in the following table.

Microsoft can make price discounts/reductions in competitive situations.

Support is included (can open a support ticket with desktop support), but not Premier support.

Table 9: Microsoft Office 365 ATP Plan 2 pricing

Price	Notes
\$5.00/user/month (annual commitment)	Includes all Office 365 ATP Plan 1 benefits and more. Includes: • Configuration, protection, and detection • Automation, investigation, remediation, and education

Proofpoint PRO+TAP

They do have other tiers than are listed here, but those tiers and pricing were not available to the author as of this writing. They are able to get pretty aggressive when it comes to discounts when more solutions are being added.

The pricing for Proofpoint PRO+TAP is listed in the following table.

Table 10: Proofpoint PRO+TAP pricing

Price	Notes
\$14,000 (estimated, after tax)	For the 1–250 user price bracket. Is for a one-year contract. Support is included. Unclear if updates are included.
\$22,000 (estimated, after tax)	For the 250+ user price bracket. Is for a one-year contract. Support is included. Unclear if updates are included.



Note: Calculating from the Proofpoint price brackets to match the Microsoft pricing approach, the two products' pricing align very closely:

Proofpoint \$14,000 for 1–250 users = \$4.67/user/month (minimum; for fewer users, it increases)

The upper end of the next price bracket was not available, so it is unknown how much the \$/user/month would be for that bracket.

Evaluation Experience

This section compares how easy it is to evaluate each product.

Comparison Table

Table 11: Ease of Evaluation table

Office 365 ATP Plan 2	Proofpoint PRO+TAP	Notes
		Microsoft: Microsoft Office ATP Plan 2 design and business model is quite different, and Currently, there is no evaluation mode for Office 365 ATP where it doesn't impact real users. With no Office 365 ATP evaluation mode, there is nothing to compare to the Proofpoint product. Proofpoint: Due to the Proofpoint product design and business model, their evaluation process is very detailed, requiring extensive information from the customer or client company. For details, go to Evaluating Proofpoint TAP.

Evaluating Office 365 ATP Plan 2

Currently, there is no evaluation mode for Office 365 ATP where it doesn't impact real users. (Proofpoint uses a journaling approach.) With no Office 365 ATP evaluation mode, there is nothing to compare to the Proofpoint product.

Evaluating Proofpoint PRO+TAP

The evaluation process for Proofpoint TAP required the following steps. There are multiple ways of initiating contact with Proofpoint, and regardless of the approach, you achieve the same result. For completeness, both initial processes are listed, followed by how the process continues.



Note: In the [Appendix](#), there is a copy of the main steps in this section, but instead of the screen captures, the actual emails are imbedded.

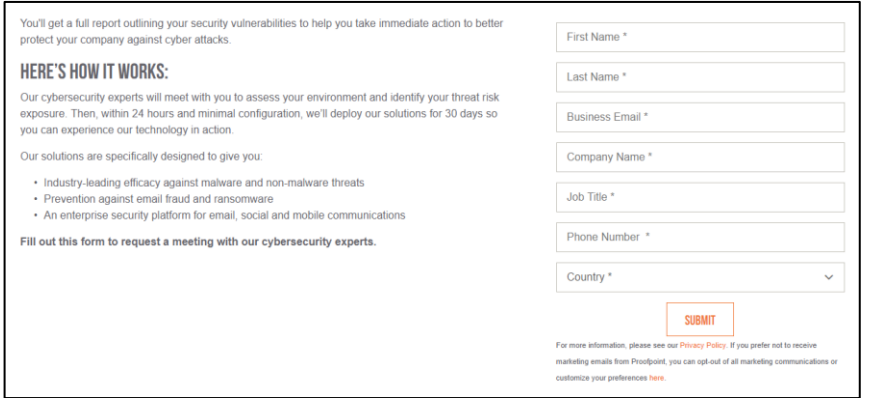
Initiating contact with Proofpoint: Approach 1 of 2

Table 12: Evaluation steps (approach 1 of 2) table

Step	Details
1. Go to the Proofpoint Targeted Attack Protection page of the Proofpoint site.	
2. In the lower right-hand corner of the browser window, click the bot icon.	
3. The bot will ask, Welcome to Proofpoint! How can we help you today? Click Product Information .	
4. The bot will state, Please provide your email below to allow us to better assist you. Enter your email address.	

Initiating contact with Proofpoint: Approach 2 of 2

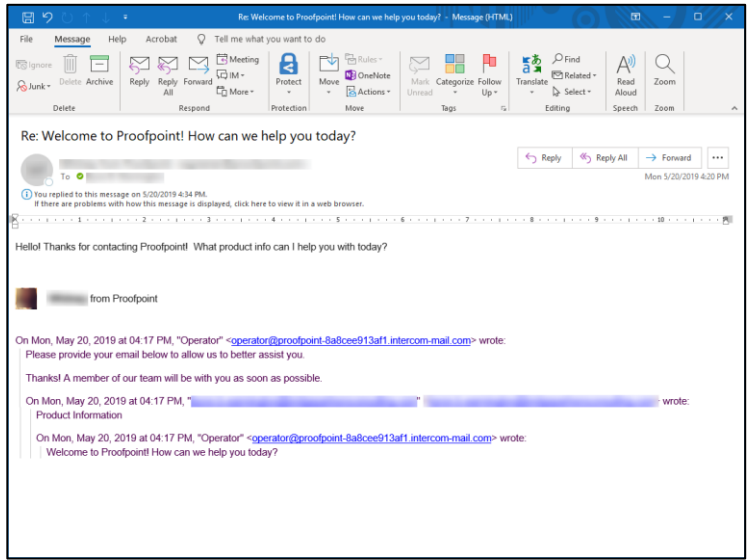
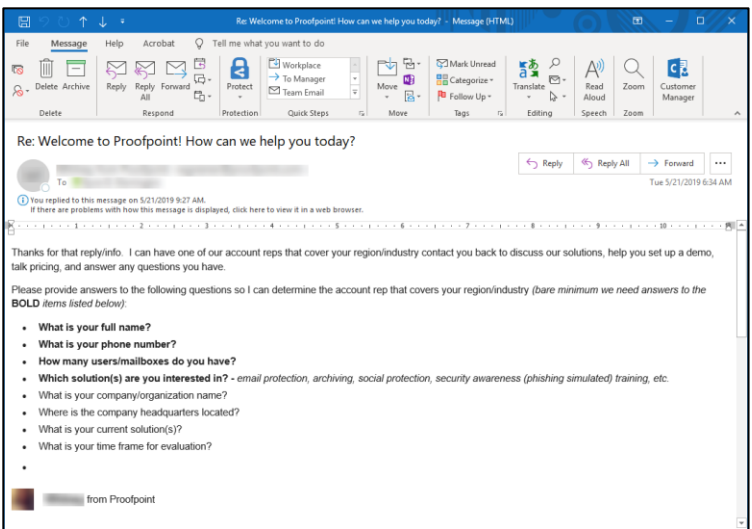
Table 13: Evaluation steps (approach 2 of 2) table

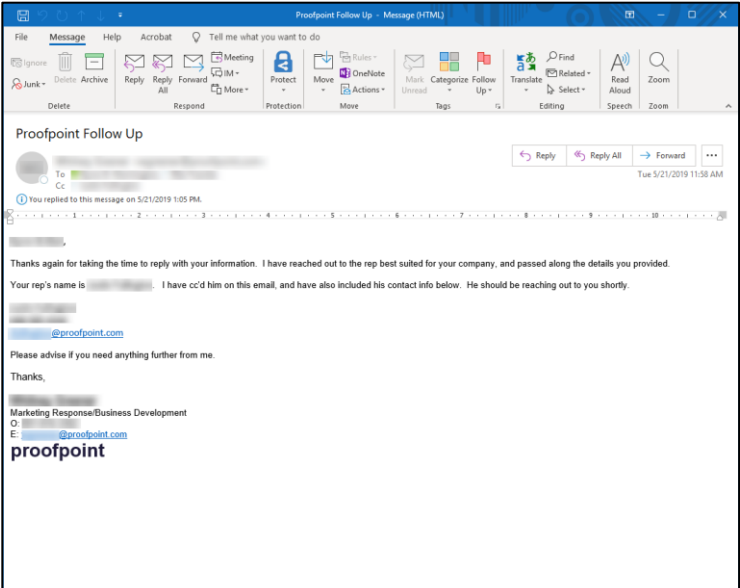
Step	Details
1. Go to the Proofpoint Targeted Attack Protection page of the Proofpoint site.	
2. Near the bottom of the page, click GET PROTECTED to start a free trial.	
3. Enter the required (fields with asterisks) information, then.	
4. Click SUBMIT .	

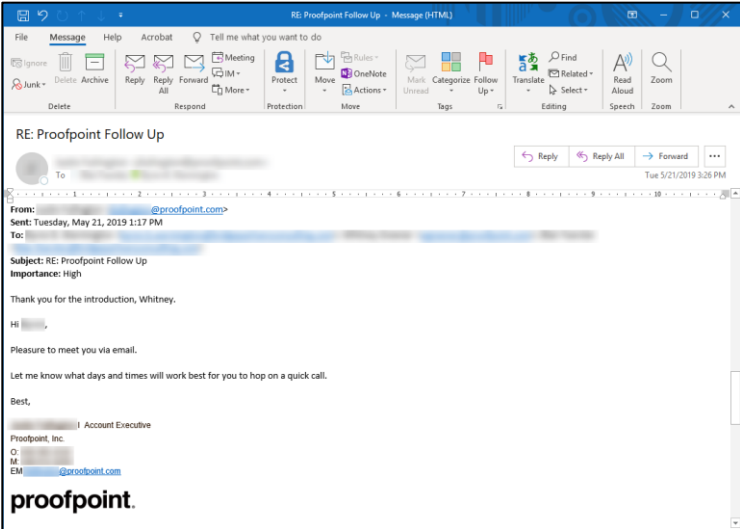
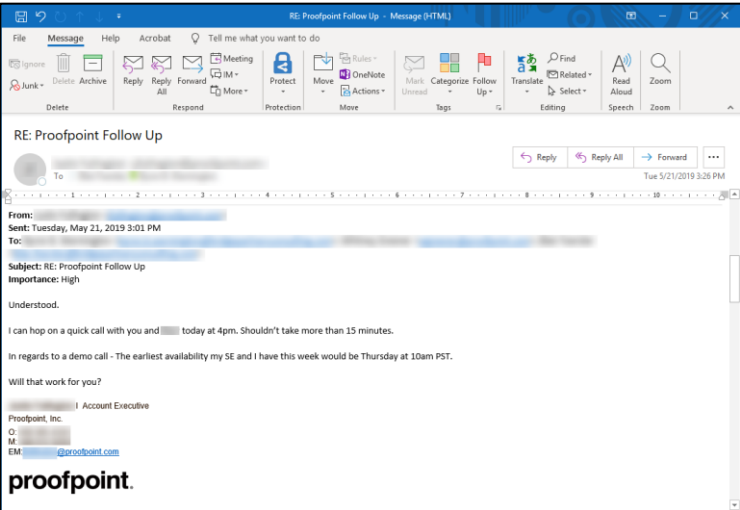
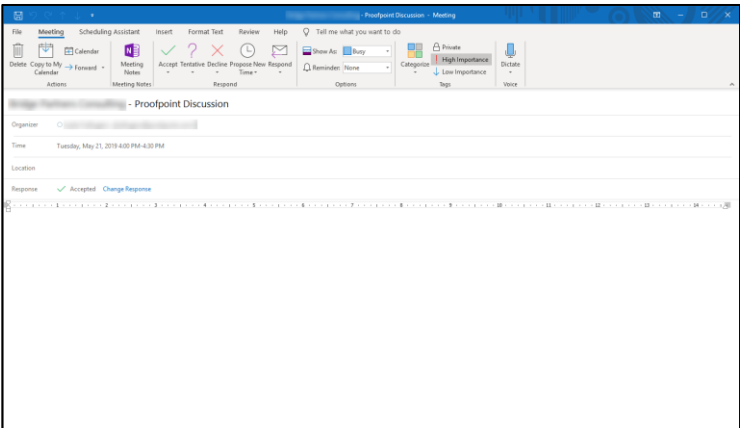
Communicating with Proofpoint: The process continues

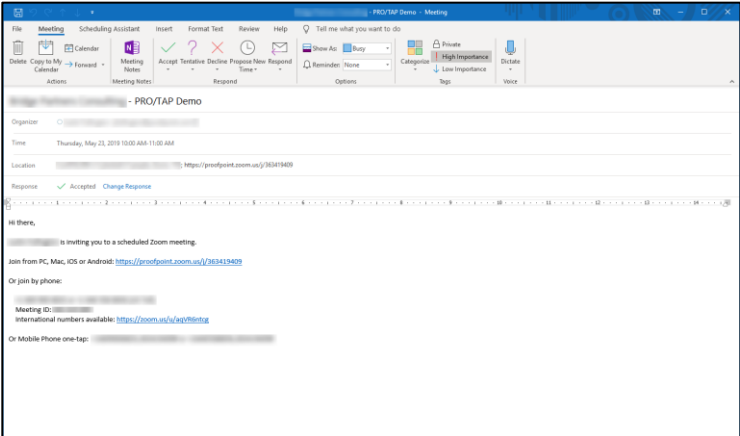
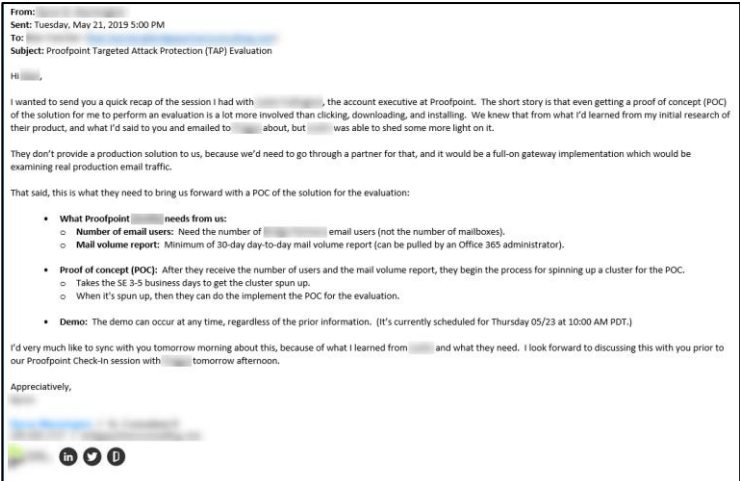
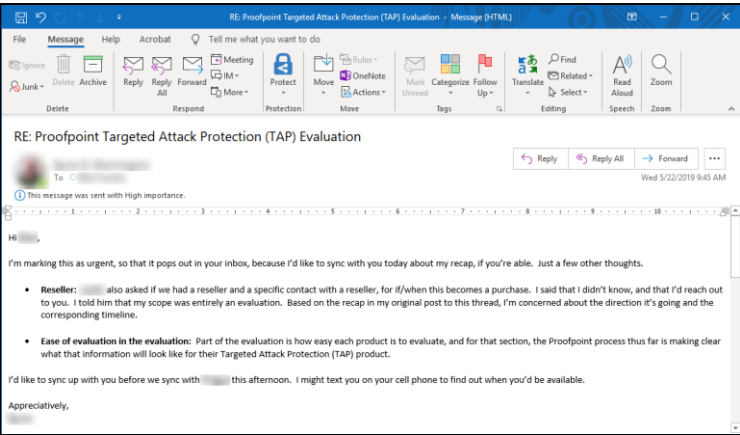
Regardless of which of the two methods you use, the process continues with the following steps.

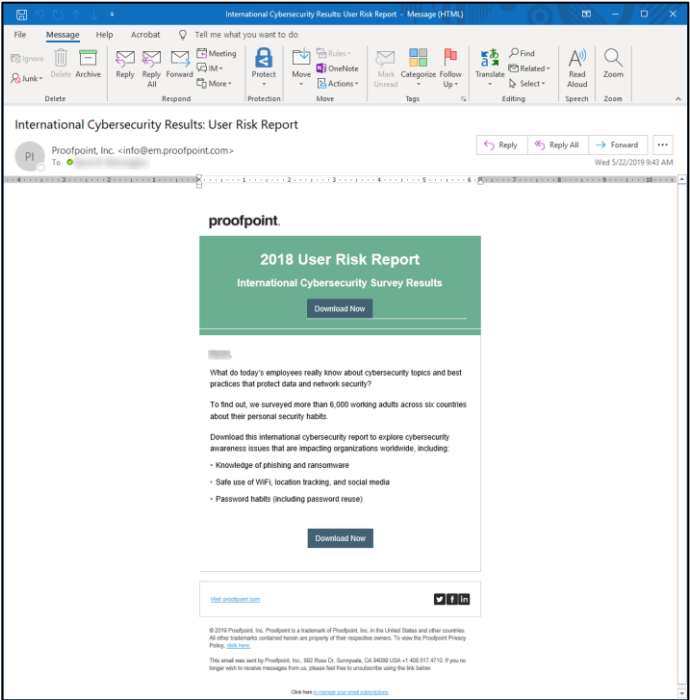
Table 14: Evaluation steps (continued process) table

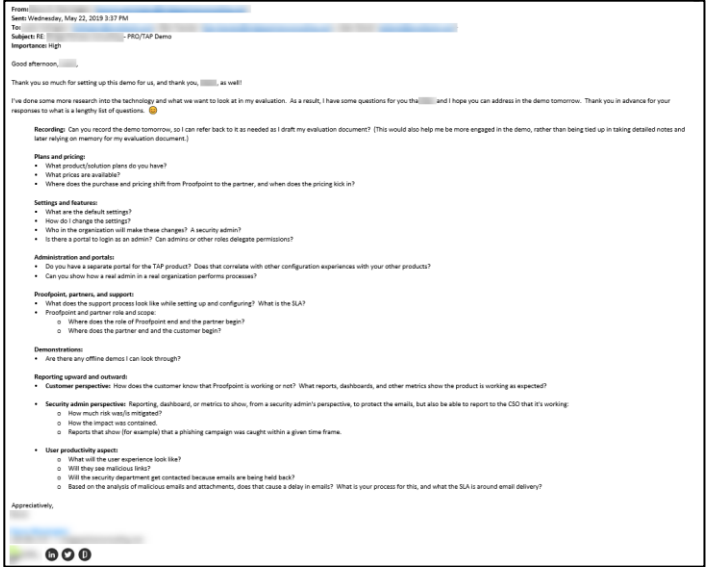
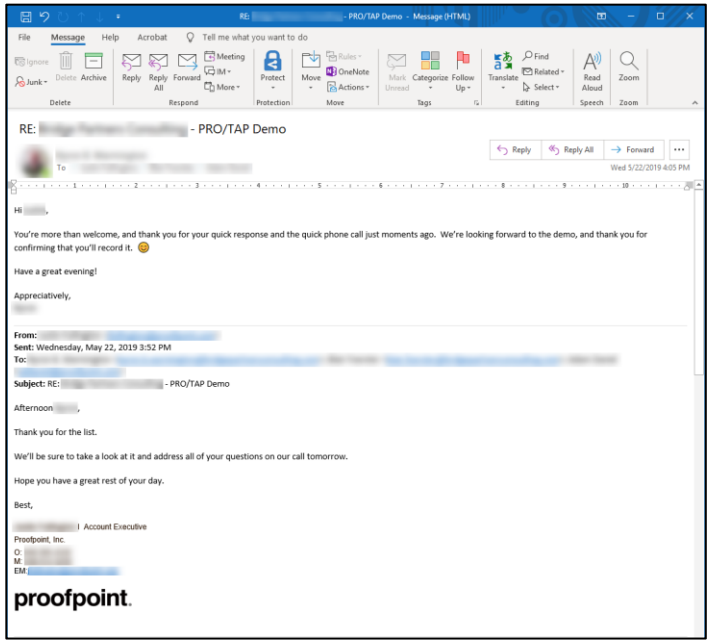
Step	Details
5. You will receive an email from a Proofpoint contact.	
6. Respond, describing your request to evaluate Proofpoint TAP.	
7. The account rep will respond to you with a list of questions so that they can route you to the appropriate account rep for your region and industry.	
8. The Proofpoint contact might follow up with additional questions (such as the those listed in the Details column). Respond to the questions.	Are you wanting to evaluate to be able to understand it for resell? Or are you wanting to purchase internally? Are you an MSP ?

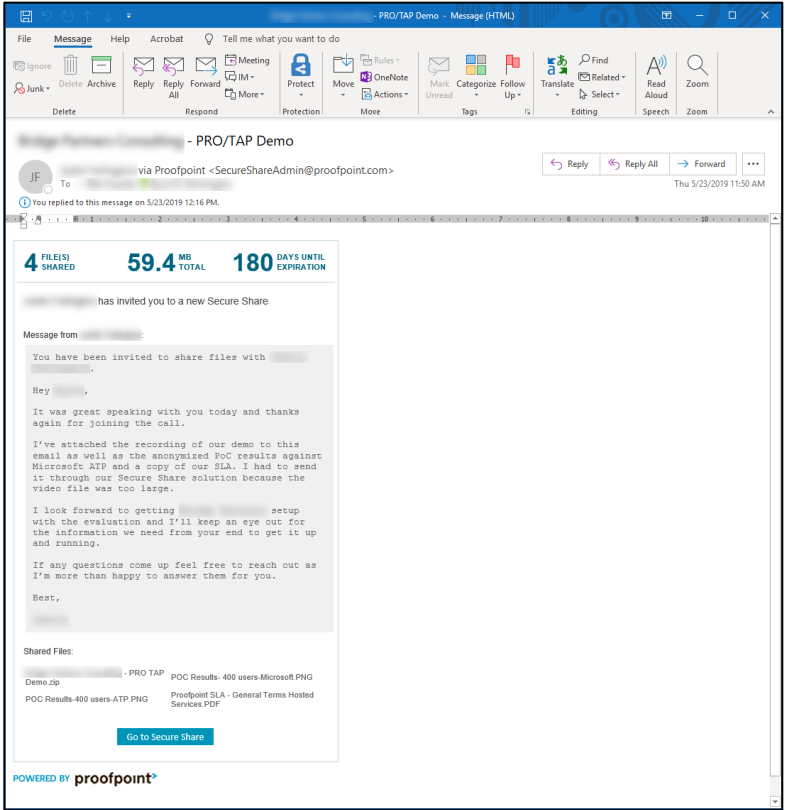
Step	Details
9. The Proofpoint contact will then respond to you, and then they will create a separate email thread, introducing you to the account rep.	 The screenshot shows an Outlook email interface. The title bar reads 'Proofpoint Follow Up - Message (HTML)'. The ribbon includes 'File', 'Message', 'Help', and 'Acrobat'. The 'Message' tab is active, showing options like 'Ignore', 'Delete', 'Archive', 'Reply', 'Reply All', 'Forward', 'Forward All', 'More', 'Protect', 'Move', 'OneNote', 'Mark', 'Categorize', 'Follow Up', 'Translate', 'Find', 'Read Aloud', 'Zoom', and 'Speech'. The email content is as follows: Proofpoint Follow Up To: [Redacted] Cc: [Redacted] You replied to this message on 5/21/2019 1:05 PM. [Redacted] Thanks again for taking the time to reply with your information. I have reached out to the rep best suited for your company, and passed along the details you provided. Your rep's name is [Redacted]. I have cc'd him on this email, and have also included his contact info below. He should be reaching out to you shortly. [Redacted] @proofpoint.com Please advise if you need anything further from me. Thanks, [Redacted] Marketing Response/Business Development O: [Redacted] E: [Redacted] proofpoint

Step	Details
10. The account rep will email you to ask about scheduling a brief 30-minute discovery call and to schedule a 60-minute demonstration.	 
11. If you respond that you'd like to have both a discovery call and a demonstration, the account rep will schedule the discovery call.	

Step	Details
12. Then, the account rep will schedule and send you an invitation to the demonstration, using Zoom. The demonstration will include you, the account rep, and a Proofpoint SE.	
13. In the discovery call, the account rep will answer your questions and will also ask you for some very specific information. Without that information, they will not create a proof of concept (POC) environment for you to try out and evaluate their product. The information they need is: • Number of email users: Need the number of the customer company's email users (not the number of mailboxes). • Mail volume report: Minimum of 30-day day-to-day mail volume report (can be pulled by an Office 365 administrator). • Action request: They usually ask this later in the process, but they will ask that the customer's Exchange administrator be prepared to set up the Journal Rule and associated Send Connector in the Office 365 Exchange Admin Console. If you ask about pricing, they will ask if you have a preferred reseller.	 

Step	Details
14. Then (typically the next day), you'll receive an email offering you the opportunity to download their 2018 User Risk Report .	

Step	Details
15. In this instance, we sent them questions prior to the demonstration, which they gleefully accepted. (as well as anytime later). <u>You can ask them to record the demonstration and share the recording. Also ask them for their SLA.</u>	 
16. They performed the demonstration, introduced by the account rep, then the SE demonstrated the product and responded to the emailed questions, then the account rep finished up the session. They were diligent about answering all of the questions and invited us to send more or reach out to them, if needed.	See the Proofpoint PRO+TAP References section for the link to the <i>Recorded Proofpoint Demonstration</i> and other supporting materials.)

Step	Details
17. The account rep will send you a recording of the demonstration if you requested it. In this instance, we requested their SLA, which they also sent. All files that the account rep sends to you will be through their secure portal.	 PRO/TAP Demo - Message (HTML) File Message Help Acrobat Tell me what you want to do Ignore Delete Archive Reply Reply All Forward More Protect Move OneNote Mark Unread Categorize Follow Up Translate Find Related Select Read Aloud Zoom PRO/TAP Demo via Proofpoint <SecureShareAdmin@proofpoint.com> You replied to this message on 5/23/2019 12:16 PM. 4 FILE(S) SHARED 59.4 MB TOTAL 180 DAYS UNTIL EXPIRATION has invited you to a new Secure Share Message from [Redacted]: You have been invited to share files with [Redacted]. Hey [Redacted], It was great speaking with you today and thanks again for joining the call. I've attached the recording of our demo to this email as well as the anonymized PoC results against Microsoft ATP and a copy of our SLA. I had to send it through our Secure Share solution because the video file was too large. I look forward to getting [Redacted] setup with the evaluation and I'll keep an eye out for the information we need from your end to get it up and running. If any questions come up feel free to reach out as I'm more than happy to answer them for you. Best, [Redacted] Shared Files: PRO TAP POC Results- 400 users-Microsoft.PNG Demo.zip POC Results-400 users-ATP.PNG Proofpoint SLA - General Terms Hosted Services.PDF Go to Secure Share POWERED BY proofpoint  Proofpoint SLA - General Terms Hosted

Step	Details																											
18. In the demonstration, the account manager will offer to send you the following information. If you say yes, they will send these two items with anything else you might have requested: Advanced Threat Detection Summary Unknown, Zero-hour Threats Reputation only check is ineffective <table><thead><tr><th>Threat Messages</th><th>25 Day Results</th><th>Annualized</th></tr></thead><tbody><tr><td>Messages with Malicious URIs (phishing & malware)</td><td>1,634</td><td>23,564</td></tr><tr><td>Messages with Malicious Attachments (phishing & malware)</td><td>46</td><td>703</td></tr><tr><td>Total Messages</td><td>1,629</td><td>23,785</td></tr></tbody></table> Numbers don't tell the full story. Some messages are common malware threat types (e.g., both malicious URIs and a malicious attachment). These messages are considered low threat risk. • Data representing January 26 to February 20, 2018 • Messages that passed Microsoft and identified malicious by Proofpoint • 1,518 (93.2%) were proactively detected and would be blocked in production • 73 had URL's that would have been rewritten and delivered • 24 contained attachments that would have been delivered, but cleaned up by TRAP Advanced Threat Results Message Quarantine Hundreds of Credential Phish Thousands of Spam/Adult & Grey mail <table><thead><tr><th>Message Type (Inbound)</th><th>25 Day Results</th><th>Annualized</th></tr></thead><tbody><tr><td>Malware + Phish</td><td>279</td><td>4,073</td></tr><tr><td>Spam + Adult</td><td>7,496</td><td>109,471</td></tr><tr><td>Bulk (Grey Mail)</td><td>127,246</td><td>1,857,792</td></tr><tr><td>Total Messages</td><td>135,021</td><td>1,971,336</td></tr></tbody></table> • Data representing January 26 to February 20, 2018 • Messages that passed Microsoft and identified as unwanted by Proofpoint • Separate quarantine folders allow for granular policy control	Threat Messages	25 Day Results	Annualized	Messages with Malicious URIs (phishing & malware)	1,634	23,564	Messages with Malicious Attachments (phishing & malware)	46	703	Total Messages	1,629	23,785	Message Type (Inbound)	25 Day Results	Annualized	Malware + Phish	279	4,073	Spam + Adult	7,496	109,471	Bulk (Grey Mail)	127,246	1,857,792	Total Messages	135,021	1,971,336	
Threat Messages	25 Day Results	Annualized																										
Messages with Malicious URIs (phishing & malware)	1,634	23,564																										
Messages with Malicious Attachments (phishing & malware)	46	703																										
Total Messages	1,629	23,785																										
Message Type (Inbound)	25 Day Results	Annualized																										
Malware + Phish	279	4,073																										
Spam + Adult	7,496	109,471																										
Bulk (Grey Mail)	127,246	1,857,792																										
Total Messages	135,021	1,971,336																										
19. The account rep will follow up after the demonstration, asking if they can reach out to a reseller on your behalf, to get you pricing information.	RE: PRO/TAP Demo - Message (HTML) File Message Help Acrobat Tell me what you want to do Ignore Delete Archive Reply Reply All Forward More Protect Move OneNote Mark Unread Categorize Follow Up Tags Editing Select Speech Zoom RE: PRO/TAP Demo To: [Redacted] This message was sent with High Importance. You're very welcome, [Redacted]. We try to be as quick as possible! Would you like for me to connect you with a reseller so we can work on some pricing? [Redacted] Account Executive Proofpoint, Inc. O: [Redacted] M: [Redacted] EM: [Redacted] proofpoint. From: [Redacted] Sent: Thursday, May 23, 2019 12:16 PM To: [Redacted] Subject: RE: PRO/TAP Demo Hi [Redacted], Wow, that was fast! Thank you and [Redacted] so much for the demo this morning, and for the additional files you'd mentioned in the demo. All of this will definitely be helpful with the my evaluation, which I'm still in the early stages of drafting. Thank you for your patience and support while I gather information and develop the understanding I need to draft my document. Before I responded to you, I wanted to make sure that I could successfully download and open all of the files, and I sure could. Your secure portal is fast! There was a lot for me to consume from the demo, so after I look through my notes, the recording, and the files some more (like we'd talked about this morning) I'll likely have more questions from my original list, and might even have a few more. Thank you for being a resource for me as I work through some of those details; I look forward to following up with you about them when I get to that point. Appreciatively, [Redacted]																											

Dashboards and Reporting

This section compares the dashboards and reporting of each product.

- How do the dashboards and reports compare between the two products?
- What tools/reports are available for automated and manual threat investigation? What does that process look like?
- How can customers see if the product is working and effective? What reports are available, how often are they delivered?
- How can users and security administrators report suspicious content?

Comparison Table

Table 15: Dashboards and Reporting comparison table

Office 365 ATP Plan 2	Proofpoint Targeted Attack Protection (TAP)	Notes
Ease of Access and Use 	Ease of Access and Use 	There are two main elements to this comparison: the ease of accessing and using the dashboards and reporting and the effectiveness of the dashboards and reporting. These are examined separately here and are given separate star ratings. Ease of Access and Use: • Microsoft: The Microsoft UI uses a completely different approach (see Different Dashboard and Reporting Approach) than Proofpoint, making access and use more difficult. The approach does not have the uniformity and ease of their Proofpoint counterparts, requiring the user to go to an entirely different report when with Proofpoint, it's a drill-down or different view of tab of the same report. • Proofpoint: The dashboard and reports are thoughtfully designed and organized, making deep analysis within a report just a few clicks into the dashboard. Effectiveness of dashboards and reporting: • Microsoft: While Microsoft has a longer list of reports, Proofpoint includes report data akin to Microsoft, just organized differently (see prior ratings for ease of access and use). Microsoft does provide custom reports, but they lack an Effectiveness Report and other key reports that Proofpoint includes. (See Dashboards and Reporting for Both Products.) • Proofpoint: Proofpoint is more effective as a result of both dashboards and reports design and because they provide reports and views that Microsoft does not. However, they do not include custom reporting.
Effectiveness of Dashboards and Reporting 	Effectiveness of Dashboards and Reporting 	

Different Dashboard and Reporting Approach

The two products have vastly different approaches to their dashboards and reporting, which is detailed further in this section. In short, Microsoft uses a provides fewer initial selections (**Dashboard** and **Explorer**) so the user must click down further to find data that's available higher up in the Proofpoint UI. These differences and more are detailed further in this section.

Organizing and Grouping Reports

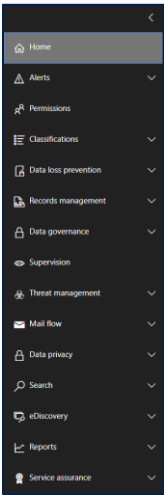
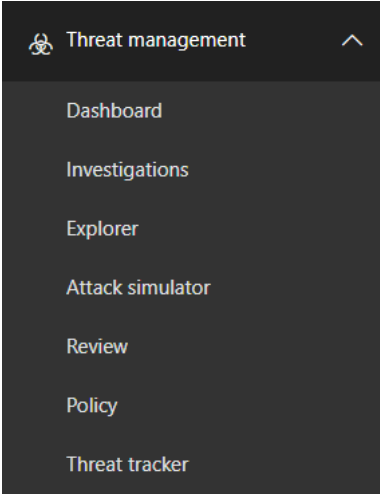
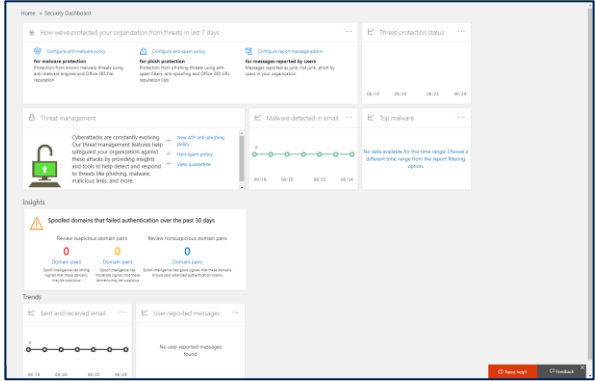
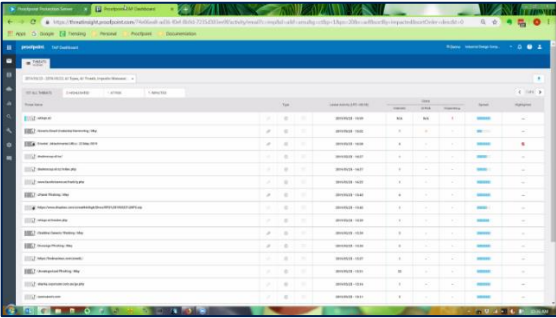
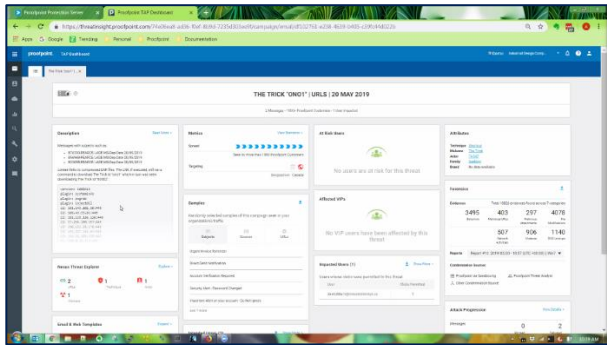
Office 365 ATP: The Microsoft tile approach (while showing an active thumbnail of the reports, requires clicking the tile to get to the actual report.

Proofpoint TAP: Proofpoint gathers reports in the dashboard with a drill-down and ladder-up approach, putting a lot of useful information in a single dashboard report, with the ability to click each element for more details. In some cases (as shown in [Dashboards and Reporting for Both Products](#)) one Proofpoint TAP report shows what's in four Microsoft reports.

Ease of Accessing Dashboards and Reporting

Here you can clearly see the difference in the first two clicks, and how the two products structure and group the reporting, and present the data.

Table 16: Accessing and using the reports for both products

No Clicks	First Click	Second Click
Microsoft 	Microsoft 	Microsoft Not yet viewing an actual report. 
Proofpoint Already in the dashboard. 	Proofpoint Already in a report (Threat list). 	Proofpoint Inside the next level of report, able to do deeper analysis, or filtering for further details. 

Dashboards and Reporting for Both Products

The dashboard and reporting are extensive for both products, so the following table lists both dashboards and reports for both products, to help highlight the similarities and differences. Each type of dashboard or report type is listed, along with the ones provided by each product, to show which ones align with which, and where there are no reports that align. For further details, go to the [Threats](#), [Effectiveness Report](#), [Login Locations](#), [People-Centric Report](#), and [Custom Reports](#) sections.

Table 17: Dashboards and reports for both products

Type of Report or Dashboard	Office 365 ATP Plan 2	Proofpoint PRO+TAP	Notes
Threats	Threat Protection Status report	Threats (Threat list and Forensic Report)	Microsoft offers multiple separate threat reports, while Proofpoint provides the ability to see multiple views and different information within the same reports (Threat list and Forensic Report). See further detail in the Threats section.
	ATP File Types report		
	ATP Message Disposition report		
	Threat Explorer (and real-time detections)		
	Email security reports		
Effectiveness Report	None. Custom Reports only.	Effectiveness Report	As of this writing, there are no Microsoft ATP effectiveness reports. The custom reports (created by the user using PowerShell) are a start at effectiveness reports.
Login Locations	None	Login Locations	There appears to be no Microsoft analog to the Proofpoint <i>Login Locations</i> report.

Type of Report or Dashboard	Office 365 ATP Plan 2	Proofpoint PRO+ TAP	Notes
People-Centric Report (Opportunity for Security and Awareness Training)	Top Senders and Recipients report	People report	Microsoft: The Microsoft <i>Top Senders and Recipients</i> report gives the ability to use the Show data for list to select whether to view data for top senders, receivers, spam recipients, and malware recipients. You can also see who received malware that was detected by Exchange Online Protection. Proofpoint: The Proofpoint <i>People</i> report of All Users, All Threats, and Any Exposure details specific learning opportunities for users and user groups.
Custom Reports	ATP Safe Links URL trace (This is a report you generate by using PowerShell.)	No custom report, but the <i>Effectiveness Report</i> contains this kind of information.	Microsoft: In the combination of these three custom reports, Microsoft assembles something akin to an effectiveness report (like the Proofpoint <i>Effectiveness Report</i>). Proofpoint: As of this writing, there is no capability for generating custom reports. However, the Proofpoint TAP product has this kind of information in the <i>Effectiveness Report</i>.
	EOP and ATP results (This is a custom report you generate by using PowerShell.)	No custom report, but the <i>Effectiveness Report</i> contains this information.	
	EOP and ATP detections (This is a custom report you generate by using PowerShell.)	No custom report, but the <i>Effectiveness Report</i> contains this information.	

Automated and Manual Threat Investigation

Within dashboards and reporting, what automated and manual threat investigation tools do both products have? Neither product identifies threats before they occur, though Proofpoint does have a separate product, *Threat Response Auto-Pull (TRAP)* to contain, quarantine, and clean up malicious email before users have a chance to open it.

So, starting with the existence of the threat, threat investigation (as approached by these products) is part of a cyclic process.

The following table details this functionality for both products.

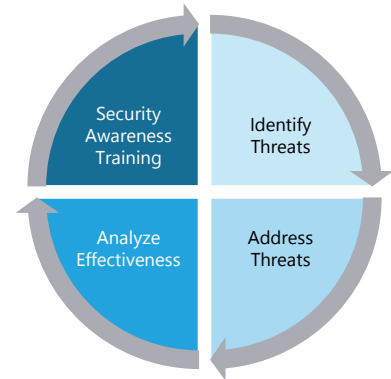


Table 18: Automated and manual threat investigation and hunting

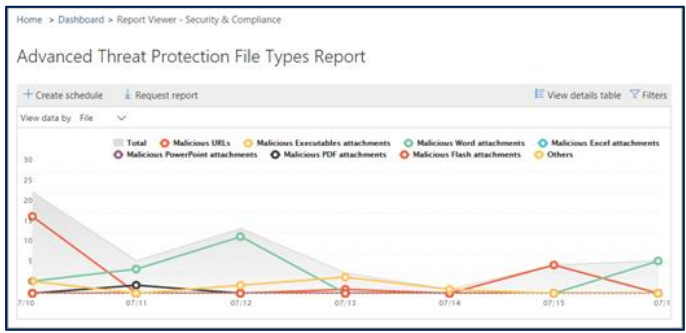
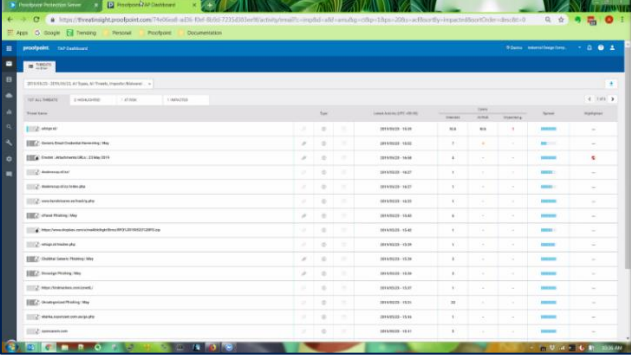
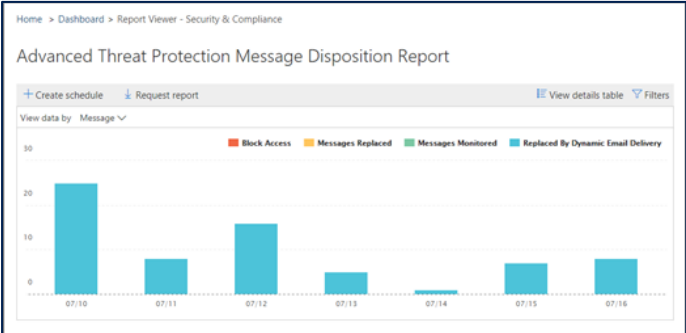
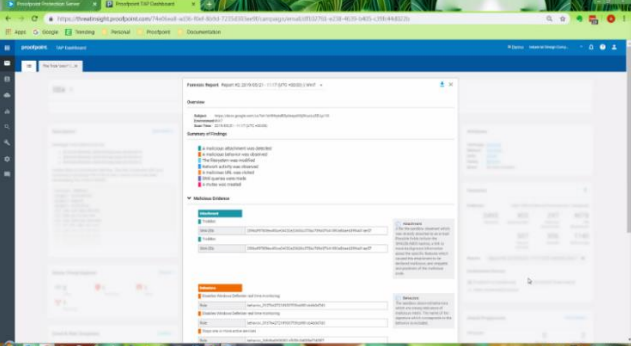
Stage in the Cycle	Office 365 ATP Plan 2	Proofpoint PRO+TAP	Notes
Identify Threats	• Threat Protection Status report • ATP File Types report • ATP Message Disposition report • Threat Explorer (and real-time detections) • Email security reports	• Login Locations • Threat • Forensic Report	Automatic / Manual: Both product dashboards and reporting gather threat data in real time, automatically. Microsoft: A variety of reports to view specific threat types. Proofpoint: Small number of reports providing the ability to view multiple alert types at once and can click down into more detail.
Address Threats	• Pulsing • Sandboxing • Quarantining	• Pulsing • Sandboxing • Quarantining	Automatic / Manual: Both product dashboards provide threat information, with settings that automatically address known threats based on the product settings (see Default Settings). Microsoft: Ability to use the existing reports to take action on specific threats. Sandboxing and quarantining are used, but differently than Proofpoint. See Quarantine Experience for more details. Proofpoint: Using the reports to identify and take action on pulsing URL threats and uses sandboxing and quarantining. See Quarantine Experience for more details.
Analyze Effectiveness	None	Effectiveness Reports	Automatic / Manual: Both product dashboards provide threat information, with settings that automatically address known threats based on the product settings (see Default Settings), while also providing the capability to manually address threats. Microsoft: As mentioned, Microsoft has no pre-built effectiveness reports, but has custom reports that are a start at them. Proofpoint: Using Proofpoint's Effectiveness reports, you can validate the impact of the product. For further information, see Effectiveness Reports.

Threats

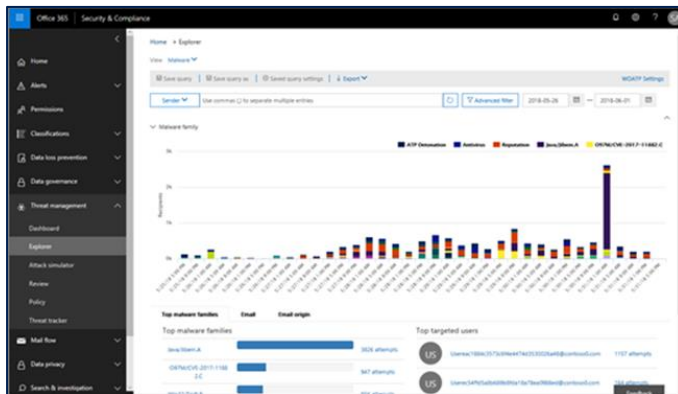
The following is a side-by-side comparison table of the threat reports for both products.

Microsoft offers multiple separate threat reports, while Proofpoint provides the ability to see multiple views and different information within the same reports (Threat list and Forensic Report).

Table 19: Threat dashboards and reports for both products

Office 365 ATP Plan 2	Proofpoint PRO+TAP
Threat Protection Status report 	Threats (Threat list and Forensic Report) The first view in Proofpoint TAP is the THREATS tab, listing all the threats discovered by TAP. Within that tab are four other tabs or views: • ALL THREATS • HIGHLIGHTED • AT RISK • IMPACTED Inside and to the left of each tab label is the number of items in each category.
ATP File Types report 	Threat List 
ATP Message Disposition report 	Forensic Report (image 1 of 3) 

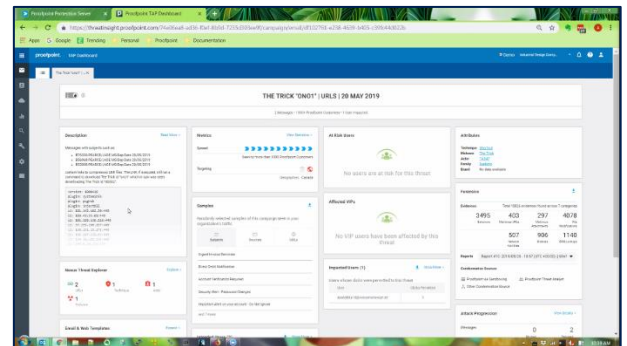
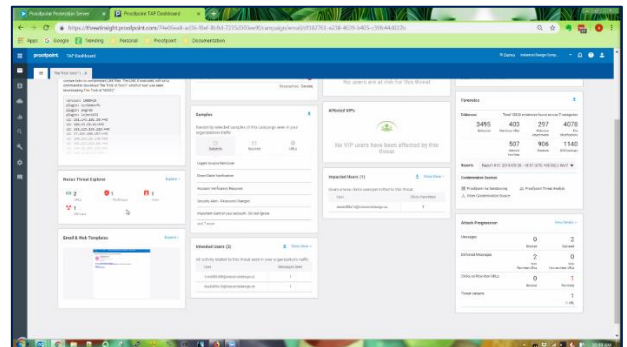
Office 365 ATP Plan 2

Threat Explorer (and real-time detections)**Email security reports**

There are nine email security reports:

- [Encryption report \(NEW!\)](#)
- [Threat Protection Status report](#)
- [Malware Detections report](#)
- [Top Malware report](#)
- [Top Senders and Recipients report](#)
- [Spoof Detections report](#)
- [Spam Detections report](#)
- [Sent and received email report](#)
- [User-reported messages report](#)

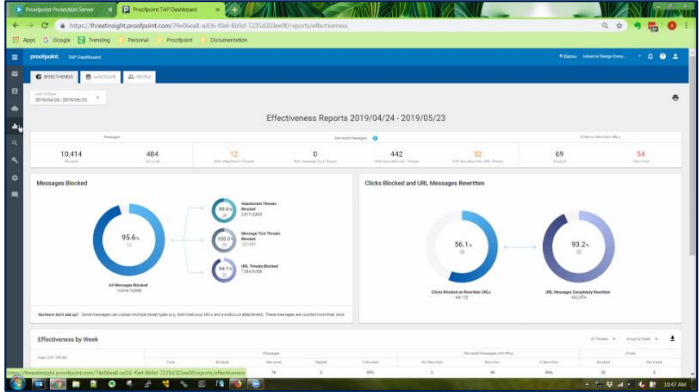
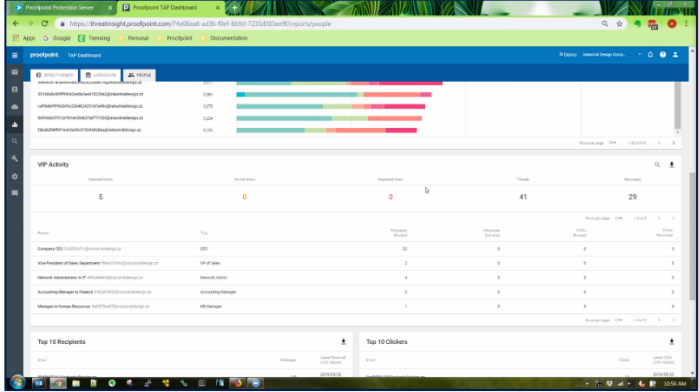
Proofpoint PRO+TAP

Forensic Report (image 2 of 3)**Forensic Report (image 3 of 3)**

Effectiveness Report

The following table shows and describes the effectiveness reports for both products.

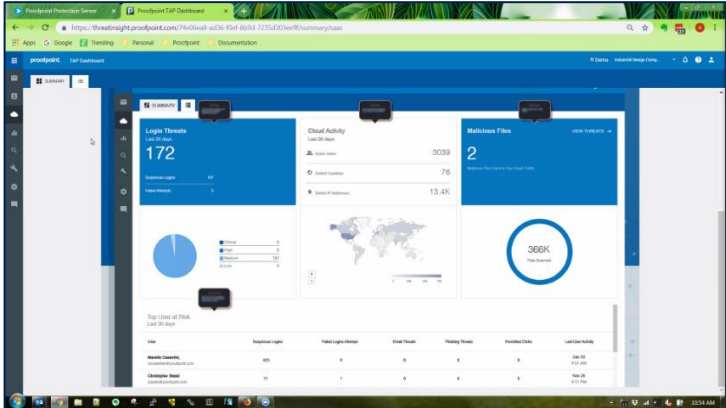
Table 20: Effectiveness reporting

Microsoft Office 365 ATP	Proofpoint TAP
As of this writing, there are no Office 365 ATP effectiveness reports. There are Custom Reports (see Custom Reports section). In the combination of the three custom reports, Microsoft assembles something akin to an effectiveness report (like the Proofpoint <i>Effectiveness Report</i>).	Effectiveness Reports tabs: EFFECTIVENESS, LANDSCAPE, and PEOPLE. Examples: EFFECTIVENESS Includes data and charts for information including (but not limited to) messages blocked and clicks blocked and URL messages rewritten. Also includes effectiveness by week.  PEOPLE: People-centric view. 

Login Locations

The following table shows and describes the login locations reports for both products.

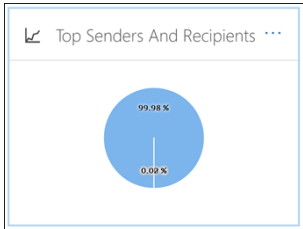
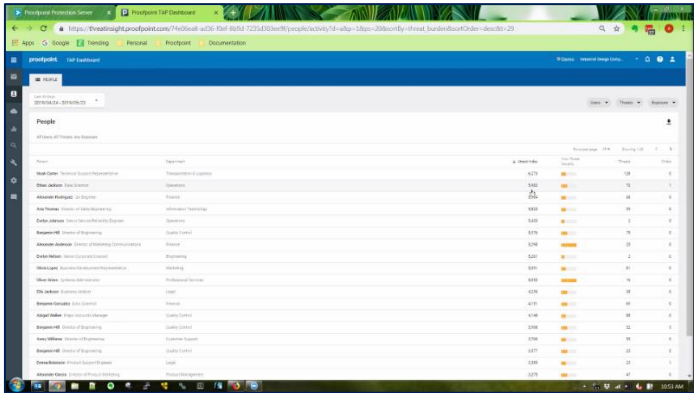
Table 21: Login locations reporting

Microsoft Office 365 ATP	Proofpoint TAP
As of this writing, there are no Office 365 ATP Login locations reports.	Login locations: Shows unusual login locations, too-fast-to-travel instances, excessive login attempts and failures, and too many connections from unknown or unusual IP addresses. For further details and context, see this Proofpoint blog entry titled Cyber Attacks: Visibility, Insight & Action - Part 3 of 3.  The screenshot displays the Proofpoint TAP dashboard with various security metrics. Key elements include: Login Threats: A blue box showing 172 threats, with a sub-section for 'Top Users at Risk'. Cloud Activity: A box showing 3039 events, 79 blocked attempts, and 13.4K blocked IP addresses, accompanied by a world map. Malicious Files: A box showing 2 malicious files and a 366K file count. Table: A table with columns: User, Suspicious Logins, Failed Logins, Email Threats, Phishing Threats, Suspicious Files, and Last Seen Activity. It lists users like 'Brenda Connelly' and 'Christopher Allen'.

People-Centric Report (Opportunity for Security and Awareness Training)

The following table shows and describes the people-centric reports for both products.

Table 22: People-centric reporting (Opportunity for Security and Awareness Training)

Microsoft Office 365 ATP	Proofpoint TAP
The Microsoft Top Senders and Recipients report gives the ability to use the Show data for list to select whether to view data for top senders, receivers, spam recipients, and malware recipients. You can also see who received malware that was detected by Exchange Online Protection. Top Senders and Recipients  Home > Dashboard > Report Viewer - Security & Compliance Top senders and recipients Show data for: Top Spam Recipients (dropdown menu open showing: Top Mail Senders, Top Mail Recipients, Top Spam Recipients, Top Malware Recipients, Top Malware Recipients (ATP))	The Proofpoint <i>People</i> report of All Users, All Threats, and Any Exposure details information showing security and awareness learning opportunities for users and user groups. 

Custom Reports

The following table shows and describes the custom reports for both products.

Table 23: Custom reporting

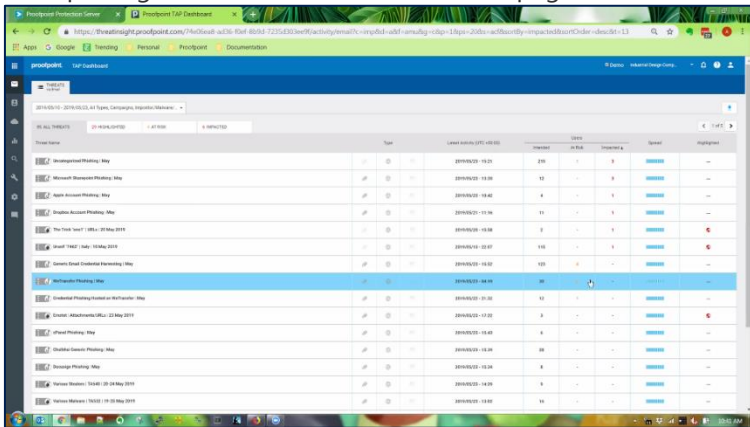
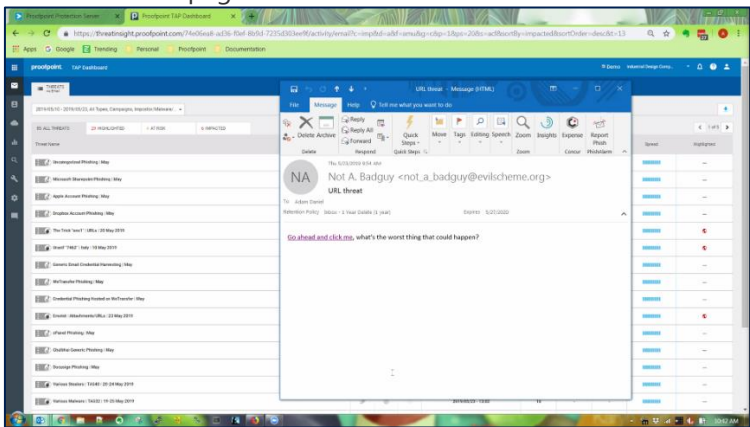
Microsoft Office 365 ATP	Proofpoint TAP
ATP Safe Links URL trace (This is a report you generate by using PowerShell.) EOP and ATP results (This is a custom report you generate by using PowerShell.) EOP and ATP detections (This is a custom report you generate by using PowerShell.)	No custom report, but the <i>Effectiveness Report</i> contains this information.

Pulsing and Sandboxing

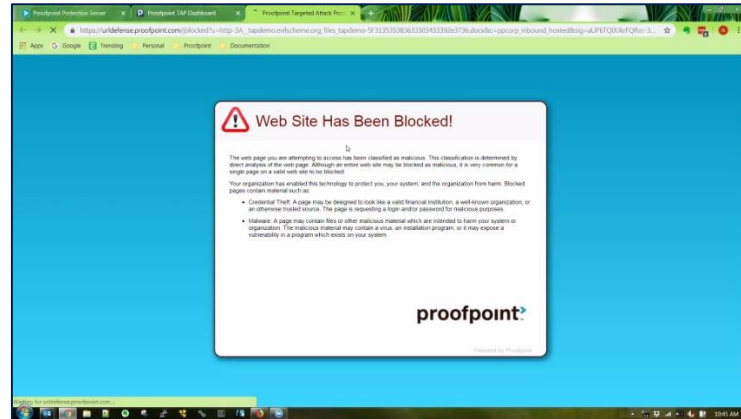
Pulsing and sandboxing are two concepts that are helpful to understand about security and threat detection, as well as how both products use them. First here is what those two terms mean:

- **Pulsing:** Pulsing is a type of attack in which a malicious email is sent with a URL, but that URL itself is harmless. Typically, that URL would pass threat detection. What happens next (and why it's called *pulsing*) is that the attacker takes a second step and weaponizes the site that the URL points to.
- **Sandboxing:** Often used in combination with detonation (sandboxing and detonation), this term refers to taking malicious content (such as email and/or attachments) and putting them in a safe location (the sandbox) where they can be observed and analyzed, and even opened. Opening or using the malicious content in the sandbox is called *detonation*.

The following table contrasts the pulsing and sandboxing behavior of both products.

Pulsing and Sandboxing	Microsoft Office 365 ATP Plan 2	Proofpoint PRO+TAP
Pulsing	Resolution of pulsing attacks is available to all Exchange Online Protection (EOP) customers. They call the feature Zero Hour Auto Purge (ZAP). For more details view the Microsoft Zero-hour auto purge - protection against spam and malware article.	Example: 1. A pulsing email is found on the Threats page.  2. The security administrator opens the email from the entry on the Threats page. 

3. The admin clicks the link on the pulsing email hyperlink, which is blocked.

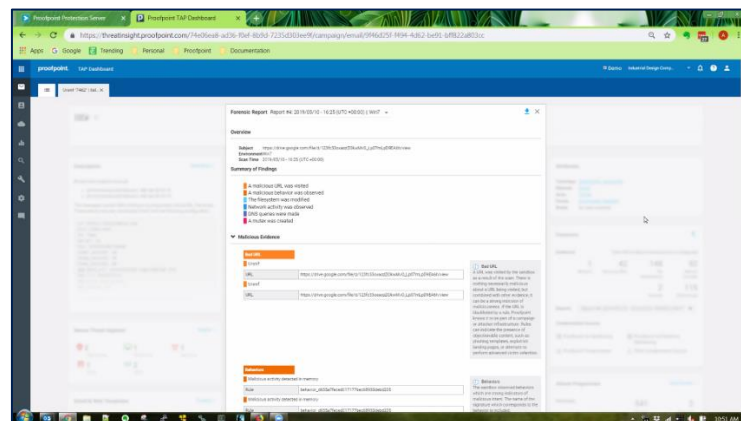
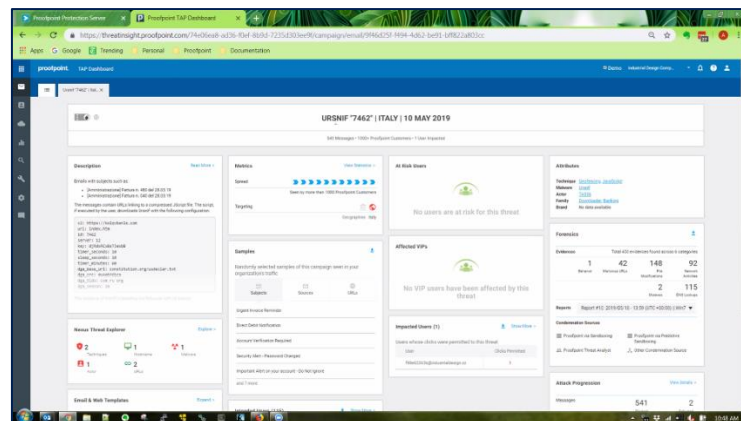


Sandboxing and Detonation

Microsoft uses sandboxing and detonation to isolate and analyze malicious content.

Proofpoint TAP sandboxes and allows detonation in both the prior pulsing example, and also in the following example of a malicious website.

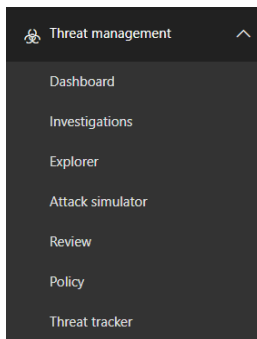
Proofpoint sandboxes the content of web sites. Not many products are doing that (as stated by their SE in a product demo).



Dashboards and Reporting of Office 365 ATP Plan 2

The Office 365 ATP dashboards and reporting (as you will also see with Proofpoint PRO+TAP) are rolled into the same user interface (UI). They are discussed in some detail at [View reports for Office 365 Advanced Threat Protection](#).

The dashboards and reporting are available through the **Threat Management** selections in the left navigation pane.



The reports included in Office 365 ATP Plan 2 are listed in the following table and are accessed from the **Dashboard** and **Explorer** selections under **Threat Management**.

Table 24: Dashboards and reporting for Office 365 ATP Plan 2

Report	Details
Threat Protection Status report	The Threat Protection Status report is a single view that brings together information about malicious content and malicious email detected and blocked by Exchange Online Protection (EOP) and Office 365 ATP .
ATP File Types report	The ATP File Types report shows you the type of files detected as malicious by ATP Safe Attachments .
ATP Message Disposition report	The ATP Message Disposition report shows you the actions that were taken for email messages that were detected as having malicious content.
Threat Explorer (and real-time detections)	Office 365 ATP Plan 2 customers have Explorer ; Office 365 ATP Plan 1 customers have real-time detections .
Email security reports	Such as a Top Senders and Recipients report, a Spoof Mail report, and a Spam Detections report. For further details, go to the View email security reports in the Security & Compliance Center article.
ATP Safe Links URL trace (This is a report you generate by using PowerShell.)	This report shows the results of ATP Safe Links actions over the past seven (7) days. Get-UrlTrace cmdlet reference
EOP and ATP results (This is a custom report you generate by using PowerShell.)	This report contains information, such as Domain, Date, Event Type, Direction, Action, and Message Count. Get-MailTrafficATPReport cmdlet reference
EOP and ATP detections (This is a custom report you generate by using PowerShell.)	This report contains details about malicious files or URLs, phishing attempts, impersonation, and other potential threats in email or files. Get-MailDetailATPReport cmdlet reference

Dashboards and Reporting of Proofpoint PRO+TAP

The Proofpoint TAP dashboards and reports contain multiple views and features. The following table summarizes a sampling of usage scenarios for each report type detailed in the prior section, to lead into the next part of this section that goes into detail about the dashboard used for accessing these reports.

Proofpoint Dashboard and Reporting Usage Scenarios

Table 25: Sampling of dashboards and reporting usage scenarios for Proofpoint PRO+TAP

Dashboard Reporting Feature	Usage Scenarios
Threat list	Forensic report
	Pulsing phishing email
	Sandboxing
Effectiveness report	Using Proofpoint's Effectiveness reports, you can validate the impact of the product.
Login locations	Shows unusual login locations, too-fast-to-travel instances, excessive login attempts and failures, and too many connections from unknown or unusual IP addresses.
People-centric reporting (Opportunity for Security and Awareness Training)	Using the Proofpoint <i>People</i> report of All Users , All Threats , and Any Exposure details specific learning opportunities for users and user groups.

Proofpoint TAP Dashboard

The Proofpoint TAP dashboard is a web-based graphical dashboard providing data at organizational, threat, and user levels, to help prioritize and act on alerts. It displays detailed forensic information on individual threats and campaigns in real time.

Along the left side of the dashboard are icons or hyperlinked images to select different areas of the dashboard.

Table 26: Areas within the Proofpoint TAP Dashboard

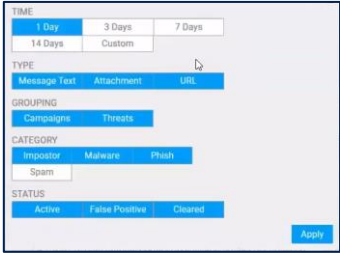
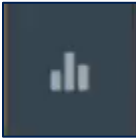
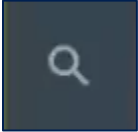
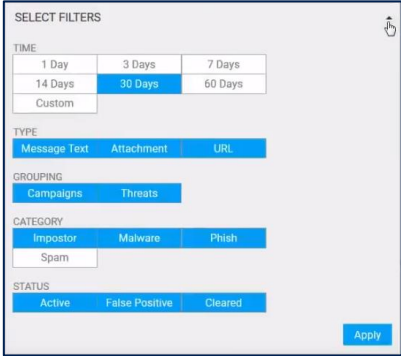
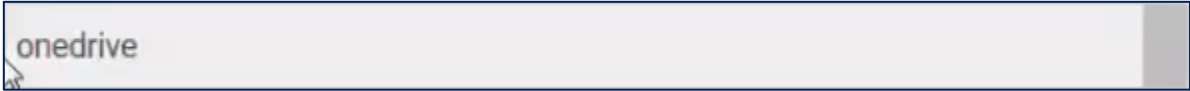
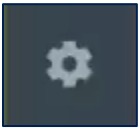
Image	Dashboard and Reporting Information
	Threats via email: Identifies and displays threats which might affect your organization. You can filter the results displayed by using the filter box.  Threats are divided into the following tabs: ALL THREATS, HIGHLIGHTED, AT RISK, or IMPACTED.
	Reports: A statistical overview of TAP effectiveness over a period of time. Reports are divided into EFFECTIVENESS, LANDSCAPE, or ORGANIZATION. A drop-down filter provides the ability to select a date range of up to one year with a default of 30 days.  Reports can be printed or downloaded as a CSV file.

Image	Dashboard and Reporting Information
	Search: To find individual threats and campaigns, based on criteria you specify in the filter and/or the search box.  
	Tools: Can be used in conjunction with the URL Defense service. The single tab (URL DECODER) is for the URL Decoder, which allows you to translate a rewritten link to the original link.
	Settings: Can perform various site-wide configuration tasks. • PRIVILEGES: To specify which users can access the Threat Insight dashboard and select their privilege level. • CUSTOM BLOCKLIST: Customer-defined set of URLs which are blocked. • CONNECTED APPLICATIONS: To define sets of credentials used to authenticate to the Proofpoint APIs. • ORGANIZATION: ○ To define which verticals (industries) your organization participates in. ○ Customize the block page. (The block page is the page the users see then they access a URL on the CUSTOM BLOCKLIST.) ○ Define VIP users in your organizations, to quickly identify threat activity associated with certain individuals. Threats can then appear on the landing page with a red VIP icon, indicating the threat needs immediate attention.

Default Settings

This section compares the approach to advanced threat protection default settings of each product, and where possible, compares the settings themselves.

Describing and differentiating the default settings of both products is important for two main reasons: differing out-of-the-box (OOB) default functionality and additional configuration.

- **Differing OOB default functionality:** Different solutions provide different default settings resulting in differing OOB default functionality. To match what one product does OOB usually requires additional configuration in a comparable product.
- **Additional configuration:** While one product might come with service and support to soften the impact of additional configuration, other products do not, or they do at additional cost, but either way, that is an additional consideration.
- **Result:** So, there is a resulting need (and time and effort/labor cost) for having to configure one product and not another. In short, seeing the difference helps to compare the configuration and customization needs of one product compared to others.

How the Information was Gathered

For the Microsoft product, the default setting information was manually gathered one-by-one by using screen captures of both a shared tenant and a new trial version of an Office 365 E5 tenant.

For the Proofpoint product, default settings were harvested from the *PoD Proofpoint Administration Guide*.

Comparison Table

Table 27: Advanced threat protection default settings comparison table

Office 365 ATP Plan 2	Proofpoint Targeted Attack Protection (TAP)	Notes
Ease of Changing Settings 	Ease of Changing Settings 	There are two main elements to this comparison: the ease of changing settings and the effectiveness of the default settings. These are examined separately here and are given separate star ratings. Ease of Changing Settings: • Microsoft: The Microsoft policy setting UI design is very easy to reach and get to each policy, but once within each policy, the approach differs from policy to policy. There's an opportunity for Microsoft to make the UI across all of the policies much more uniform. • Proofpoint: Distributed throughout the Proofpoint product, and the difficulty in finding, enabling, or configuring the settings, makes the process much more difficult for the administrator. Effectiveness of default settings: • Microsoft: Microsoft errs on the side of caution, putting phishing and spam emails into the Junk Email folder by default. While this is good for false positives, it does create undue exposure from true positives. Proofpoint defaults don't seem to create enough of a negative user experience for them to change their approach (read on for more about Proofpoint). • Proofpoint: The Proofpoint approach to defaults and quarantining (see the Quarantine Experience section and the quarantine settings for both products throughout this section) are more extreme than Microsoft. For example, while Microsoft puts email in the Junk Email folders (for phishing and spam), Proofpoint puts them in a Quarantine subfolder.
Effectiveness of Default Settings 	Effectiveness of Default Settings 	

Default Settings for Both Products

Each of the two products have a completely different approach to their product design and implementation (see the [Both Products](#) section for details).

As a result, viewing and changing each product advanced threat protection default settings is a completely different experience and process. So, while it is possible to compare some settings in parallel, it is not possible for all.

This section lists default settings for both products, and a separate comparison table for those that can be compared in parallel.

Microsoft Approach

Viewing default settings for Office 365 ATP Plan 2: Microsoft lists the settings in their **Policy** feature (click **Threat Management**, then click **Policy**).

Proofpoint Approach

Viewing default settings for Proofpoint PRO+TAP: Use step-by-step processes for opening each of the following features:

- Quarantine
- Spam Detection module
- Virus Protection module
- Zero-Hour Anti-Virus module
- Targeted Attack Protection

Alignment of Comparable Settings

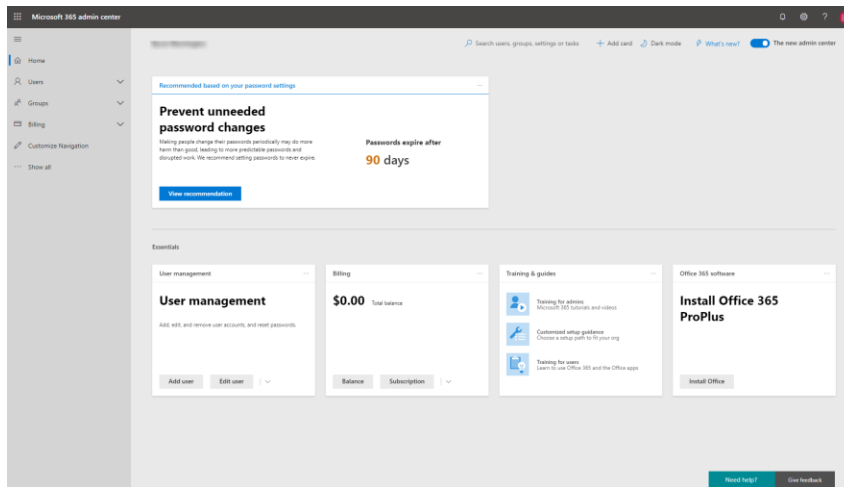
The following table shows how the two products' policies and setting interfaces align, where each category is in each of the products' user interface.

Table 28: Advanced threat protection default settings alignment table

Category	Microsoft ATP Policy	Proofpoint TAP Module
Anti-phishing	ATP anti-phishing	Spam Detection Module
Attachments	ATP safe attachments	Targeted Attack Protection Module
Links	ATP safe links	Targeted Attack Protection Module
Spam	Anti-spam	Spam Detection Module
DKIM (DomainKeys Identified Mail)	DKIM (DomainKeys Identified Mail)	Email Authentication Module
Anti-malware	Anti-malware	Spam Detection Module

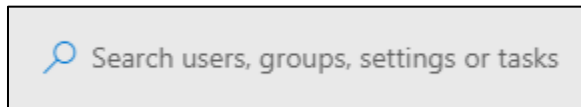
Default Settings of Office 365 ATP Plan 2

To open Office 365 ATP, for an existing Office 365 subscription go to <https://portal.microsoft.com> and sign in. The **Microsoft 365 admin center** will open.



There are two ways to get to Office 365 Security and Compliance: (A) Search or (B) Go directly to the URL.

- A. Search: In the **Search users, groups, settings, or task** box, enter **Security & Compliance**.

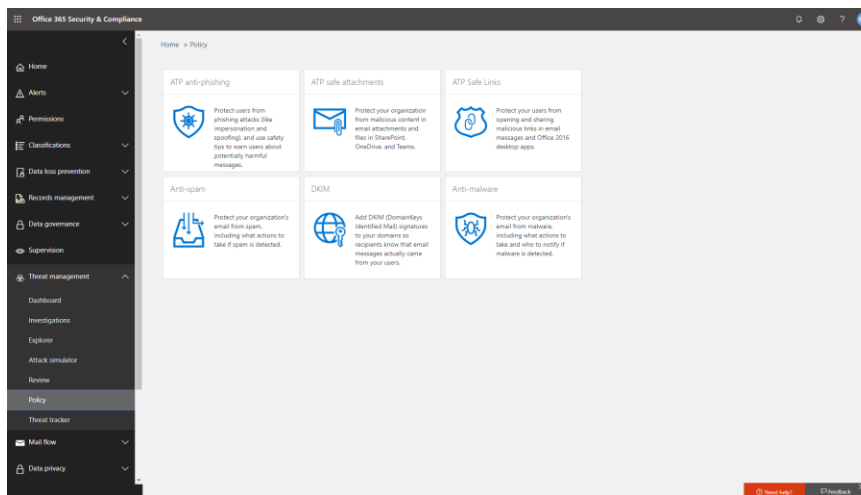


In the resulting list, click **Compliance admin center**.

- B. Or, instead of the search, go directly to <https://protection.office.com/homepage>.

The default settings are within the policies. To view them, click **Threat management**, then click **Policy**.

Figure 2: Microsoft Office 365 ATP Policy page



Policies

There are six policies, detailed in the following table.

Policy	Thumbnail	Description
ATP anti-phishing	ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.
ATP safe attachments	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.
ATP safe links	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.	Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam	Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	Protect your organization's email from spam, including what actions to take if spam is detected.
DKIM (DomainKeys Identified Mail)	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.
Anti-malware	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

Policy Settings

Within each policy are the following settings.



Note: In the following tables, if it was unclear from the source information what the default setting was (see [How the Information was Gathered](#)), the correspond cells in the **Default Setting** column are empty.

Table 29: Office 365 ATP: All ATP settings

Policy	Setting Category	Setting
ATP anti-phishing		Name
		Priority
		Status
		Last modified
	Policy setting	Applied to If the recipient is <specified domain>
	Impersonation	Users to protect
		Protect all domains I own
		Protect specified domains
		Action > User impersonation
		Action > Domain impersonation
		Safety tips > User impersonation
		Safety tips > Domain impersonation
		Safety tips > Unusual characters
		Mailbox intelligence
		Mailbox intelligence > Protection
		Mailbox intelligence > Action
	Spoof	Enable antispoofting protection
	Advanced settings	Action
		Advanced phishing thresholds
ATP safe attachments	New safe attachments policy	Turn on ATP for SharePoint, OneDrive, and Microsoft Teams
		ENABLED
		NAME
		PRIORITY
		Description
		Safe attachments unknown malware response
		Enable redirect

Policy	Setting Category	Setting
		Apply the above selection if malware scanning for attachments times out or error occurs.
		Applied to: If the message: Is sent to <email address>
ATP safe links	Policies that apply to the entire organization	Condition
		Except if the message: <exception>
		Name:
	Policies that apply to specific recipients	Do not track when users click safe links:
		Do not let users click through safe links to original URL:
		Applied to: Office 2016 on Windows
		ENABLED
		Name
		Description
		PRIORITY
		Priority: Relative priority
		Select the action for unknown potentially malicious URLs in messages.
		Use safe attachments to scan downloadable content.
		Apply save links to email messages sent within the organization.
		Do not track when users click safe links.
		Do not let users click through safe links to original URL.
Anti-spam	Standard (on)	Spam action
		Mark bulk email as spam
		Bulk threshold
		Mark NDR backscatter as spam
		Safety tips
		Bulk email
		Phishing email
		Allow lists
		Block lists
		Spoof intelligence
	Custom (off)	Default spam filter policy (always ON)

Policy	Setting Category	Setting
		Connection filter policy (always ON)
		Outbound spam filter policy (always ON)
		Spoof intelligence policy
DKIM (DomainKeys Identified Mail)		NAME
		ACCEPTED DOMAIN
		DOMAIN TYPE
		Status:
Anti-malware		ENABLED
		NAME
		PRIORITY
		Malware detection response
		Sender notifications
		Administrator notifications
		Customized notification text

Default ATP Anti-Phishing Settings

By default, ATP does not list an **ATP anti-phishing** policy. However, a default policy is enabled, but not listed in the policy list. Click **Default policy** to see the default policy settings.

Figure 3: Office 365 ATP: ATP anti-phishing policy

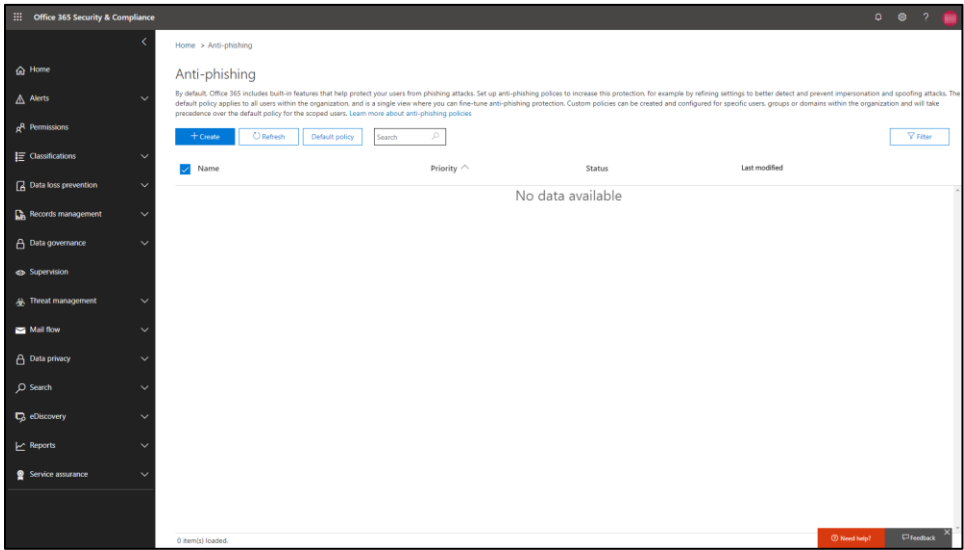
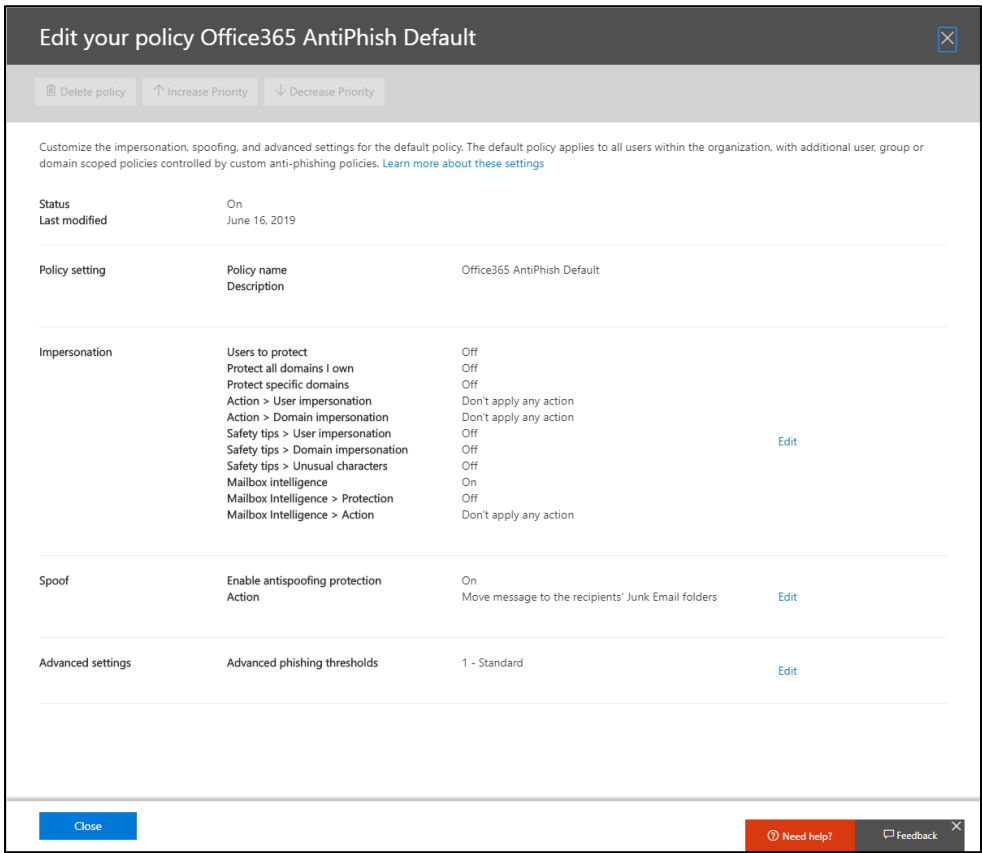


Figure 4: Office 365 ATP: Default ATP anti-phishing policy settings



The following table lists the default settings.

Table 30: Office 365 ATP: Default ATP anti-phishing settings

Policy	Setting Category	Setting	Default Setting
ATP anti-phishing		Name	Office365 AntiPhish Default
		Priority	<blank>
		Status	On
		Last modified	June 16, 2019
	Policy setting	Applied to If the recipient is <specified domain>	
	Impersonation	Users to protect	Off
		Protect all domains I own	Off
		Protect specified domains	Off
		Action > User impersonation	Don't apply any action
		Action > Domain impersonation	Don't apply any action
		Safety tips > User impersonation	Off
		Safety tips > Domain impersonation	Off
		Safety tips > Unusual characters	Off
		Mailbox intelligence	On
		Mailbox intelligence > Protection	Off
		Mailbox intelligence > Action	Don't apply any action
	Spoof	Enable antispoofting protection	On
		Action	Move message to the recipients' Junk Email folders
	Advanced settings	Advanced phishing thresholds	1 - Standard

Default ATP Safe Attachments Settings

By default, ATP does not list an **ATP safe attachments** policy and unlike the **ATP anti-phishing** policy (which has a hidden, unlisted default policy), there is no hidden, unlisted **ATP safe attachments** policy.

If you create a new policy (to do so, click the **+** sign), the following default settings are there, unless you change them.

Figure 5: Office 365 ATP: ATP safe attachments policy

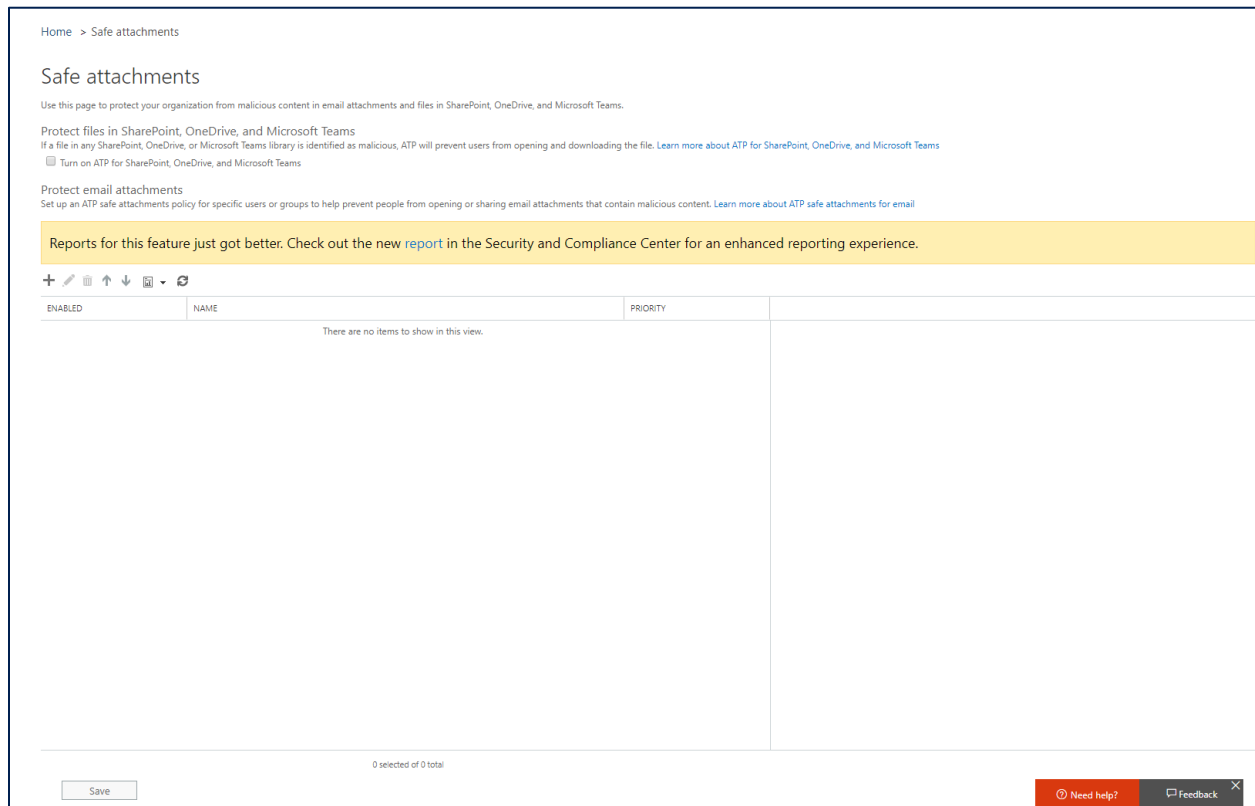


Figure 6: Office 365 ATP: Default ATP safe attachments policy settings

new safe attachments policy

*Name:

Description:

Safe attachments unknown malware response
Select the action for unknown malware in attachments. [Learn more](#)

Warning
Monitor, Replace and Block actions may cause significant delay to email delivery. [Learn more](#)
Dynamic Delivery is only available for recipients with hosted mailboxes. [Learn more](#)
If you choose the Block, Replace or Dynamic Delivery options and malware is detected in attachment, the message containing the attachment will be quarantined and can be released only by an admin.

☒ Off - Attachment will not be scanned for malware.
☐ Monitor - Continue delivering the message after malware is detected; track scan results.
☐ Block - Block the current and future emails and attachments with detected malware.
☐ Replace - Block the attachments with detected malware, continue to deliver the message.
☐ Dynamic Delivery - Deliver the message without attachments immediately and reattach once scan is complete.

Redirect attachment on detection
Send the blocked, monitored, or replaced attachment to an email address.

☐ Enable redirect
 Send the attachment to the following email address:

☒ Apply the above selection if malware scanning for attachments times out or error occurs.

Applied To
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...
 Select one
 add condition

Except if...
 add exception

Save Cancel

The following table lists the default settings.

Table 31: Office 365 ATP: Default ATP safe attachments settings

Policy	Setting Category	Setting	Default Setting
ATP safe attachments	New safe attachments policy	Turn on ATP for SharePoint, OneDrive, and Microsoft Teams	Off
		ENABLED	Off
		NAME	<blank>
		PRIORITY	<blank>
		Description	<blank>
		Safe attachments unknown malware response	Off
		Enable redirect	Off
		Apply the above selection if malware scanning for attachments times out or error occurs.	On
		Applied to: If the message: Is sent to <email address>	Select one
		Condition	add condition
		Except if the message: <exception>	add exception

Default ATP Safe Links Settings

By default, ATP lists an **ATP safe links** policy for **Policies that apply to the entire organization**. There is no default policy for **Policies that apply to specific recipients**.

If you create a new policy (to do so, click the **+** sign), the following default settings are there, unless you change them.

Figure 7: Office 365 ATP: ATP safe links policy and default ATP safe links policy settings

Home > Safe links

Safe links

Safe links help prevent your users from following links in email and documents that go to web sites recognized as malicious. Use this page to set up policies that determine how all or specific users in your organization interact with safe links. [Learn more about safe links](#)

Reports for this feature just got better. Check out the new [report](#) in the Security and Compliance Center for an enhanced reporting experience.

Policies that apply to the entire organization

NAME	Summary
Default	Settings: - Do not track when users click safe links: Enabled - Do not let users click through safe links to original URL: Enabled Applied to: - Office 2016 on Windows: Disabled

1 selected of 1 total

Policies that apply to specific recipients

ENABLED	NAME	PRIORITY
There are no items to show in this view.		

0 selected of 0 total

[Need help?](#) [Feedback](#)

The following table lists the default settings.

Table 32: Office 365 ATP: Default ATP safe links settings

Policy	Setting Category	Setting	Default Setting
ATP safe links	Policies that apply to the entire organization	Name:	Default
		Do not track when users click safe links:	Enabled
		Do not let users click through safe links to original URL:	Enabled
		Applied to: Office 2016 on Windows	Disabled
	Policies that apply to specific recipients	ENABLED	Disabled (user must create a policy; none by default)
		Name	<blank>
		Description	<blank>
		PRIORITY	<blank>
		Priority: Relative priority	<blank>
		Select the action for unknown potentially malicious URLs in messages.	Off
		Use safe attachments to scan downloadable content.	Off
		Apply save links to email messages sent within the organization.	Off
		Do not track when users click safe links.	Off
		Do not let users click through safe links to original URL.	Off

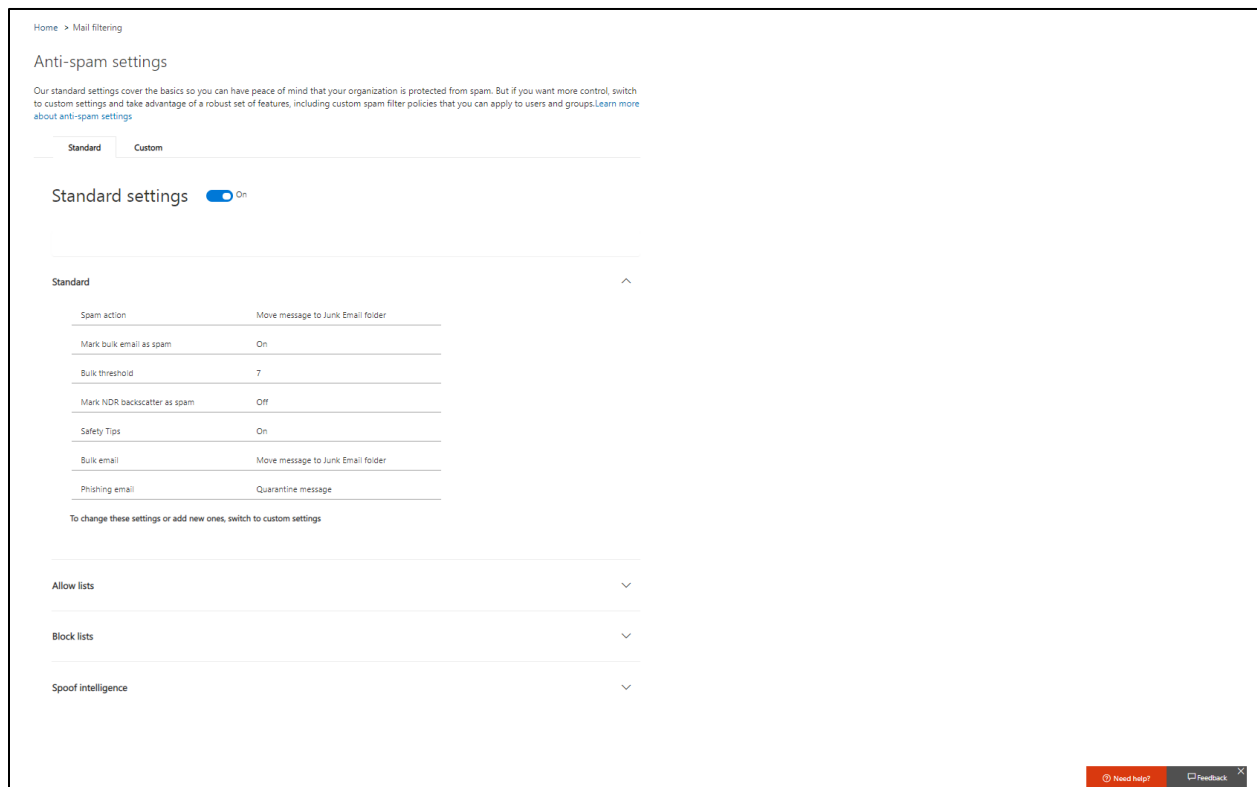
Default Anti-Spam Settings

By default, ATP displays two **Anti-spam** policies, **Standard** and **Custom**. The **Standard** policy on with default settings and the **Custom** policy is off.

(To create a custom policy, click **Custom**, click to turn **Custom settings** on, then create the custom policy with custom settings.)

The standard settings are on, and include four sets of settings: **Standard**, **Allow lists**, **Block lists**, and **Spoof intelligence**.

Figure 8: Office 365 ATP: Anti-spam policy and default Anti-spam policy settings



The following table lists the default settings.

Table 33: Office 365 ATP: Default Anti-spam settings

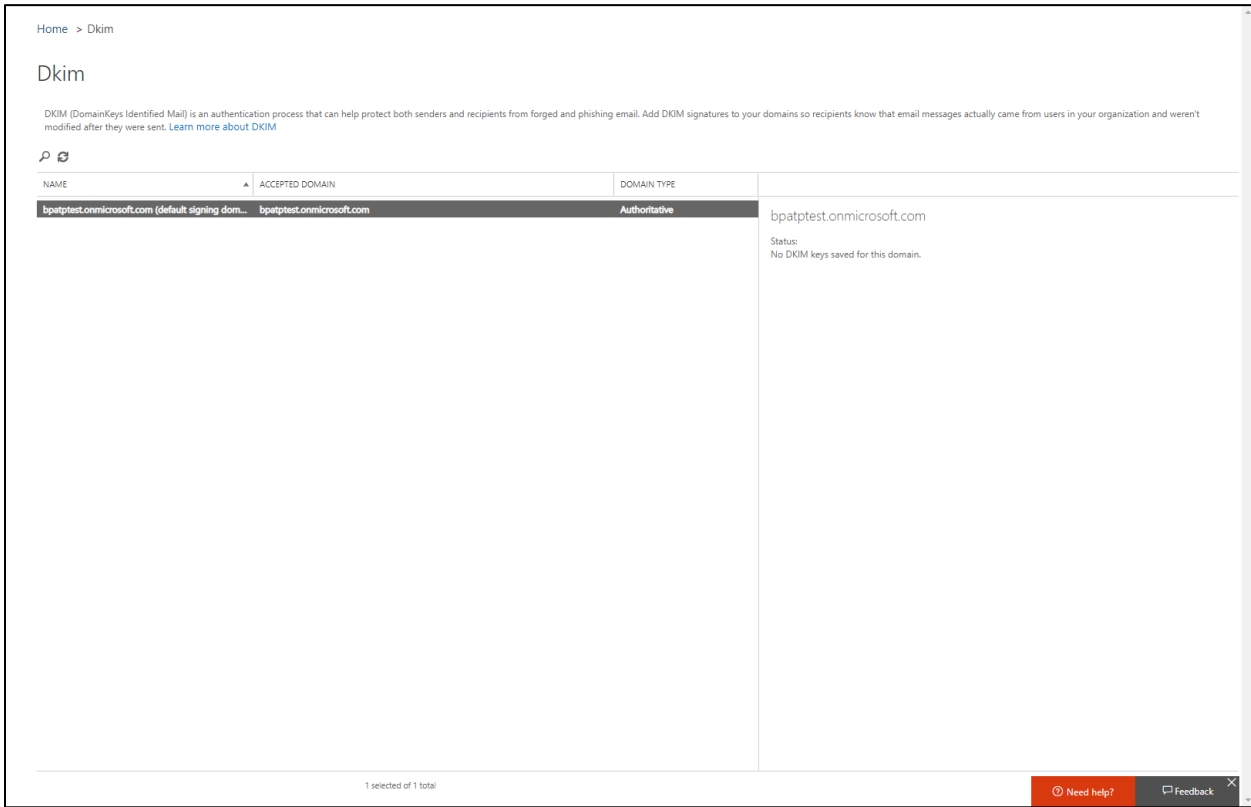
Policy	Setting Category	Setting	Default Setting
Anti-spam	Standard (on)	Spam action	Move message to Junk Email folder
		Mark bulk email as spam	On
		Bulk threshold	7
		Mark NDR backscatter as spam	Off
		Safety tips	On
		Bulk email	Move message to Junk Email folder
		Phishing email	Quarantine message
		Allow lists	<blank>
		Block lists	<blank>
		Spoof intelligence	<blank>
	Custom (off)	Default spam filter policy (always ON)	Off
		Connection filter policy (always ON)	Off
		Outbound spam filter policy (always ON)	Off
		Spoof intelligence policy	Off

Default DKIM (DomainKeys Identified Mail) Settings

By default, ATP displays the one DKIM policy, built from the domain for the Office 365 E5 account (in this example, **bpatptest.onmicrosoft.com**).

There are no DKIM keys saved by default.

Figure 9: Office 365 ATP: DKIM policy and default DKIM policy settings



The following table lists the default settings.

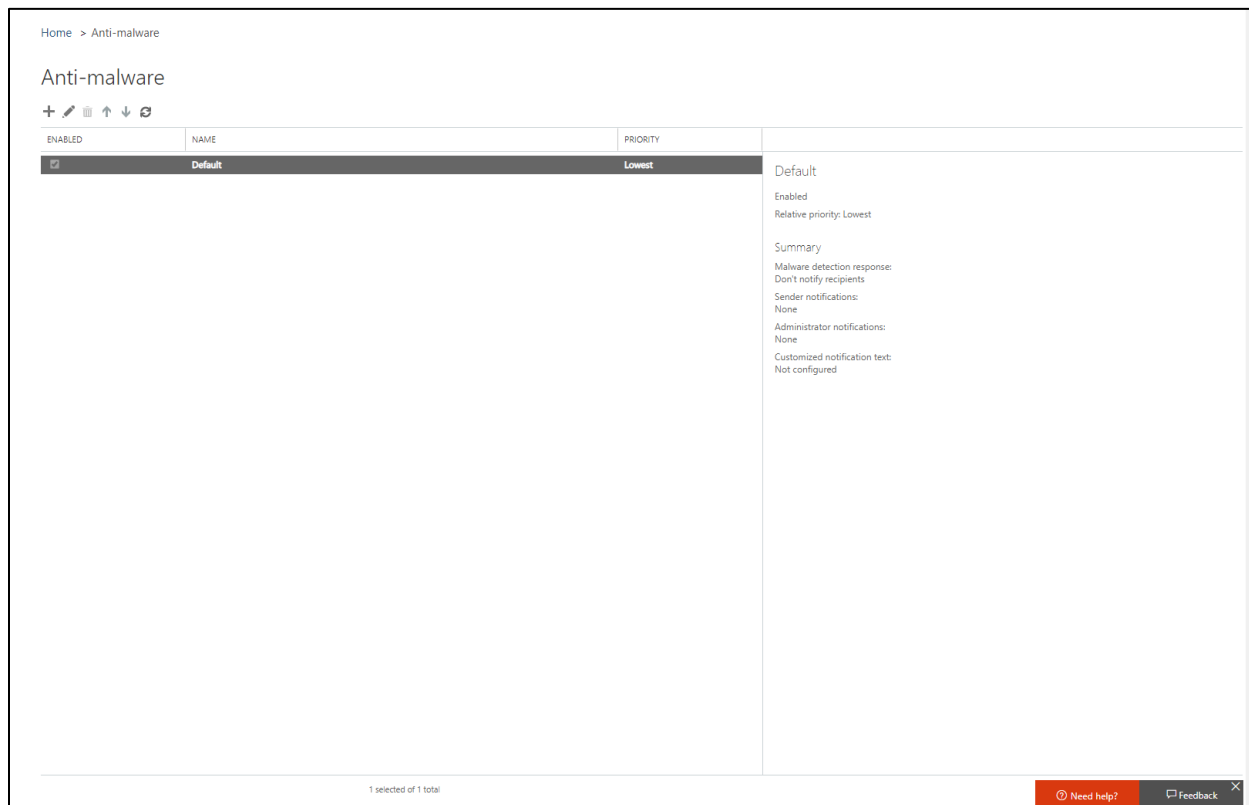
Table 34: Office 365 ATP: DKIM (DomainKeys Identified Mail) settings

Policy	Setting Category	Setting	Default Setting
DKIM (DomainKeys Identified Mail)		NAME	<Office 365 account domain name> (default signing domain)
		ACCEPTED DOMAIN	<Office 365 account domain name>
		DOMAIN TYPE	Authoritative
		Status:	No DKIM keys saved for this domain.

Default Anti-Malware Settings

By default, ATP lists the one default **Anti-malware** policy as **Enabled**. To the right of the policy are the policy settings.

Figure 10: Office 365 ATP: Default Anti-malware policy and default Anti-malware policy settings



The following table lists the default settings.

Table 35: Office 365 ATP: Anti-malware settings

Policy	Setting Category	Setting	Default Setting
Anti-malware		ENABLED	On
		NAME	Default
		PRIORITY	Lowest
		Malware detection response	Don't notify recipients
		Sender notifications	None
		Administrator notifications	None
		Customized notification text	Not configured

Default Settings of Proofpoint PRO+TAP

Features and Modules

The default settings are throughout the product, within the following features and modules:

- Quarantine
- Spam Detection module
- Virus Protection module
- Zero-Hour Anti-Virus module
- Targeted Attack Protection module

Settings

The following tables list advanced threat analysis default settings for Proofpoint PRO+TAP, and where to find them.



Note: In the following tables, if it was unclear from the source information what the default setting was (see [How the Information was Gathered](#)), the correspond cells in the **Default Setting** column are empty.

Quarantine

Table 36: Proofpoint PRO+TAP advanced threat protection settings: Quarantine

Feature or Module	Setting Category	Setting Location	Setting	Default Setting	Notes
Quarantine	Layout defaults	System > Quarantine > Settings > Layout	Results Per Page		
			Wrap Recipient Column		
			Show These Fields In This Order		
	Folders and message expiration: Folder disposition parameters		Quarantine (folder)	All messages destined for the quarantine will be stored in the Quarantine folder.	
	Quarantine folder and subfolders		Release	Enabled	Administrators can disable the Release and Resubmit links for messages in a Quarantine folder.
			Submit	Enabled	Administrators can disable the Release and Resubmit links for messages in a Quarantine folder.
			Smart Send (folder) encryption: Allow User to Send Unencrypted	Off	This folder stores messages that triggered rules enabled for Smart Send. Users can release or delete messages from this folder without administrator help.
			Smart Send Released (folder): <Specify the location for messages released from Smart Send folder>	Smart Send Released folder	When users release messages from the Smart Send folder, they are placed in this folder.
			End User Services > Web Application	Show Quarantine	On

Spam Detection Module

Table 37: Proofpoint PRO+TAP advanced threat protection settings: Spam Detection module

Feature or Module	Setting Category	Setting Location	Setting	Default Setting	Notes
Spam Detection Module	Spam policies and rules	Spam Detection > Settings > General	Spam Detection Module	Enabled	
	Spam rule	Email Protection	Malware Spam		Messages caught by this rule are quarantined in the Malware folder.
			Imposter Spam		Messages caught by this rule are quarantined in the Impostor folder.
			Definite Spam	Disabled	Discards messages that score 100 without sending copies to the Quarantine.
			Phish Spam	Enabled	Messages caught by this rule are quarantined in the Phish folder.
			Adult Spam		
			Spam Quarantined		Messages that score 50 and above are discarded and copies are sent to the Quarantine.
			Low Priority		This rule displays only if your Organization is licensed for SCSS (the Stateful Composite Scoring Service). Messages that meet conditions that classify them as Low Priority will be included in the Low Priority Mail - Delivered (or Low Priority Mail - Quarantined) sections of the email Digest and End User Web Application so that users can act upon those messages.
			Bulk Email	Enabled	Newsletters and advertisements are typically classified as bulk email. By default, bulk email is delivered to user's inboxes and is also visible to users in their email Digests and Web Application.
			Delay Suspected Messages		The <i>suspected spam</i> classifier is scored based on several message attributes which are found in spam but by themselves are not enough to generate a spam score above 50. By delaying such messages until later spam definitions are received, it is likely that you will be able to stop additional spam that would not otherwise have been stopped.
			Circle of Trust		Requires a license for the Stateful Composite Scoring Service - SCSS. This rule is meant for a small group of users in your Organization.
			Not Spam		This rule is unique in that its condition cannot be modified, and the rule cannot be disabled, removed, or re-ordered in the list of rules.

Virus Protection Module

Message conditions: The Virus Protection Module classifies messages into any of these conditions:

- The message is not infected, continue to process it.
- The message is infected with a specific virus - create a rule to handle all messages that contain the specific virus.
- The message contains scan errors and further analysis is impossible.
- The message contains protected data (password-protected or encrypted attachment).
- The message contains riskware or spyware.

Table 38: Proofpoint PRO+TAP advanced threat protection settings: Virus Protection module

Feature or Module	Setting Category	Setting Location	Setting	Default Setting	Notes
Virus Protection Module	Virus protection policies and rules	Protection > Settings > General	Virus Protection Module	Enabled	The Virus Protection Module provides a default policy, which you can edit or clone as the basis for creating another policy. You cannot delete the default policy; you can only modify the set of rules for it.
		Email Protection	Messages Not Infected	Continue	
			Messages Infected		
		Virus Protection > Virus Policies > Rules	Messages Infected: Messages Contain Specific Virus	<Not specified by default>	If necessary, add a rule that determines how to handle messages that contain a specific virus.
			Messages Infected	Enabled	By default, infected messages are discarded and a copy is sent to the Quarantine.

Zero-Hour Anti-Virus Module

Categories: Suspected Messages, Rescan Messages May Contain Probable Virus, and Error Messages. Each category contains one rule that applies a disposition to the messages in that category. You can edit the default rule or add more rules to each category.

Table 39: Proofpoint PRO+TAP advanced threat protection settings: Zero-Hour Anti-Virus module

Feature or Module	Setting Category	Setting Location	Setting	Default Setting	Notes
Zero-Hour Anti-Virus Module	Zero-Hour policies	Email Protection	Zero-Hour Anti-Virus Module	Enabled	The Zero-Hour Module ships with a default policy that includes rules for messages classified with a potential virus threat of medium or high, for messages containing a probable virus, and for messages that could not be analyzed because of a temporary connection failure to the Proofpoint Attack Response Center. The Zero-Hour Anti-Virus Module includes a preconfigured default policy. The default policy is comprised of one rule for each category of messages that the Zero-Hour Module filters: Suspected Messages, Rescan Messages May Contain Probable Virus, and Error Messages. You can edit (change) the rules in the existing default policy, add more rules to the default policy, or create new policies with new rules. Creating a Zero-Hour policy is a two-step process: first create a policy, and then add rules to the policy.
	Zero-Hour category classifications	Email Protection	Suspected Messages	Enabled	For suspected messages, the default threat rule discards the original message (it is not delivered to the recipient) and places a copy in the Quarantine folder Zerohour .
			Rescan Messages May Contain Probable Virus	Enabled	The suspected messages are resubmitted to the Virus Protection Module for virus scanning after they have been delayed in the Quarantine and after Proofpoint has distributed new virus signature files. If the Virus Protection Module indicates the messages are free of virus, and if the Zero-Hour Module still suspects the messages are infected or cannot verify that the messages are free of virus, they are classified as probable. For probable virus messages, the probable rule discards the original message (it is not delivered to the recipient) and places a copy in the Quarantine folder Probable Virus with an added subject header. The default folder settings delete the messages after two weeks.
			Error Messages	Enabled	These messages cannot be scanned by the Zero-Hour Module because of a connection failure or module error that prevents updates to the latest emerging virus threats. Error messages continue to filter through the other filtering modules according to the <i>error</i> rule. If no other rules are triggered in the other filtering modules, the messages are delivered to their intended recipients.

Targeted Attack Protection Module

Targeted Attack Protection Module requirements:

- **Enable Traffic Statistics Feedback to Proofpoint** must be enabled on the **System > Settings > System** page in order to use the Targeted Attack Protection Module.
- If you have purchased Targeted Attack Protection without also purchasing Proofpoint Enterprise Protection, you must set **Enable Audit Mode** to **On** on the **System > Settings > System** page. In Audit mode messages are processed and rewritten without affecting the mail stream.
- The service requires that each filtering agent can make an outbound query over port 443. If an outbound SSL proxy is configured on the **System > Settings > Proxy** page, the filtering agent will use that proxy server for the query.

Targeted Attack Protection Module Settings

Table 40: Proofpoint PRO+TAP advanced threat protection settings: Targeted Attack Protection

Feature or Module	Setting Category	Setting Location	Setting	Default Setting	Notes
Targeted Attack Protection Module	Targeted Attack Protection Module	Email Protection	Targeted Attack Protection Module	Enabled	The Targeted Attack Protection Module consists of URL Defense, Attachment Defense, and the Dashboard. The module protects your organization from phishing, spear phishing, and other malicious attacks.
	Targeted Attack Protection Module policies	Email Protection	URL Defense		When URL Defense is enabled, URLs in a message may be rewritten and directed to Proofpoint's cloud-based service. You have the option of limiting URL Defense to specific Policy Routes. By default, all messages that match the default_inbound Policy Route may have their URLs rewritten. You may need to exclude a group of recipients from having their messages rewritten, or perhaps exclude all messages from a set of hosts. URL Defense redirects the URL to Proofpoint's service when a user clicks a URL in an email message. If the URL is not known to be malicious, the user will be redirected to the original URL. Once redirected, the URL Defense service is no longer in the traffic flow between the user and the web site. If the URL is malicious, the user will see a warning message and the site is blocked in the browser.
			Attachment Defense		When enabled, Attachment Defense protects your organization from malware contained in file attachments. By default, all messages with attachments that match the <i>default_inbound</i> Policy Route are scanned. You can apply Attachment Defense to specific Policy Routes on a global organizational level and also to Policy Routes on a per-rule level. Processing phases: • Phase 1 - Identify Attachments of Interest • Phase 2 - Process Attachments of Interest • Phase 3 - Attachment Awaits Judgment • Phase 4 - Take Action
			Dashboard	Enabled	The Dashboard alerts administrators of email attacks and provides the detail they need to search for targeted attack information, triage to reduce potential damage, submit feedback to Proofpoint, and create detailed reports for security and executive personnel.

This section contains sample screen captures of Proofpoint PRO+TAP modules and default settings.

[illegible]

Email Protection Module (continued)

The screenshot displays the Proofpoint TAP Dashboard for the 'proofpointdemo_demo4' instance. The interface is divided into a left-hand navigation pane and a main content area. The navigation pane includes sections for Email Firewall, Email Authentication, Email Fraud Defense (with sub-sections like Spam Detection, Policies, and Rules), and Virus Protection. The main content area is titled 'Spam Rules' and contains a table of configured rules. Each rule has an 'Enabled' checkbox, a 'Classification', a 'Description', a 'Condition', an 'Action', and an 'Order'.

Enabled	Classification	Description	Condition	Action	Order
☒	malware	Malware Spam	Malware spam score greater than or equal to 50	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine folder [Malware] - Discard the message.	1
☒	impostor	Impostor Spam	Impostor spam score greater than or equal to 60	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine folder [Impostor] - Discard the message.	2
☒	phish	Phish Spam	Phish spam score greater than or equal to 80	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine folder [Phish] - Discard the message.	3
☒	adult	Adult Spam	Adult spam score greater than or equal to 80 AND Spam score greater than or equal to 50	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine folder [Adult] - Discard the message.	4
☒	spam_definite	Definite Spam	Spam score greater than or equal to 100	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine folder [Quarantine] - Discard the message.	5
☒	spam	Spam - Quarantined	Spam score greater than or equal to 50	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine - Discard the message.	6
☐	lowpriority	Low Priority	Low Priority score greater than or equal to 80	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Add header X-Proofpoint-Tag=lowpriority. - Include in "Low Priority Mail - Delivered" folder in the End User Web Application and Digest. - Continue to process the message.	7
☒	bulk	Bulk Email	Bulk email score greater than or equal to 80	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine folder [Bulk] - Discard the message.	8
☒	suspect	Delay Suspected	Suspected spam score greater than or equal to 80	- Add header X-Proofpoint-Spam-Details=\$SpamDetails - Send to quarantine folder [Suspect Spam]	9

At the bottom of the dashboard, a 'CLUSTER STATUS' section provides real-time metrics: 0 Mbps/sec, 0 Connections, 39247 Quarantine Messages, and a Load Average of 2.49. A 'Config Master' status shows 'demo-4' as healthy. System information on the right indicates the software was updated on 2019-05-23 15:21:34 (UTC-07:00) and shows disk space and inode usage levels.

Virus Protection

The screenshot shows the Proofpoint TAP Dashboard with the 'Virus Protection' settings. The 'Rules' tab is selected, displaying a table of virus rules. The 'Messages Not Infected' rule is highlighted. The 'Messages Infected' rule is also visible, showing actions like 'Set subject to [Virus \$VirusName] \$Subject' and 'Add header X-Proofpoint-Virus-Version=\$VirusVersion'.

Condition	Action
Messages Not Infected	- Add header X-Proofpoint-Virus-Version=\$VirusVersion. - Continue to process the message.
Messages Infected	- Set subject to [Virus \$VirusName] \$Subject. - Add header X-Proofpoint-Virus-Version=\$VirusVersion. - Send to quarantine folder [Virus]. - Discard the message.
Messages with Scan Errors	- Set subject to [Virus Error] \$Subject. - Add header X-Proofpoint-Virus-Version=\$VirusVersion.

The screenshot shows the Proofpoint TAP Dashboard with the 'Virus Protection' settings. The 'Rules' tab is selected, displaying a table of virus rules. The 'Messages Not Infected' rule is highlighted. The 'Messages Infected' rule is also visible, showing actions like 'Set subject to [Virus \$VirusName] \$Subject' and 'Add header X-Proofpoint-Virus-Version=\$VirusVersion'.

Condition	Action
Messages Not Infected	- Add header X-Proofpoint-Virus-Version=\$VirusVersion. - Continue to process the message.
Messages Infected	- Set subject to [Virus \$VirusName] \$Subject. - Add header X-Proofpoint-Virus-Version=\$VirusVersion. - Send to quarantine folder [Virus]. - Discard the message.
Messages with Scan Errors	- Set subject to [Virus Error] \$Subject. - Add header X-Proofpoint-Virus-Version=\$VirusVersion.
Messages with Password Protected Attachments	- Set subject to [Not Virus Scanned] \$Subject. - Add header X-Proofpoint-Virus-Version=\$VirusVersion. - Send to quarantine folder [Virus]. - Discard the message.
Messages Contain Riskware/Spyware	- Set subject to [Riskware \$VirusName] \$Subject. - Add header X-Proofpoint-Virus-Version=\$VirusVersion. - Send to quarantine folder [Virus]. - Discard the message.

Quarantine Folders

The screenshot shows the Proofpoint TAP Dashboard interface. The main content area is titled "Quarantine > Folders" and contains a table of quarantine folders. The table has the following columns: Folder Name, Messages, Size (MB), Disposition, Expiration Timing, and Quarantine Action. The "Phish" folder is highlighted in blue.

Folder Name	Messages	Size (MB)	Disposition	Expiration Timing	Quarantine Action
Adult	484	8	Store Messages	3 Days	Delete
Attachment Defense	231	7.9	Store Messages	2 Weeks	Delete
Audit	0	0	Store Messages	2 Weeks	Delete
Blocked	0	0	Store Messages	2 Weeks	Delete
Bounce Management	0	0	Store Messages	2 Weeks	Delete
Bulk	1170	7.9	Store Messages	3 Days	Delete
Deleted	0	0	Store Messages	2 Weeks	Delete
Impostor	13404	24	Store Messages	2 Weeks	Delete
Malware	3898	23	Store Messages	2 Weeks	Delete
outbound_malware	0	0	Store Messages	2 Weeks	Delete
Phish	548	8.8	Store Messages	3 Days	Delete
Provable Virus	0	0	Store Messages	2 Weeks	Delete
Quarantine	10503	191	Store Messages	3 Days	Delete
Smart Send	0	0	Delay Delivery	30 Minutes	Release With Scan
Smart Send Released	0	0	Store Messages	2 Weeks	Delete
Spoofed	0	0	Store Messages	2 Weeks	Delete
Suspected Spam	0	0	Delay Delivery/Spam Updates	30 Minutes / 2 Spam Updates	Resubmit
Test Policy	0	0	Store Messages	2 Weeks	Delete
Untrusted Senders	0	0	Store Messages	2 Weeks	Delete
Virus	756	33	Store Messages	3 Days	Delete
Zerohour	0	0	Delay Delivery/AV Updates	12 Hours / 2 AV Updates	Resubmit
Total:	20992	306			

The bottom status bar shows the following information:

- CLUSTER STATUS:** 0 Mails / sec, 0 Connections, 39095 Quarantine Messages
- Config Master:** demo-4, Status: Healthy
- System Health:** 0 Mails / sec, 0 Connections, 0 ACQuise Messages, 2.98 Load Average
- Updated:** 2019-05-23 10:23:26 (UTC-08) - 11
- PPS Disk Space:** 44% (26 GB Avail)
- Swap:** 49% (4 GB of 8 GB Avail)
- Index Usage:** 8% (588433 of 3764764 Avail)

Quarantine Experience

This section compares the quarantine experiences of both products. That is, how does the quarantine behavior compare between the two products?

Comparison Table

Table 41: Quarantine Experience comparison table

Office 365 ATP Plan 2	Proofpoint Targeted Attack Protection (TAP)	Notes
		Microsoft: The default behavior of ATP makes it easier for a user to access false positive emails and content (emails identified as threats that are not threats). But, that ease has a downside: real threats going to the user's Junk Email folder, too. Effectiveness outweighs ease of use in this case, since the purpose of the product is to provide security. Proofpoint: The default behavior of TAP errs on the side of caution, putting all emails that are a potential threat (including false positives) in quarantine. While that makes getting harmless emails from quarantine more difficult, that does not seem to be an issue as a use case, as Proofpoint provides the user with a view and access to what is in quarantine (depending on how restrictive the security administrator makes the Quarantine settings and Spam Detection Module settings).

Quarantine Experience with Office 365 ATP Plan 2

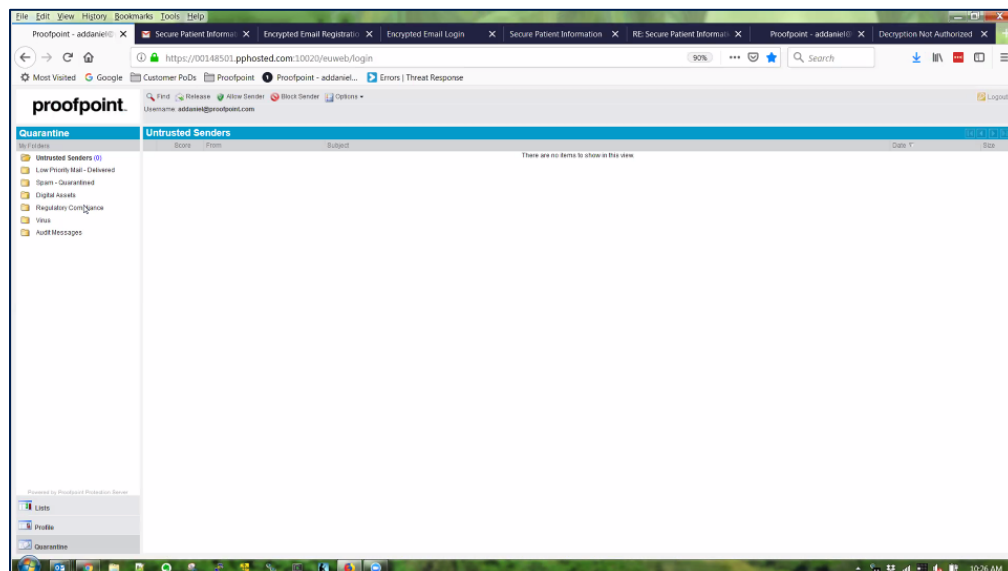
Prior sections detail how Office 365 ATP Plan 2 uses quarantining, so this section will refer to those prior references and not repeat them. Key elements of the quarantine experience for ATP are:

- The default to move malicious emails and content to Junk Email, not quarantine. (See [Default Anti-Spam Settings](#).)
- As a result, there is exposure and risk from a potential threat that could have been eliminated if the product default behavior was to quarantine the malicious email and/or content (move it to a quarantine folder).
- The two products took a different approach to the potential of a false positive (identifying an email and its content as a threat when it is not a threat). Microsoft chose to move potential threat emails to **Junk Email** folder, to make it easier for a user to retrieve emails that are false positives (not really a threat). The downside to that is that true threats also go to the **Junk Email** folder.

Quarantine Experience with Proofpoint PRO+TAP

Prior sections detail how Proofpoint PRO+TAP uses quarantining, so this section will refer to those prior references and not repeat them. Key elements of the quarantine experience for PRO+TAP are:

- The default to move malicious emails and content to quarantine. (See [Default Settings of Proofpoint PRO+TAP](#), especially the [Quarantine](#) settings and [Spam Detection Module](#) settings.)
- As a result, there is exposure and risk from a potential threat is eliminated, no matter if the email is malicious or not (emails that are a false positive are quarantined, as well).
- The two products took a different approach to the potential of a false positive (identifying an email and its content as a threat when it is not a threat). Proofpoint chose to move potential threat emails to a quarantine folder. The downside is that both true and false positive emails go to quarantine, which makes it more difficult for the end user to retrieve the email if it is a false positive. They do have a process for a user to remove items from quarantine.
 - Proofpoint provides settings (see [Default Settings of Proofpoint PRO+TAP](#), especially the [Quarantine](#) settings and [Spam Detection Module](#) settings) to either make it more or less difficult to access and use quarantined emails (move them out of quarantine).
 - The user can access the **Quarantine** web page to view (and if the settings allow) access quarantined items.



FAQ

Table 42: FAQ

#	Topic	Product	Question	Response
1	Recording	Proofpoint PRO+TAP	Can the account rep record the demo, for your later reference, as needed?	Yes. The recording typically is an MP4 file, which the account manager will share through a secure portal.
2	Plans and Pricing	Proofpoint PRO+TAP	What product/solution plans do you have?	There is a wide array of products in the Proofpoint suite. The full list is in the Proofpoint Products and Plans section of this document. Further details are in the Proofpoint product line card .
3	Plans and Pricing	Proofpoint PRO+TAP	What prices are available?	Pricing is done through their resellers. The pricing approach and estimated pricing for two pricing brackets are listed in Proofpoint PRO+TAP in the <i>Pricing</i> section.

#	Topic	Product	Question	Response
4	Plans and Pricing	Proofpoint PRO+TAP	Where does the purchase and pricing shift from Proofpoint to the partner, and when does the pricing kick in?	Proofpoint does not engage with partners. Proofpoint does rely entirely on resellers for their product pricing and acquisition process. A typical customer engagement: 1. Starts with the prospective customer contacting Proofpoint for a free trial/POC of their product. 2. A Proofpoint representative engages a Proofpoint account rep with the customer. (Step-by-step details for this are listed in the Evaluation Evaluating Proofpoint TAP section of this document.) 3. The prospect will ask about pricing and the account rep will offer to connect them with either the prospect's preferred reseller or if they don't have one, the rep offers to contact one for them. 4. The account rep arranges for a demo and begins acquiring the information needed to set up an evaluation POC. (Step-by-step details for this are listed in the Evaluation Evaluating Proofpoint TAP section of this document.) 5. The POC cluster is spun up. (It takes the Proofpoint SE 3 to 5 business days to get the cluster spun up.) When it's spun up, then they can implement the POC for the evaluation. From this point onward, the reseller is the prospect's contact for pricing and Proofpoint is the prospect's contact for everything else regarding their products and services.
5	Plans and Pricing	Microsoft ATP	What is the cost of each Microsoft plan?	The price differs depending on the plan. For details, go to this pricing table .
6	Settings and Features	Proofpoint PRO+TAP	What are the default settings?	The default settings are listed in the Default Settings of Proofpoint PRO+TAP section.

#	Topic	Product	Question	Response
7	Settings and Features	Proofpoint PRO+TAP	How do I change the settings? Who in the organization will make these changes? A security admin?	The Proofpoint policy and module settings are not as centralized as they are with Microsoft ATP. Setting locations are detailed in the Default Settings of Proofpoint PRO+TAP section. Settings can be changed by a security administrator. In Email Protection, you can create roles with access based on each module, as well as whether they should be able to manage the settings for that module. In TAP, there are two roles: Admin (can make changes), Standard (can only view reporting).
8	Settings and Features	Proofpoint PRO+TAP	Is there a portal to login as an admin? Can admins or other roles delegate permissions?	Yes there is an admin portal. In Email Protection, you can create roles with access based on each module, as well as whether they should be able to manage the settings for that module. In TAP, there are two roles: Admin (can make changes), Standard (can only view reporting).
9	Administration and Portals	Proofpoint PRO+TAP	Do you have a separate portal for the TAP product? Does that correlate with other configuration experiences with your other products?	Yes, for reporting/visibility. The configuration is in the same Admin GUI as Email Protection.

#	Topic	Product	Question	Response
10	Administration and Portals	Proofpoint PRO+TAP	Can you show how a real admin in a real organization performs processes?	Here are two examples (worst case scenarios): Example 1: Phish Link 1. A message comes in with a clean URL; it is rewritten and delivered. 2. After delivery, the attacker uploads a phishing template weaponizing the URL. 3. User clicks on the link, makes it through to the site, gives away their credentials (assumes worst case scenario). 4. TAP alerts Threat Response and admin. Threat Response removes any other copies of that message in all user Inboxes and puts them in quarantine. 5. Admin determines what service was being Phished based off of TAP information and the messages Threat Response quarantined. 6. If service Admin Controls, reset password of Impacted user. If service user Controls, inform user of need to reset password. Example 2: Malware Attachment 1. A message comes in with an attachment with a clean URL in it, because we do not want to break the attachment it is not rewritten and delivered. 2. After delivery, the attacker uploads a malicious iframe weaponizing the URL. 3. User clicks on the link, makes it through to the site, infects their machine (assumes worst case scenario). 4. TAP alerts Threat Response and admin. Threat Response removes any other copies of that message in all user Inboxes and puts them in quarantine. 5. Admin determines what type of malware based off of TAP information and the messages Threat Response quarantined. 6. Admin runs Threat Response Indicator of Compromise Collector to determine infection. 7. If infected, take appropriate response (likely reimage machine).

#	Topic	Product	Question	Response
11	Partners and Support	Proofpoint PRO+TAP	What does the support process look like while setting up and configuring? What is the SLA?	Support for setup and configuration is handled by the Proofpoint Professional Services team and they walk side by side with the customer when it comes to setting up specific rules, transferring rules over, whitelists, distribution lists, and much more. They'll make sure everything is set up the way the customer wants it before they give them the reins. The SLA is referenced and linked to in the References section.
12	Partners and Support	Proofpoint PRO+TAP	Proofpoint and partner role and scope: - Where does the role of Proofpoint end and the partner begin? - Where does the partner end and the customer begin?	The role of the partner is entirely for pricing estimates, pricing, and product acquisition. Proofpoint engages with the customer prior to the purchase, and if pricing is discussed, they facilitate the contact and conversation with the partner (reseller). Proofpoint handles everything else outside of that.
13	Demonstrations	Proofpoint PRO+TAP	Are there any offline demos I can look through?	There are some demonstrations of specific features on the Proofpoint Resource Center (infographics, podcasts, training modules, videos, and webinars) but to see a full product demonstration, you need to request one (see the Evaluating Proofpoint PRO+TAP section for details).
14	Reporting	Proofpoint PRO+TAP	Customer perspective: How does the customer know that Proofpoint is working or not? What reports, dashboards, and other metrics show the product is working as expected?	You will have access to the Reporting through TAP, which shows what Proofpoint sandboxes and what manages to get through including an Effectiveness report. The Quarantine folders will contain the messages caught and there are 70+ reports built into the gateway. (See Effectiveness Report and Quarantine Experience with Proofpoint PRO+TAP for further details.)
15	Reporting	Proofpoint PRO+TAP	Security admin perspective: Reporting, dashboard, or metrics to show, from a security admin's perspective, to protect the emails, but also be able to report to the CSO that it's working: - How much risk was/is mitigated? - How the impact was contained. - Reports that show (for example) that a phishing campaign was caught within a given time frame.	You will have access to the Reporting through TAP, which shows what Proofpoint sandboxes and what manages to get through including an Effectiveness report. The Quarantine folders will contain the messages caught and there are 70+ reports built into the gateway. (See Effectiveness Report and Quarantine Experience with Proofpoint PRO+TAP for further details.)

#	Topic	Product	Question	Response
16	User Experience	Proofpoint PRO+TAP	User productivity aspect: - What will the user experience look like? - Will they see malicious links? - Will the security department get contacted because emails are being held back? - Based on the analysis of malicious emails and attachments, does that cause a delay in emails? What is your process for this, and what the SLA is around email delivery?	What will the user experience look like? URLs will be rewritten if you choose (highly recommended), they may get digest messages if you choose (spam summary messages), they may have access to a web portal (either this, the digests, or both are recommended) Will they see malicious links? If the message is blocked, no. If it is rewritten (that is, it is clean as it comes through), then yes, however, if it then becomes malicious the link will redirect to the block page. Will the security department get contacted because emails are being held back? If you like. Alerts can be set up. Based on the analysis of malicious emails and attachments, does that cause a delay in emails? What is your process for this, and what the SLA is around email delivery? Yes, on average ~3–5 minutes, though you can set it not to, as well as set a maximum time.
17	Products	Proofpoint PRO+TAP	What is Proofpoint on Demand (PoD)? What is its relationship with TAP?	PoD is Proofpoint on Demand (the Proofpoint hosted environment). PoD includes TAP and is where you can manage the configuration settings for it (included in the <i>Proofpoint on Demand Proofpoint Administration Guide</i>, referenced and listed in the References section). TAP also includes the TAP Dashboard, which allows for reporting on and viewing of threats that have been sandboxed (not included in the document).

#	Topic	Product	Question	Response
18	Products	Proofpoint PRO+TAP	The customer doesn't need to choose the whole suite nor entire collection of suites, correct? Are there any dependencies across suites and applications?	Correct. However, PRO and TAP go hand-in-hand. The Proofpoint Email Protection solution identifies the "known" threats (spam, spoof, phish, bulk) as well as be your core gateway that blocks these threats. Proofpoint Targeted Attack Protection identifies the more advanced and sophisticated attacks (malicious emails that have URLs and attachments) as well as provides sandboxing capabilities for these said URLs and attachments. Since TAP is able to identify these sophisticated threats, it will relay this information to the Proofpoint Email Protection solution, which will block them outright. TAP will not work without PRO.

References

The following is a list of source content for this document as well as further information to add to your knowledge of both products.

The list is in two tables; one listing Microsoft ATP-related materials and the other listing Proofpoint TAP-related materials.

Microsoft ATP References

Table 43: Microsoft ATP References

Item and Link	Purpose	Microsoft or Proofpoint	Notes
Conversations with Pragya Pandey	Source content for this document	Microsoft	
Technical docs on configuring policies: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-atp	For further reference.	Microsoft	
Quick start guide: https://docs.microsoft.com/en-us/office365/securitycompliance/protect-against-threats	For further reference.	Microsoft	
Product page that includes details on Office 365 Advanced Threat Protection Plan 1 and Plan 2.	For further reference.	Microsoft	The new SKUs went on price list on Feb 1.
Advanced Threat Protection in Office 365 video by Microsoft Mechanics, that talks about the capabilities within Office 365 ATP and our differentiated benefits.	For further reference.	Microsoft	Duration: 11:11.
An eBook supporting the Microsoft Mechanics video, free for download on the product page.	For further reference.	Microsoft	
A customer ready deck that combines the capabilities and value props of Office 365 ATP and Office 365 Threat Intelligence.	For further reference.	Microsoft	Microsoft internal and confidential deck inside Infopedia.
An updated battlecard for Proofpoint .	For further reference.	Microsoft	Microsoft internal and confidential battlecard inside Infopedia.
Ignite sessions: • BRK4001 - Secure enterprise productivity with Office 365 threat protection services including EOP, A... • BRK4002 - Securing your Office 365 environment from advanced phishing campaigns with Office 365 Adva... (has demos of configurations)	For further reference.	Microsoft	Ignite sessions.

Item and Link			Purpose	Microsoft or Proofpoint	Notes
Content from last field airlift:			For further reference.	Microsoft	Microsoft internal and confidential airlift video and deck inside Infopedia.
Office 365 ATP	4.56	Jason			

Proofpoint PRO+TAP References



Important: All of these items (with the exception of the [Targeted Attack Protection Dashboard – PPS Tutorial](#) YouTube video) are located in the [Office 365 ATP Proofpoint comparison project](#) folder.

To the best of our knowledge, this is publicly available information that anyone requesting a demonstration or looking at public information could get.

Table 44: Proofpoint PRO+TAP References

Item and Link	Purpose	Microsoft or Proofpoint	Notes
Recorded Proofpoint demonstration	Source content for this document	Proofpoint	
Proofpoint SLA - General Terms Hosted Services.PDF		Proofpoint	Proofpoint SLA.
POC Results-400 users-ATP.PNG	For further reference	Proofpoint	Advanced Threat Detection Summary: Proofpoint data sheet of the difference between what Proofpoint captured that Microsoft ATP did not.
POC Results- 400 users-Microsoft.PNG	For further reference	Proofpoint	Message Quarantine Results (attached): Proofpoint data sheet of the difference between what Proofpoint quarantined that Microsoft ATP did not.
Products.PNG	Source content for this document	Proofpoint	Image excerpt from their product line card showing where the account executive (Justin Fullington) yellow-highlighted the items he gave the ballpark price on.
Proofpoint-Targeted Attack Protection-Datasheet.pdf	For further reference.	Proofpoint	Proofpoint TAP datasheet. Also located here on their site.
Proofpoint Targeted Attack Protection URL Re-writing (2).PDF	For further reference.	Proofpoint	Tech brief about Proofpoint TAP URL rewriting.
Proofpoint-Email-Protection-Solution Brief.pdf	For further reference.	Proofpoint	Proofpoint email protection solution brief.

Item and Link	Purpose	Microsoft or Proofpoint	Notes
Journaling diagram (Journaling.png)	For further reference.	Proofpoint	Proofpoint diagram showing the connection between the Proofpoint on Demand (PoD) and Exchange Online Protection (EOP), and how messages (email) flow through Office 365 and Proofpoint PoD.
Proofpoint on Demand (PoD) Administration Guide (PoD_Admin_Guide_revA_8.12.X.pdf)	Source content for this document and for further reference.	Proofpoint	Detailed 436-page administration guide, including 24 chapters, a glossary, and index. (The table of contents alone is 17 pages.) A few example chapters are <i>User Management</i>, <i>Quarantine</i>, <i>End User Services</i>, <i>Logs and Reports</i>, <i>Content Control</i>, <i>Encryption</i>, <i>Spam Detection Module</i>, <i>Virus Protection Module</i>, <i>Zero-Hour Anti-Virus Module</i>, <i>Targeted Attack Protection</i>, <i>Frequently Asked Questions</i>, <i>Glossary</i>, and <i>Index</i>.
Targeted Attack Protection Dashboard – PPS Tutorial	Source content for this document and for further reference.	Proofpoint	A publicly available (on YouTube) short (5-minute) but detailed walkthrough and description of how to use the TAP dashboard.
Sample Reports - Landscape.png	For further reference	Proofpoint	Screen capture of a Threat Landscape report.
Sample Reports - Effectiveness.PNG	For further reference	Proofpoint	Screen capture of an Effectiveness report.
Sample Reports - People Centric.PNG	For further reference	Proofpoint	Screen capture of a People Centric report.
Sample OneDrive Phish Detail.PNG	For further reference	Proofpoint	Screen capture of a OneDrive Phishing detailed report.

Appendix

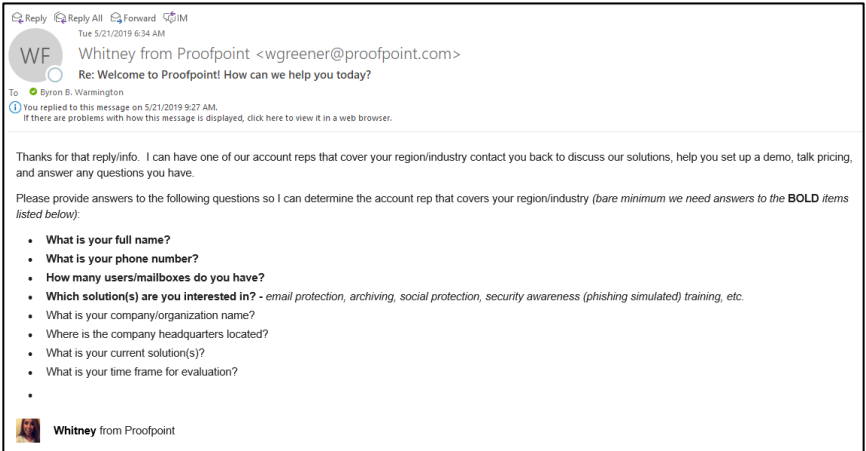
Evaluating Proofpoint PRO+TAP

The following is the table from the [Communicating with Proofpoint: The process continues](#) section, but with the original source emails in the **Details** column.

Communicating with Proofpoint: The process continues

Regardless of which of the two methods you use, the process continues with the following steps.

Table 45: Evaluation steps (continued process) table

Step	Details
6. You will receive an email from a Proofpoint contact.	 Re_ Welcome to Proofpoint! How car
7. Respond, describing your request to evaluate Proofpoint TAP.	
8. The account rep will respond to you with a list of questions so that they can route you to the appropriate account rep for your region and industry.	 Whitney from Proofpoint <wgreener@proofpoint.com> Re: Welcome to Proofpoint! How can we help you today? To: Byron B. Warrington You replied to this message on 5/21/2019 9:27 AM. If there are problems with how this message is displayed, click here to view it in a web browser. Thanks for that reply/info. I can have one of our account reps that cover your region/industry contact you back to discuss our solutions, help you set up a demo, talk pricing, and answer any questions you have. Please provide answers to the following questions so I can determine the account rep that covers your region/industry (bare minimum we need answers to the BOLD items listed below): • What is your full name? • What is your phone number? • How many users/mailboxes do you have? • Which solution(s) are you interested in? - email protection, archiving, social protection, security awareness (phishing simulated) training, etc. • What is your company/organization name? • Where is the company headquarters located? • What is your current solution(s)? • What is your time frame for evaluation? • Whitney from Proofpoint
9. The Proofpoint contact might follow up with additional questions (such as the those listed in the Details column). Respond to the questions.	Are you wanting to evaluate to be able to understand it for resell? Or are you wanting to purchase internally? Are you an MSP ?

10. The Proofpoint contact will then respond to you, and then they will create a separate email thread, introducing you to the account rep.	 Proofpoint Follow Up.msg
11. The account rep will email you to ask about scheduling a brief 30-minute discovery call and to schedule a 60-minute demonstration.	 RE_ Proofpoint Follow Up.msg
12. If you respond that you'd like to have both a discovery call and a demonstration, the account rep will schedule the discovery call.	 Bridge Partners Consulting - Proofp
13. Then, the account rep will schedule and send you an invitation to the demonstration, using Zoom. The demonstration will include you, the account rep, and a Proofpoint SE.	 Bridge Partners Consulting - PRO_T/

14. In the discovery call, the account rep will answer your questions and will also ask you for some very specific information. Without that information, they will not create a proof of concept (POC) environment for you to try out and evaluate their product. The information they need is:

- **Number of email users:** Need the number of the customer company's email users (not the number of mailboxes).
- **Mail volume report:** Minimum of 30-day day-to-day mail volume report (can be pulled by an Office 365 administrator).
- **Action request:** They usually ask this later in the process, but they will ask that the customer's Exchange administrator be prepared to set up the Journal Rule and associated Send Connector in the Office 365



RE_ Proofpoint
Targeted Attack Prot

Exchange Admin Console. If you ask about pricing, they will ask if you have a preferred reseller.	
15. Then (typically the next day), you'll receive an email offering you the opportunity to download their 2018 User Risk Report.	International Cybersecurity Result
16. In this instance, we sent them questions prior to the demonstration, which they gleefully accepted. (as well as anytime later). <u>You can ask them to record the demonstration and share the recording. Also ask them for their SLA.</u>	RE_ Bridge Partners Consulting - PRO_TA RE_ Bridge Partners Consulting - PRO_TA
17. They performed the demonstration, introduced by the account rep, then the SE demonstrated the product and responded to the emailed questions, then the account rep finished up the session. They were diligent about answering all of the questions and invited us to send more or reach out to them, if needed.	(See the Proofpoint PRO+TAP References section for the link to the <i>Recorded Proofpoint Demonstration</i> and other supporting materials.)

18. The account rep will send you a recording of the demonstration if you requested it. In this instance, we requested their SLA, which they also sent. All files that the account rep sends to you will be through their secure portal.



Bridge Partners Consulting - PRO_T/



Proofpoint SLA - General Terms Hoste

19. In the demonstration, the account manager will offer to send you the following information. If you say yes, they will send these two items with anything else you might have requested:

- **Advanced Threat Detection Summary:** Their data sheet of the difference between what Proofpoint captured that Microsoft ATP did not.
- **Message Quarantine Results:** Their data sheet of the difference between what Proofpoint quarantined that Microsoft ATP did not.

Advanced Threat Results
Advanced Threat Detection Summary

Unknown, Zero-hour Threats
Reputation only check is ineffective

Threat Messages	25 Day Results	Annualized
Messages with Malicious URLs (phishing & malware)	1,614	23,564
Messages with Malicious Attachments (phishing & malware)	48	793
Total Messages	1,662	24,357

Numbers don't tell the whole story. Some messages contain multiple threat types (e.g., both malicious URLs and a malicious attachment). These messages are counted once in this report.

- Data representing January 26 to February 20, 2018
- Messages that passed Microsoft and identified malicious by Proofpoint
- 1,518 (93.2%) were proactively detected and would be blocked in production
- 73 had URL's that would have been rewritten and delivered
- 24 contained attachments that would have been delivered, but cleaned up by TRAP

proofpoint

Advanced Threat Results
Message Quarantine

Hundreds of Confidential Phish
Thousands of Spam/Adult & Gray mail

Message Type (Inbound)	25 Day Results	Annualized
Malware + Phish	279	4,073
Spam + Adult	7,498	109,471
Bulk (Gray Mail)	127,246	1,857,795
Total Messages	135,023	1,971,339

- Data representing January 26 to February 20, 2018
- Messages that passed Microsoft and identified as unwanted by Proofpoint
- Separate quarantine folders allow for granular policy control

proofpoint

20. The account rep will follow up after the demonstration, asking if they can reach out to a reseller on your behalf, to get you pricing information.	 RE_ Bridge Partners Consulting - PRO_T/
---	--