Defender for Office 365 Plan 2 vs Mimecast

Defender for Office 365 Plan 2 Pros and Cons

Pros	Cons
End to end XDR and traces including giving a holistic view of payloads clicked from an email. Can utilize this to then remove messages from user inboxes.	Steep learning curve. Will need training for new and existing staff to implement and manage.
All in one solution for XDR.	Many tasks are only able to be done using Powershell. This results in time wasted if you don't know Powershell well and/or need to look up commands. It also adds challenge to training new staff and existing since they also need to learn Powershell as well.
	"High Confidence" phishing and spam is auto blocked by Microsoft with little ability for admins to control or manage this. There is no "white list" for these emails and the only way to "force" them to get delivered is by submitting them to Microsoft every 30 days until they white list them on their back end.
	More difficult to learn how to effectively use than Mimecast.
	Poor or outdated documentation. Difficult to find help for basic tasks or general setup.
	No specific "Graymail" filtering. Using the sliders Microsoft provides can quickly create false positives at higher levels of filtering.
	Requires significant setup and understanding of M365, Defender, Azure, Mail Flow.
	Much more complex and confusing interface requiring access to at least four different admin panels to manage and maintain (M365/Exchange/Security/Compliance).
	Not optimized or configured "out of the box".

Mimecast Pros and Cons

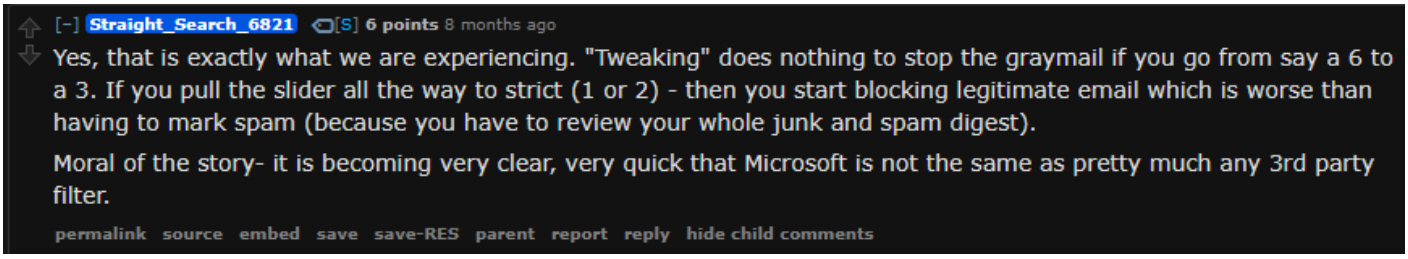
Pros	Cons

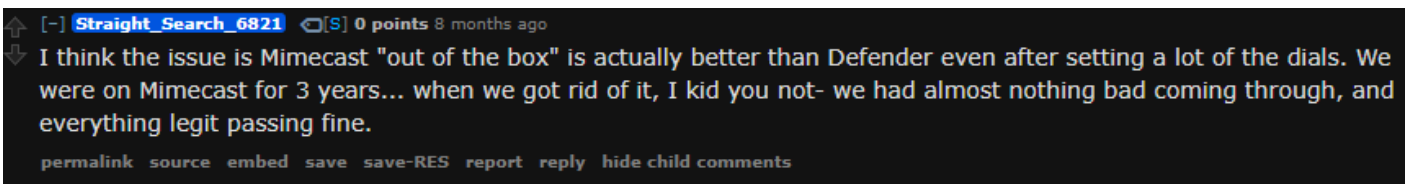
Can manage multiple tenants outside of our Azure tenant in a "single pane of glass". Multi-tenant potential exists to include EXOs in Mimecast filtering while still passing mail to M365 or existing mail servers.	Additional cost beyond the E5 licenses we'll be paying for.
Easier to learn and start managing compared to M365.	Requires understanding of mail flow from the internet to Mimecast, to M365.
Much simpler interface.	Simple setup that by default turns on "best practices" "out of the box".
Closer to "set it and forget it" when setup properly.	

Layered Approach Pros and Cons (Expanding Current M365 Functionality)

Pros	Cons
Exceptional filtering results.	Steep learning curve to utilize both. Will require training for all new and existing staff as well as exceptional documentation on how things are setup for our environment.
Multi-tenant potential exists to include EXOs in Mimecast filtering while still passing mail to M365 or existing mail servers.	Extreme complexity.
	No "single pane of glass".
	Increased chance of false positives.
	Increased cost.

Configuring Microsoft Defender vs Mimecast





[-] ITBurn-out 3 points 8 months ago

Create custom policies, don't use the default. Quarantine all domain impersonation and possibly user. It does a great job. We support 95 different tenants and no issues. High confidence goes to quarantine with only admins able to release by request. Rest go to junk and clear in 14 days.

permalink source embed save save-RES report reply hide child comments

[-] freedomit 2 points 8 months ago

What score do you set for bulk mail?

permalink source embed save save-RES parent report reply hide child comments

[-] ITBurn-out 2 points 8 months ago

One below default. If a user dossnt want it they can right click and set as junk or report it which does the same... Or block it. If it's bulk they signed up for it and should unsubscribe. They can also escalate to us to to block it or the contact at the company can have it done domain wide.

permalink source embed save save-RES parent report reply

[-] Buucket 1 point 8 months ago

What I did was configure DNS records for their domains, set the slider to 6, ran som kusto queries to find bulk senders, spam domains, and phish sending domains. I then made mail flow rules to reject these. In addition to this we did some reporting a year prior to configure their email security.

Now things have improved a lot.

permalink source embed save save-RES report reply hide child comments

Mimecast vs ProofPoint vs Defender 365

[-] Fatboy40 6 points 1 year ago

As an admin, not a reseller / MSP employee, of Mimecast and Defender one thing I greatly miss having moved a year ago from a business using Mimecast to Defender is "grey listing".

Grey listing stopped a lot of opportunistic / one time spam dead for me, the type of bulk spam etc. you receive from a compromised legitimate business or mailbox. This is not in Defender and Microsoft have no intention to introduce it, which is disappointing.

Of course there's a substantial cost difference between the two products, but personally over the past year I've found myself missing Mimecast greatly and not feeling the love for Defender. I suppose a lot also comes down to the existing Microsoft 365 licensing a business is using, in that even with my personal preferences I'd find it hard to justify not using a product I may already be paying for vs a separate billable e-mail security solution.

permalink source embed save save-RES report reply hide child comments

Mimecast or Windows Defender for 365?

[-] ernestdotpro MSP - USA 2 points 4 months ago

Microsoft's spam filter is top notch even without Plan 2.

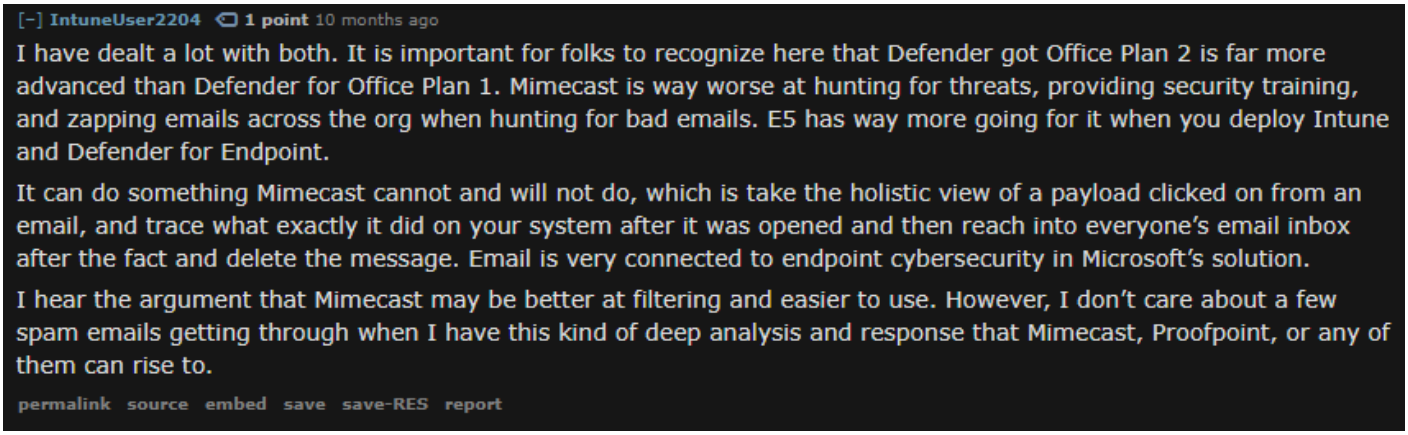
However, unlike Mimecast, it's not optimized or configured out of the box.

Spend some significant time with the documentation and best practice guides. Adjust the settings to your needs and monitor them. When you're comfortable, make the switch!

The only reason we use a 3rd party email filter across our client base is centralized control. If we could effectively manage M365's built in spam filter across hundreds of tenants, we would.

permalink source embed save save-RES report reply

What is the best email security solution, M365 E5 License or Mimecast Email Security?



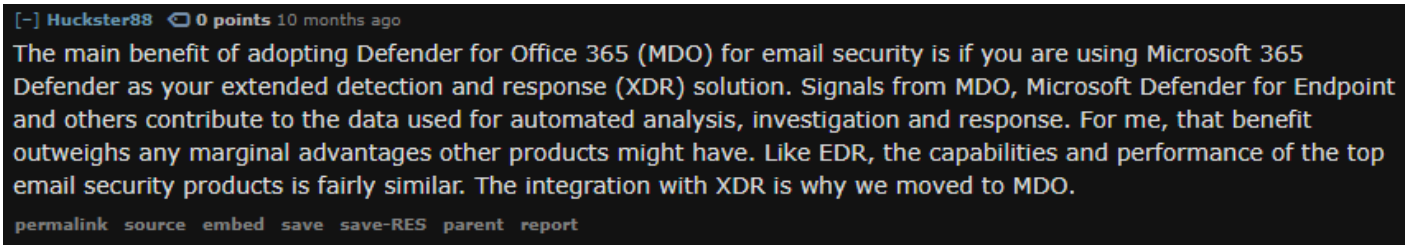
[–] IntuneUser2204 1 point 10 months ago

I have dealt a lot with both. It is important for folks to recognize here that Defender got Office Plan 2 is far more advanced than Defender for Office Plan 1. Mimecast is way worse at hunting for threats, providing security training, and zapping emails across the org when hunting for bad emails. E5 has way more going for it when you deploy Intune and Defender for Endpoint.

It can do something Mimecast cannot and will not do, which is take the holistic view of a payload clicked on from an email, and trace what exactly it did on your system after it was opened and then reach into everyone's email inbox after the fact and delete the message. Email is very connected to endpoint cybersecurity in Microsoft's solution.

I hear the argument that Mimecast may be better at filtering and easier to use. However, I don't care about a few spam emails getting through when I have this kind of deep analysis and response that Mimecast, Proofpoint, or any of them can rise to.

permalink source embed save save-RES report



[–] Huckster88 0 points 10 months ago

The main benefit of adopting Defender for Office 365 (MDO) for email security is if you are using Microsoft 365 Defender as your extended detection and response (XDR) solution. Signals from MDO, Microsoft Defender for Endpoint and others contribute to the data used for automated analysis, investigation and response. For me, that benefit outweighs any marginal advantages other products might have. Like EDR, the capabilities and performance of the top email security products is fairly similar. The integration with XDR is why we moved to MDO.

permalink source embed save save-RES parent report

Revision #4
Created 2024-04-05 14:25:12 UTC by Ryan
Updated 2025-02-12 01:11:59 UTC by Ryan