Quick Start guide.

Sabiki

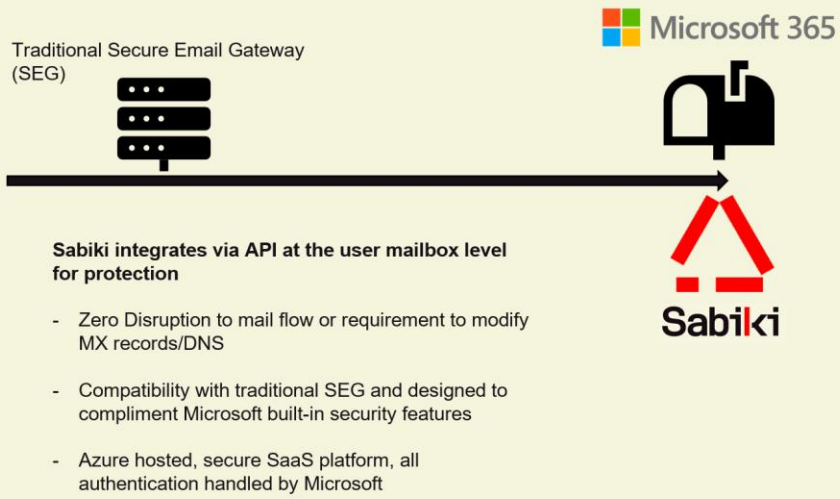
Sabiki Email Security for Microsoft 365

What is Sabiki Dynamic Email Security for Microsoft 365?

Sabiki Email Security has been developed to provide Anti-Phishing and Anti-Spam filtering for the Microsoft 365 email ecosystem. It extends the built-in protection provided within your 365 subscription by using a next-generation AI powered Dynamic engine that is designed to organically learn and protect users from the most advanced of email attacks.

Sabiki is categorized as an Integrated Cloud Email Security (ICES) solution and as such does not require any modification to mail routing or MX records. Sabiki hooks in via API at the user mailbox level to perform any scanning or actions.

It is designed to be 'Stacked' with existing email security solutions and purpose built to sit behind the available Microsoft 365 security feature set by bolstering capabilities and adding an independent last line of defense for Phishing and Advanced email threats.



What are the benefits of using Sabiki Email Security?

Sabiki is your 'needle in the haystack' solution designed specifically to detect advanced email attacks.

Whilst the pre-trained AI model out of the box is designed to bolster an environments detection capability and improve capture rates, the Sabiki team have 'opened' up the AI model with a dynamic learning capability. A Machine Learning based solution is only as good as the data set that it is trained on, so providing multiple workflow capabilities to enable this dynamic training removes the need of ever submitting a sample and allows administrators to tune the model for an even greater level of detection accuracy.

Some notable use cases from Sabiki customers in production are:

- Used as a second layer of defense behind the Microsoft stack of security capability or in tandem with a traditional Secure Email Gateway (SEG).

- Used as a tool to enable mailbox level manipulation of messages and email analysis.

- Administrators who wish to customize an email security engine through AI via a simple intuitive platform.

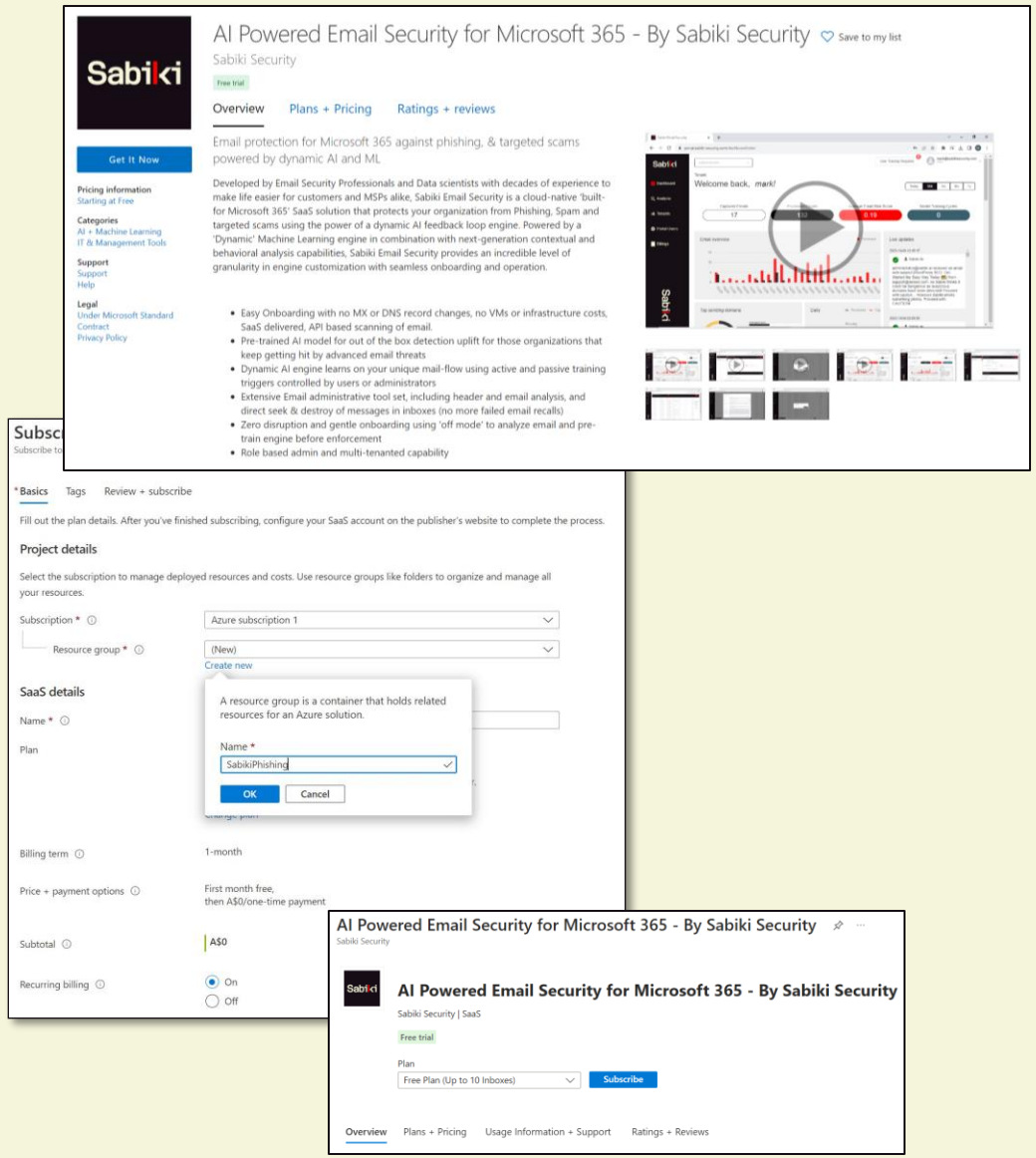
- Administrators who simply want to bolster detection rates without any tuning using the pre-trained model.

"We just needed something else to cross check all the emails that were being missed. I know we can put it through training cycles ourself quite easily but so far have just used it out of the box and it has already picked up 3 phishing emails our existing solution missed." - Michael Barbara, Senior Manager, Perfecto Foods

How do I activate Sabiki Email security?

Sabiki Email security for Microsoft 365 is available as a SaaS subscription via the Azure Marketplace.

When selecting any of the subscription options on the marketplace listing, ensure you are signed in using your Microsoft 365 tenant administrator account. A tenant administrator has the permissions required to authorize the Sabiki 'App' and its associated resources for your environment.



To subscribe via the Azure marketplace:

- Click 'Get it Now' on the offer screen
- Consent to the offer using your Azure account
- Select your plan type
- Setup basic subscription details

(Create a new resource group and give it a unique name. Note, you will NOT be charged for any backend/infra costs to run the resources required for your instance)

- Review and Subscribe

Ensure any pop-up blockers are disabled prior to starting this workflow, it is also best to be authenticated in your browser using the same Azure tenant admin account you will be using to add your first Tenant.

First Tenant Setup

- Once the Azure marketplace subscription is complete and you are logged into the console, you will be presented with the 'Adding a new tenant' workflow.

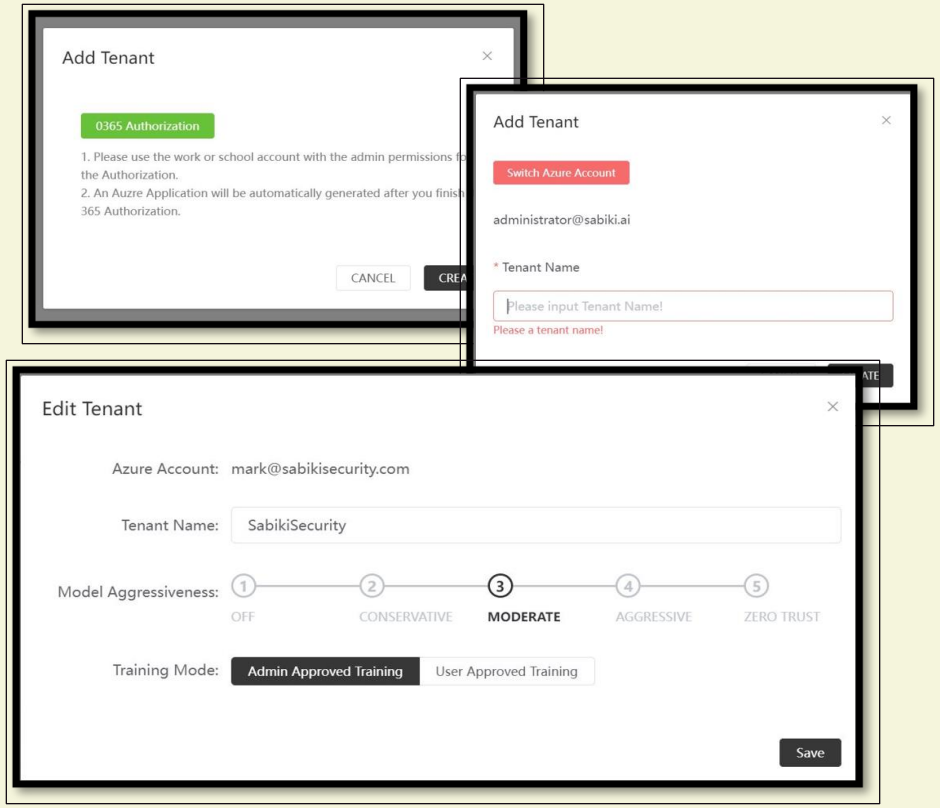
- Clicking on the 'O365 Authorization' is where you authorize which Tenant you wish to protect mailboxes for. (Ensure you are using the tenant admin credentials you wish to protect.)

- Once you name the tenant, it will then prompt you to add users. **Cancel this and complete the tenant setup first.**

- Edit the Tenant you just created and set the Model Aggression and Training modes.

- The 'Off' setting will see the model score emails but not touch/move them regardless of their score while each of the other settings progressively triggers action on lower scores.

The least disruptive method of deployment to users is 'Off' mode, a very low-risk and invisible method of gathering scores for training purposes/if selecting this mode feel free to protect ALL user mailboxes during the next step.



Which settings do I choose?

There are three main considerations when setting up protection for an email environment. What should the model aggression be? What training mode do I select, and do I enable user quarantine?

This quick start guide assumes you are aiming to introduce Sabiki into your environment in a phased approach with the lowest possible impact to your users with an option to tune the engine further with admin-based training.

Phased Quick Start settings

Model Aggression = OFF
Training Mode = Admin Approved
Mailboxes = No risk is choosing Protect ALL as there is no conviction or disruption in OFF mode.
Quarantine = No

User Approved Training

If a user drags a convicted email out of the 'Phishing' Folder a training cycle is immediately queued to 'train as good'.
If a user drags an email from anywhere else in the mail client into the 'Phsihing' folder a training cycle is immediately queued to 'train as bad'

**Model tuning is progressive, so a small number of incorrect training cycles will not result in a fully posisoned model.*

Admin Approved Training

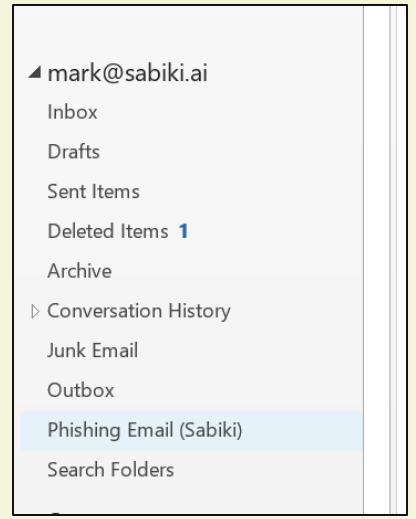
User can drag and drop email in and out of the 'Phishing' folder, but training will be queued in the administrative console.
The admin will see an alert on the main dash if there are any user training requests, they can be approved or rejected enmasse within the Email Analysis feature.

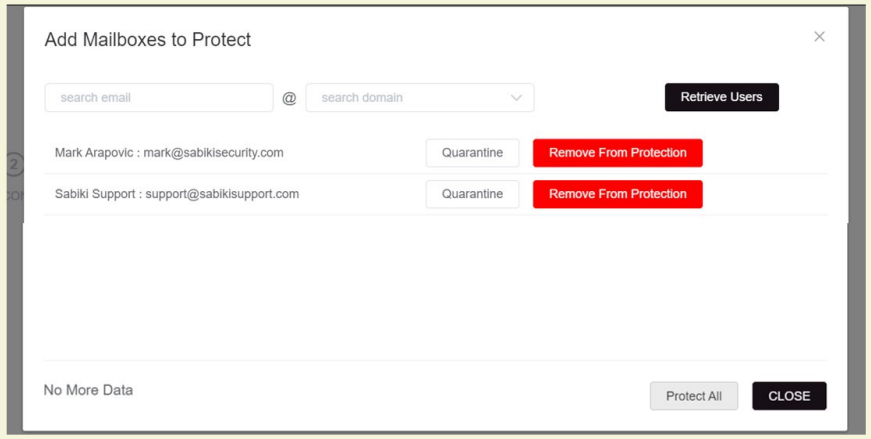
** Note, approving or rejecting training cycles does not impact what happens with the email within the user mail client, it is simply weather or not is should be added to the model training.*

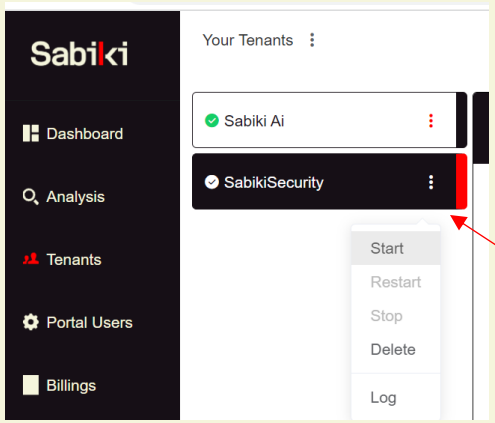
Protecting Mailboxes

Once your tenant setting have been configured, you must add mailboxes to protect. Click on the ‘Edit’ button in the lower right of the screen under the ‘Protected Mailboxes’ section.

- Click retrieve users
- You can filter by domain or search for a specific mailbox, you may also bulk select the ‘protect all’ option
- **Once protected, within the user mail client a new folder will be created called ‘Phishing Email (Sabiki)’ and the model will analyze the user mail-box for its 'model priming'.**







Don't forget to start the model for your tenant after configuring the settings!

How are End users impacted?

In OFF mode, users are not impacted at all.

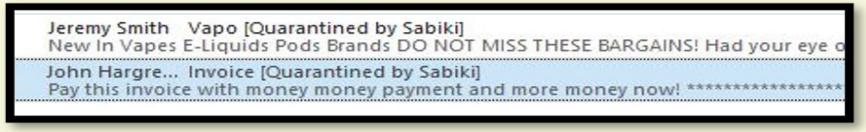
When the **'Phishing Email (Sabiki)' folder** is created within the mail client, it operates much the same way as the 'Junk' Email folder in your mail client. When Sabiki is eventually enabled in enforcement mode, any convicted message will be moved out of the Inbox and into this Phishing Email folder.

If you select user training mode for the model, each time a user moves a message into, or out of this Phishing folder, an AI model training cycle can be automatically initiated.

Fail-open design

Sabiki Email Security for Microsoft 365 has been designed with a 'fail-open' architecture, if there are any issues with the service, platform, engine etc. Mail-flow cannot be impacted. Any issue within the App/Platform will simply result in messages not being scanned.

Additional quarantine policy can be enabled on individuals to protect them from malicious attachments, links etc. When running in enforcement mode...



How do we initiate model training?

Each Email environment is unique. The concept of using OFF Mode for initial deployment is so the administrator has the chance to review the efficacy of the pre-trained Sabiki Engine.

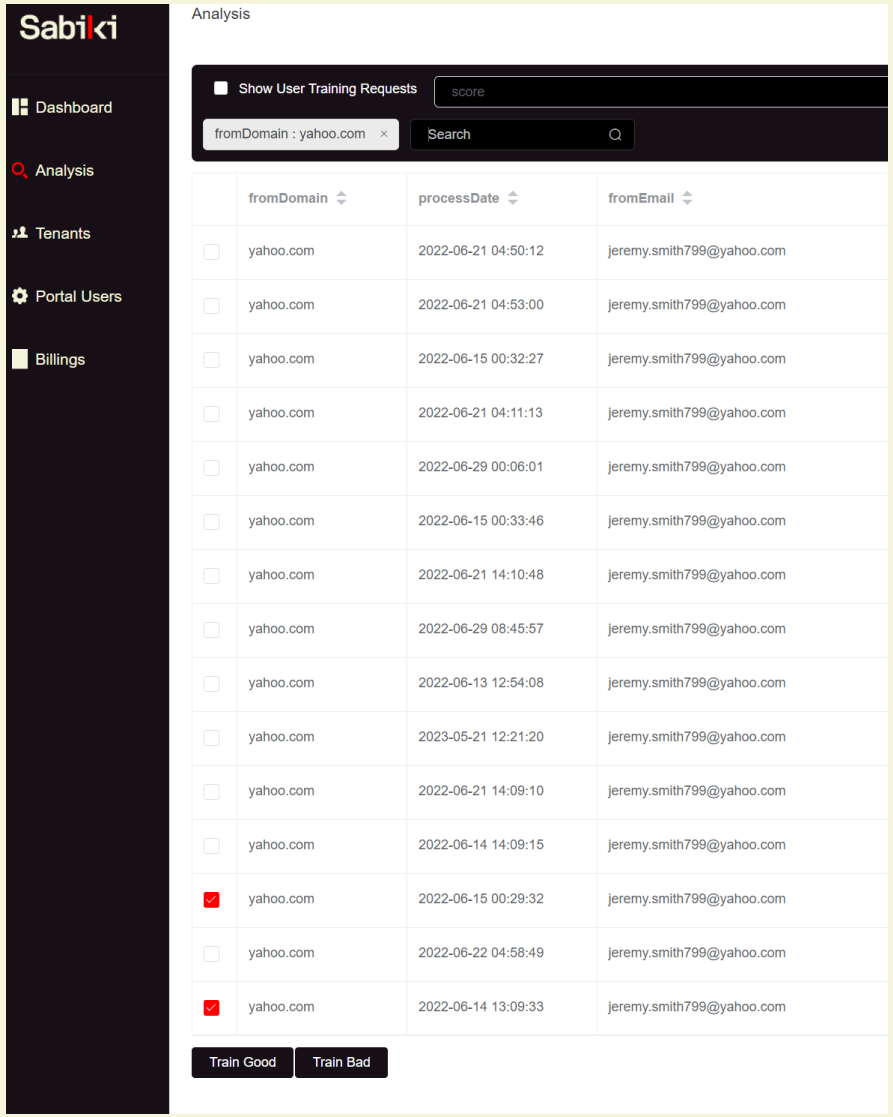
Once a mailbox is protected, you will see mail-flow statistics in the main dashboard as well as what score has been attributed to a message as to how likely it is to be a 'bad' email from 0.00 to 1.0.

Scores can be reviewed in the Email Analysis section and the AI model can be trained on tenant specific emails here by the administrator.

Additional notes:

- If an email is appropriately scored by the engine, there is no need for you to train the engine again, only for scores you do not agree with would a training cycle be done (false negative or false positive)

- How many training cycles, or if training of the model is needed at all depends on the environment. Some customers proceed straight into production and enable user mode training immediately, others elect for a phased approach over a more extended period.



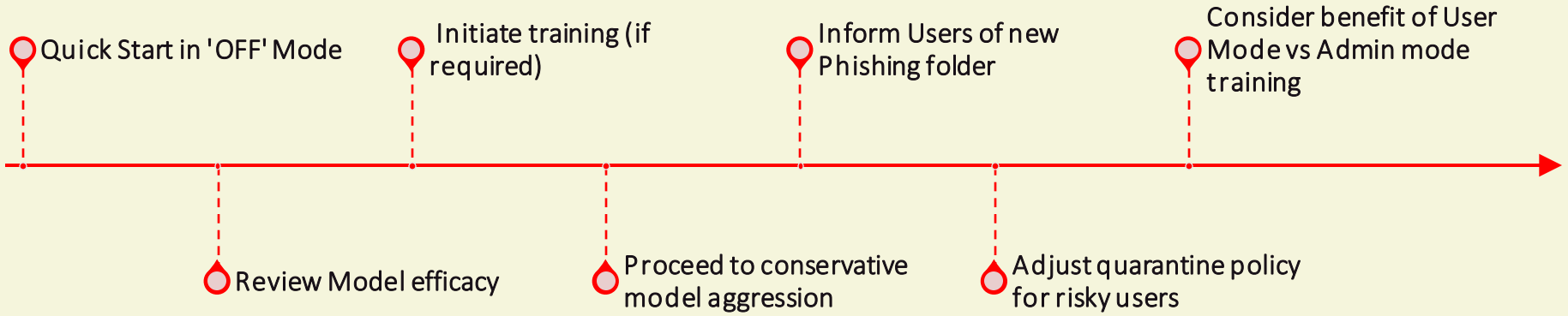
Full Production and further support

Once you are happy with testing, proceed to turn the model into a conservative aggression setting and inform users that any convicted messages will be moved into the Phishing folder (referencing the Microsoft Junk mail folder mechanic).

For further support or questions:

www.sabiki.ai

Support@sabikisupport.com



Sabiki.ai