Frequently asked questions.

Sabiki

What is Sabiki Dynamic Email Security for Microsoft 365?

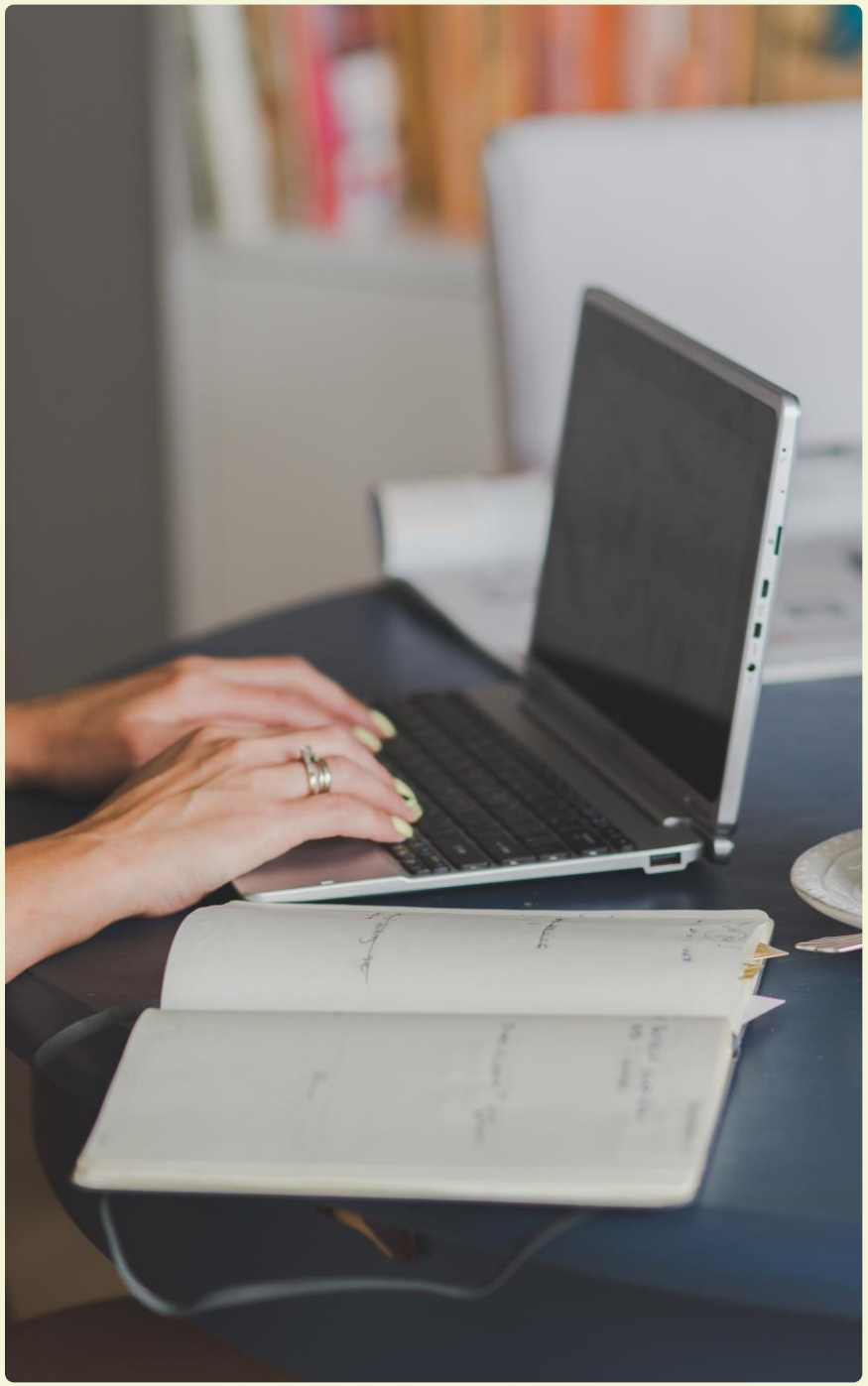
Sabiki Email Security has been developed to provide Anti-Phishing and Anti-Spam filtering for the Microsoft 365 email ecosystem. It extends the built-in protection provided within your 365 subscription by using a next-generation AI powered Dynamic engine that is designed to organically learn and protect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

In addition to adding extra depth to 365 email security features, it can also be layered with (or replace) existing 3rd party ESGs (Email Security Gateway Solutions).

What Email services do you support?

Sabiki Email Security is developed natively for the Microsoft 365 Email service (Outlook 365). We support Business subscriptions from ‘Microsoft 365 Business Basic’ up to and including the ‘Enterprise E5’ license by leveraging the Microsoft Graph API to access and secure user mailboxes.

We do not currently do not support any strictly on-premise Exchange deployment nor Google Mail services which are both in development.



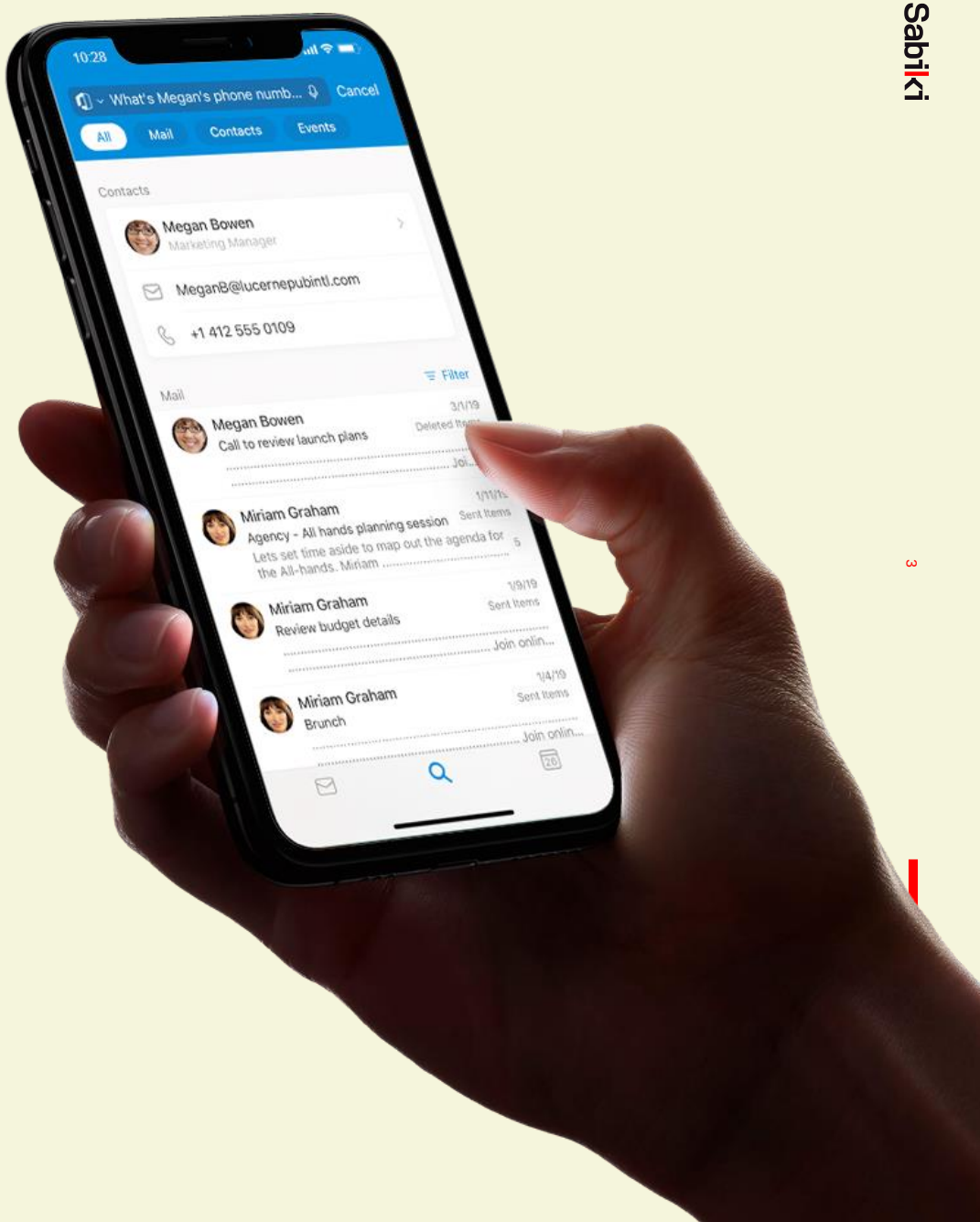
Is Sabiki Email Security a SaaS solution?

Yes, Sabiki Email Security is provided as a service and hosted on Microsoft Azure. You are not required to ‘spin up’ any virtual machines and do not incur any infrastructure costs for your environment. It is a turn-key SaaS offering based on a per mailbox subscription.

How do I route my mail to the Sabiki Platform?

There is no need to re-direct, re-route or change your mail flow in anyway. We simply hook in at the mailbox level utilizing the Microsoft Graph API to provide instantaneous filtering on email as the last step in the mail delivery process. No changes to MX and/or DNS records whatsoever.

We are a Cloud native SaaS solution built on Microsoft Azure, simply authorize the Sabiki ‘App’ during setup with your Microsoft 365 tenant administrative credentials.



How does Sabiki Dynamic Email Security for M365 work?

Sabiki is your ‘needle in the haystack’ solution designed specifically to detect Phishing based attacks.

AI engines and models are not new in the world of Email Security, but the Sabiki approach addresses the fundamental truth of AI… an AI model is only as good as its training data, and what better data set to train an Email security solution with than your own.

The Sabiki platform allows the engine training data to be derived from your environment, based on your unique mail flow. Training is triggered both actively and passively with the natural user behavior of dragging and dropping emails to and from a new folder Sabiki creates within their mail client and administrators can also initiate training cycles from the Email Analysis tool within the management console.

How are my users impacted?

The various quarantine/training workflows with Sabiki Email Security allow the administrator to be as transparent or as restrictive as they need to be depending on the user's maturity level when it comes to Phishing prevention.

When a mailbox is protected with Sabiki Email Security, a new folder is created in the user's mail client called 'Sabiki Phishing' which is used as the 'working' folder for any message quarantine and dynamic training interaction. Any message scored as 'bad' will be moved into this directory.

The policy applied by the administrator then dictates how this folder will be used and what the user is able to do with messages.

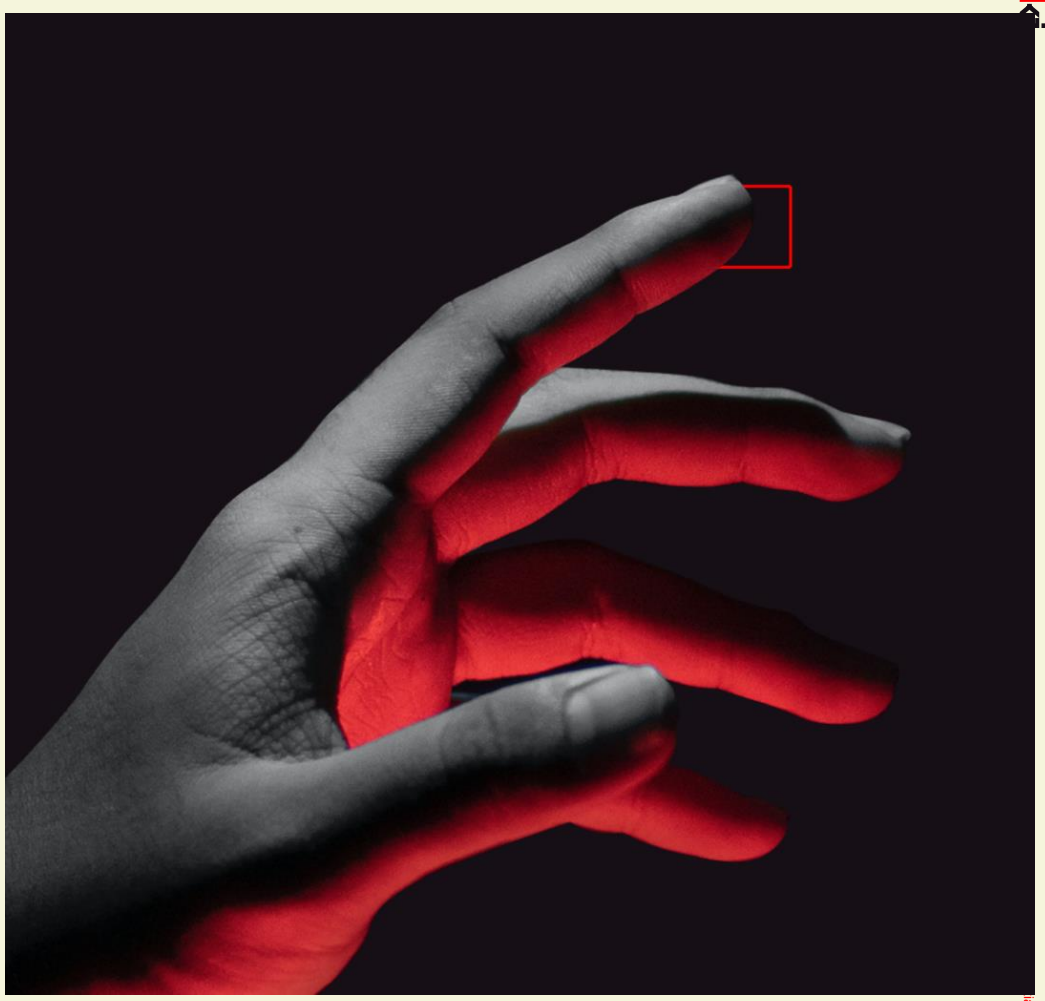
Examples:

- During a trial, you might run in 'off mode' , meaning messages are scored and reported to the Sabiki Console, but nothing is touched or moved into this 'Phishing' folder on the user side. The admin can then manually train messages as good or bad within the email analysis tool to fine tune the engine before full deployment.

- In production, Sabiki can move messages above a certain scoring threshold to this 'Phishing' folder and have any URLs/Reply-to data hidden from the user (quarantined)

- For a trusted/power user, we may allow them to drag/move a quarantined message back into their inbox which will restore URLs/Reply-To data

- We may allow the user action of moving messages in and of this phishing folder to trigger a model training cycle.



How is it different from a traditional solution?

By hooking in at the API level, not only does Sabiki simplify deployment and troubleshooting of mail flow in general, but it also provides a closer control mechanism and better analytics when performing general email administration tasks. Not to mention the revolutionary proprietary dynamic engine that is designed to boost your phishing capture rate significantly.

During the design phase of the platform, 3 key pain points were identified for email administrators (outside of the obvious Phishing capture rate issues):

Sample submission
One regular task email security admins have had to deal with for current generation platforms is sample submissions of false positives/false negatives to the solution vendor. Often if there is an incident of a false negative, there is no immediate response or method of modifying the engine immediately to fix the capture issue. The mechanics of our Dynamic engine mean any false positive can immediately be trained on and the organization is not only secure against that threat, but future variations of the message too. All without submitting a sample or writing custom rules.

Quarantine
Our development team have tried to re-imagine quarantine for users. Quite often power users can be at a disadvantage trying to guess if an important message has been quarantined out of sight. The action of having a ‘convicted message’ moved from the user inbox to the ‘Sabiki Phishing’ folder means if power users are at a low risk level, they may simply move the message back into the inbox. For high risk users, additional controls are added where any URL/attachment/Reply-to details are stripped and can only be recovered with admin permission. Remember, Phishing is often highly targeted with the user being prompted to perform an action or reply, if we take away these risks the message itself is often redundant. A spear Phish for example would be something you certainly would not want landing in a spam digest and then being automatically released by a user.

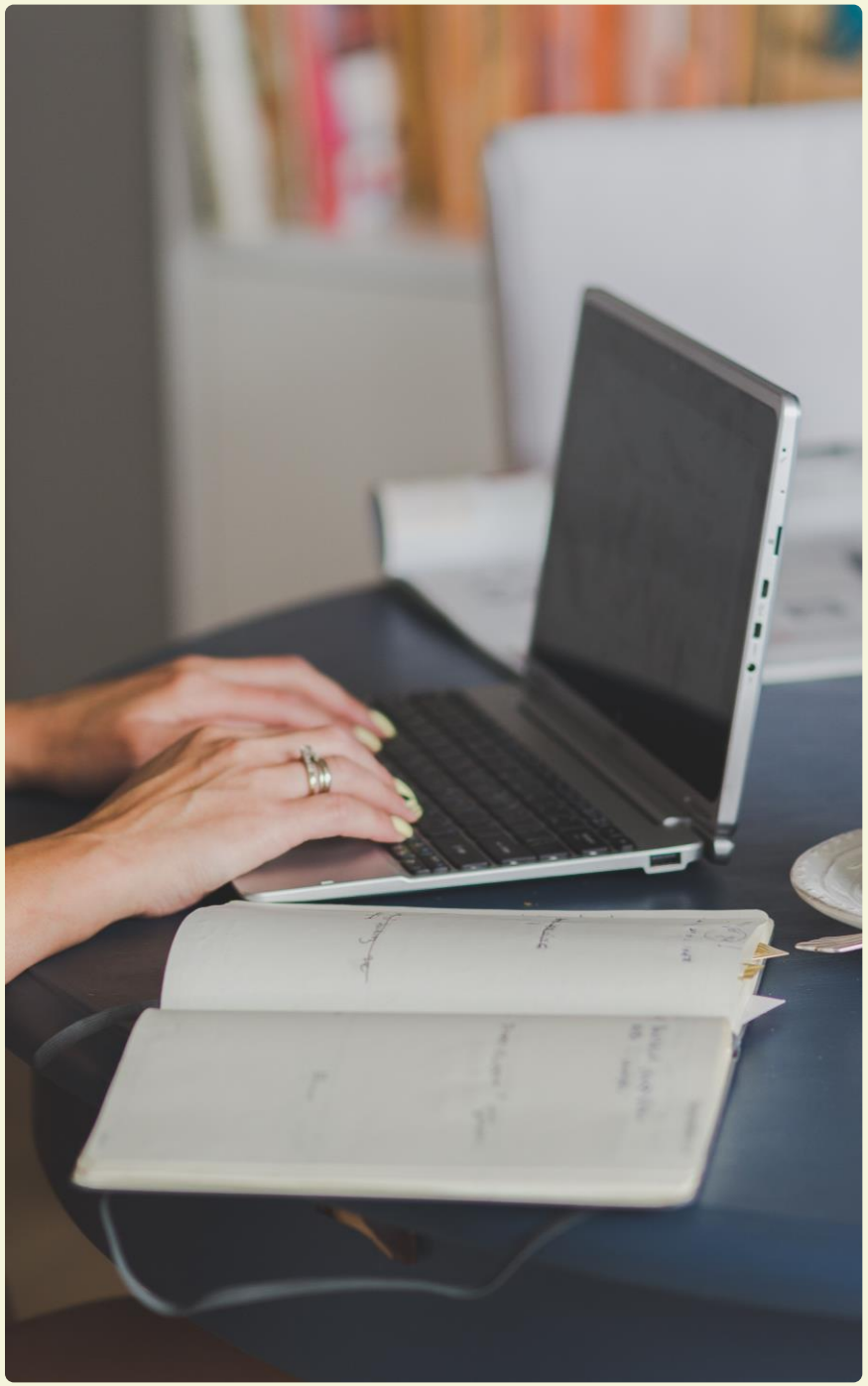
Email analysis
A core pillar of the Sabiki Platform philosophy is being able to view and manipulate everything related to email security at your fingertips. Our email analysis feature will allow admins to easily and quickly review email header information and body preview messages making their daily workflows more efficient. The Email Analysis feature of the console also acts as the admin control point for model training and email manipulation with features such as ‘Seek and Destroy’ which ensures the capability of mass deletion of a single email throughout all mailboxes for those situations where message recall just won't cut it.

Does Sabiki Dynamic Email Security use an AI Engine?

Yes, Sabiki Email security is powered by a dynamic Artificial Intelligence Engine that has been developed specifically to analyze email. The fundamental way modern Machine Learning frameworks are implemented and utilized in Cyber lend themselves to being the most efficient way to decide on how ‘bad’ an email is.

The difficulty in implementing them to analyze email has always been the format of the input data and generally the training dataset itself. Not only are email profiles drastically different between organizations (i.e., subject matter, content, theme, tone and language) but the data contained within an email can range from plain text, to HTML code, it can contain URLs and drastically different header content.

The Sabiki engine has been built from the ground up to take all of this into consideration and our unique ‘Dynamic Engine’ means we do not assume a ‘one size fits all’ model. We provide a pre-trained model that dynamically, organically grows and is tuned specifically on the email flow of your organization.



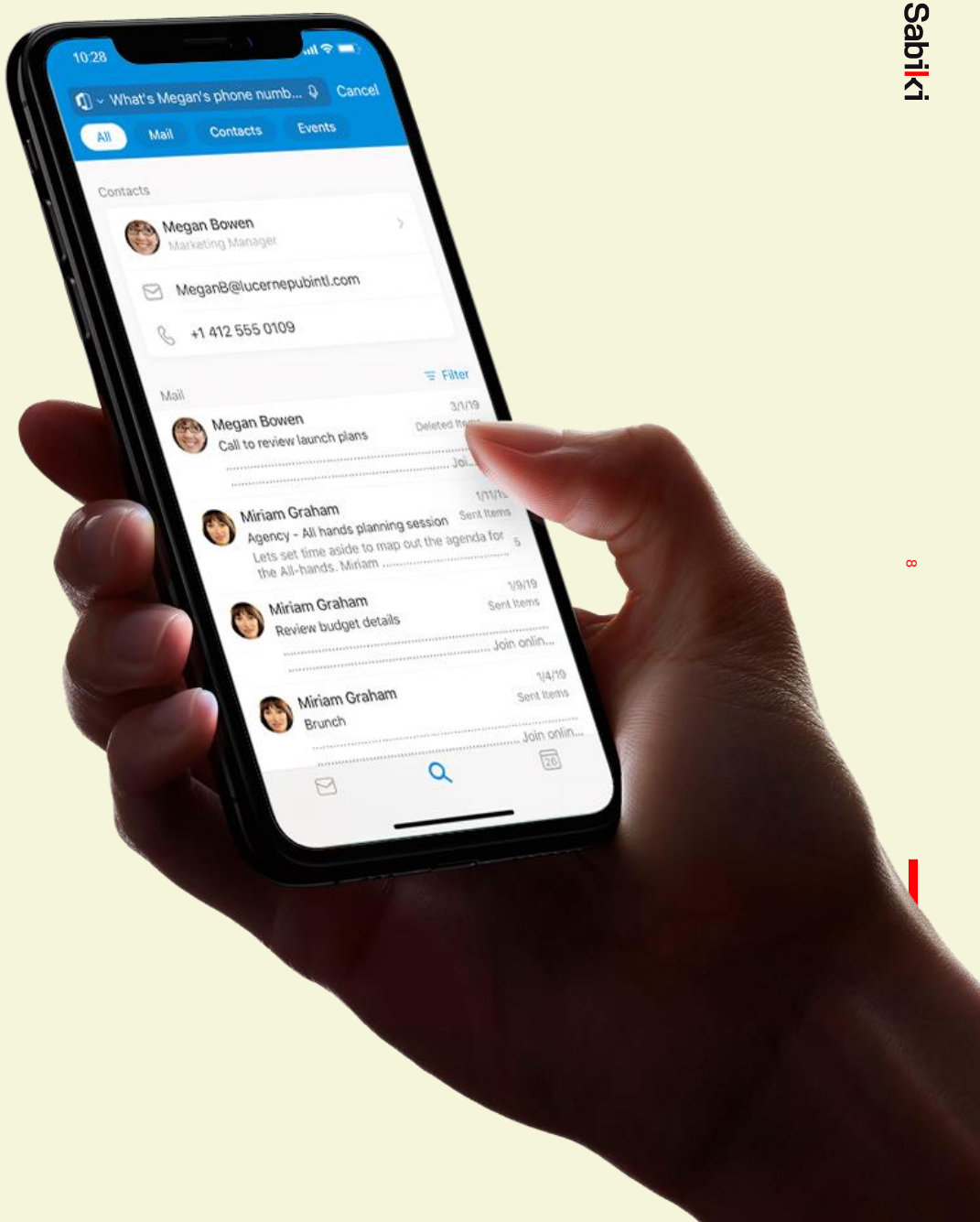
So, we can train our own model?

Absolutely, and you don't need to be a Data Scientist to do so!

Over the years we have seen the struggle of email administrators investing countless hours into policy configurations, custom rule sets and constant worrying over the threat that email as an attack vector is contributing to their environment. The application of AI to Email Security in some way, shape or form is industry standard these days, the question is how to make it as efficient, dynamic and 'personalized' as possible to deal with the most subtle of attacks.

During the Research and Development phase it became clear very quickly that the instant and dynamic nature of email needed an equally dynamic and instant method of Machine Learning. We needed to remove the old workflows of sample submissions back to the vendor, rule sets and models being updated monthly, quarterly, yearly. That's why every deployment of Sabiki Email Security is its own living and breathing model that will only ever increase in efficacy as it is used in production.

Each tenant configured within the platform has its own unique model, pre-trained and ready to go out of the box. Combining this with the Dynamic training 'feedback loop' provides a solution that is agile enough to deal with the dynamic nature of email security.



How long does it take to train, and how do we train it?

Don’t worry, we have primed the engine for you!

It wouldn’t make sense to provide a completely blank model and then expect admins to sit there for months on end trying to train it up, we have primed and pre-trained the ‘out-of-the-box’ engine with a vast data set that sees the capture rates of our customers instantly improve. It is not uncommon to see 10x improvements for heavily targeted environments or inboxes.

We could just release a model, update it once a quarter and still claim to be a robust, valuable security control on top of what customers may already have.. though the real benefit of a dynamic engine is our ability to expose the training workflow and have it trigger on user and/or admin actions.

Was there a false positive? Train on it instantly in two clicks without any sample submission or custom rules.

In the case of a false negative, train on it then ‘seek and destroy’ it instantly from all mailboxes under protection.

The method of ‘tuning’ the engine as we like to call it can be configured by the administrator. We can adopt a ‘trusted user’ method whereby users can drag and drop emails within their mail client can trigger an automatic training cycle of the model. Or we can set it to ‘admin approved’ training mode, where the admin can review the actions of their users and ‘approve’ a training cycle.

What is this ‘Seek & Destroy function I am reading about?

One of the benefits of being an API base security solution is the reach that is capable at a mailbox level.

A unique feature is the ability to ‘Seek and Destroy’ selected emails within all the organization Inboxes. There may be a situation where a disgruntled employee has sent an inappropriate email, or an email with sensitive data has accidentally been sent to all employees…

The admin can perform a mass purge of individual emails directly from the Sabiki console in 3 clicks. Customer feedback is that this has been the ‘go to’ emergency step that is more effective than a traditional mail recall.

It looks like Sabiki does more than just target Phishing; can it be used as a full SEG (Secure Email Gateway) solution?

At its core, Sabiki Email Security has been developed to target the most advanced of Email attacks, namely Phishing and other BEC (Business Email Compromise) incidents. However due to the dynamic nature of the model, it can inherently learn to target any email type and any supported language.

Sabiki Dynamic Email Security is essentially your ‘needle in the haystack’ solution. The built-in layers of Microsoft security handle any connection level security controls (SPIF, DKIM checks for example) so we focus on the essence of the message itself so any mail routing or uploading of blocklists are redundant when working within the Microsoft ecosystem.

With the training data we have used to prime the engine, it has been tested to exceed standard Spam capture rates hence you will note we refer to Sabiki as an Anti-Phishing and Anti-Spam solution. The reality is it can be tuned to target any mail type you decide and also leverage its unique functionality in use cases and workflows never before possible with traditional type solutions.

Is there any attachment scanning capability within the solution?

Yes, Sabiki has an additional engine built-in for attachment scanning. While it is not the core function of the solution, we ensure to give any attachment a ‘second check’ after it passes through the Microsoft 365-attachment scanning workflow.

What about DLP, Encryption etc.?

Sabiki Email Security does not sit at the Gateway.

It is an API based security solution and as such makes it simple to deploy without the need to re-direct mail or make changes to MX records. As a result of this design Sabiki is not involved in the routing or delivery of email, and therefore there are no options in relation to custom mail routing, or extended capabilities such as DLP and Encryption.

Another benefit of utilizing and API based security solution is that it simplifies troubleshooting of mail flow, Sabiki hooks in the instant the delivery routing is complete and is therefore exempt from any involvement in connection level/routing issues that may arise.

Do you have an MSP version of the Management Console?

The Sabiki Email Security platform supports an MSP deployment out-of-the-box.

You can manage multiple email tenants and within each, multiple domains all from a single console.

There is a unique model per Tenant and each tenant can be viewed and managed in a segregated fashion with role-based administration configuration capability .

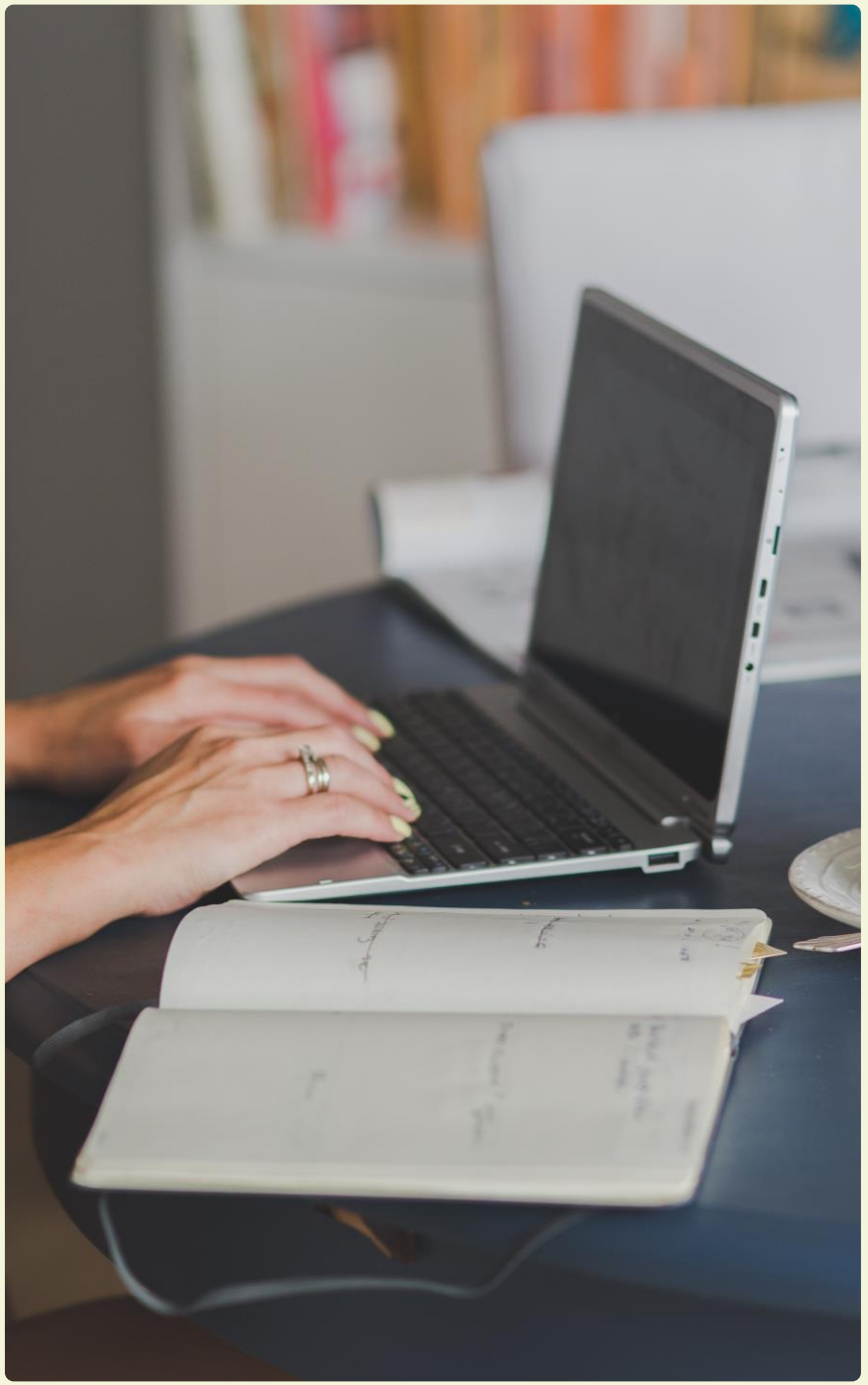
If I'm an MSP, can I give my customer access to just their own console?

Yes, we have granular role-based access rules that can be setup to allow a customer to log into the Sabiki platform but see only their environment details. In addition to this, we can place restrictions over what the MSP is allowed to see within the customer mail environment.

There are some powerful features such as email analysis that the customer might want to exclusively view and control for example.

Do my customers share the same AI Model?

No, one of the core principles of Sabiki Email Security is that each customer has a unique mail ‘fingerprint’ or ‘mail flow profile’, so it is important to maintain a unique engine model per customer. When a 365 tenant is enrolled into the Sabiki console, a unique model is generated and maintained for that tenant and all its subsequent training cycles.



Sabiki.ai