Trustifi

PARTNER PLAYBOOK

Trustifi's Partner Program enables resellers and managed service providers (MSPs) to offer innovative email security solutions from a trusted industry leader.

Partner With The Fastest Growing Email Security Solution

Through education, support, and resources, channel partners will be empowered to help their end-users gain outstanding capabilities in exerting control over their inbound and outbound data, while protecting their email systems through anti-malware, anti-phishing, data loss protection, threat detection, encryption, and more.

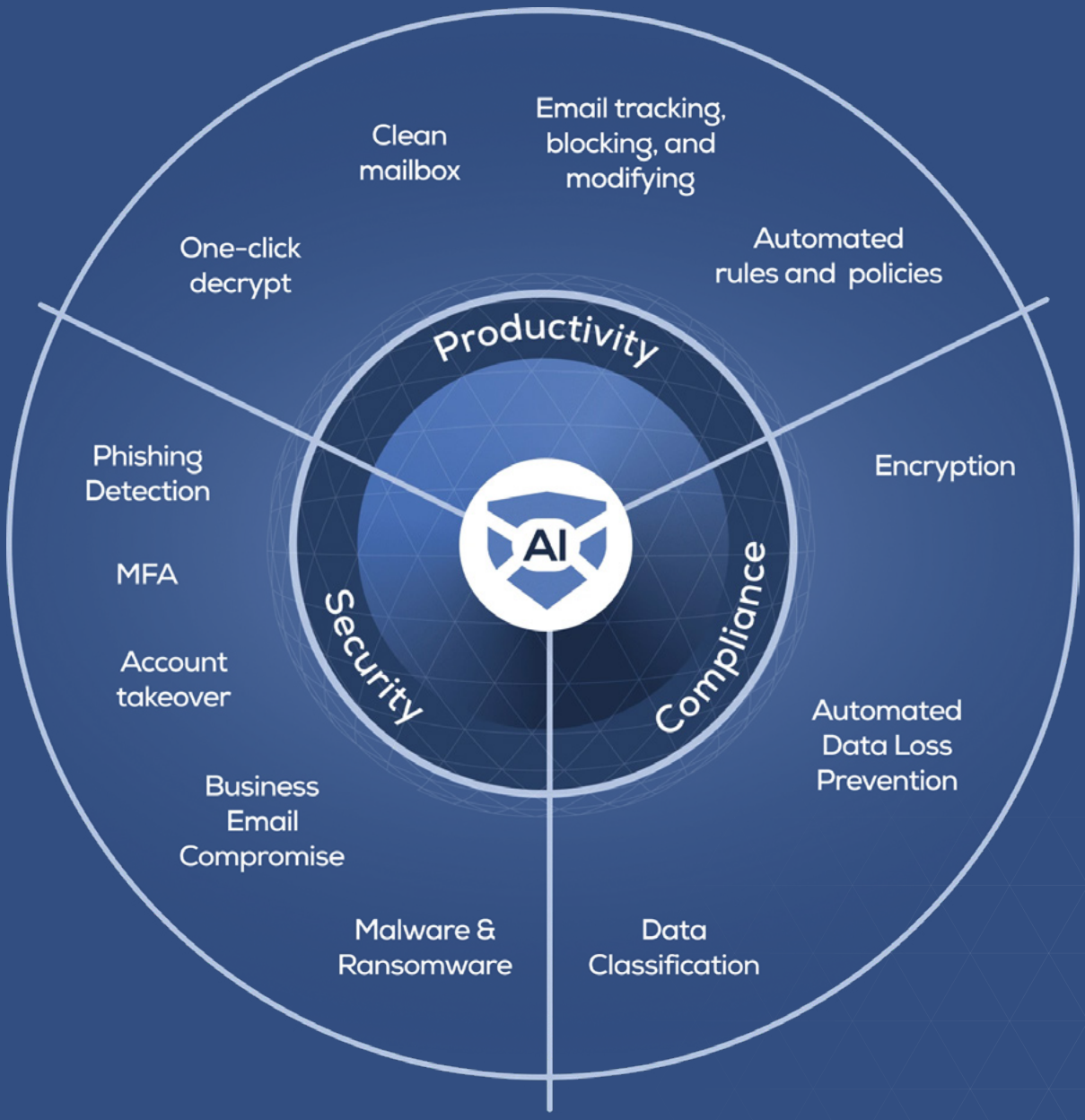
100 word elevator pitch:

> As a leading provider of comprehensive email security solutions, Trustifi offers a robust suite of features to fortify businesses against digital threats. Its AI-powered platform not only defends against phishing, spoofing, and BEC attacks with precision but also provides seamless encryption and compliance measures.
>
> With Smart Indexing Cloud Archiving, Trustifi ensures holistic retention management and eDiscovery capabilities, alongside email restoration functionalities. Moreover, its secure sharing features facilitate safe collaboration with external parties, while the Email Managed Detection and Response (EMDR) Service, managed by cybersecurity experts, provides ongoing vigilance against emerging threats.
>
> Trustifi embodies the essence of a unified, all-encompassing solution for unparalleled email security.

50 word elevator pitch:

> Trustifi leads in comprehensive email security, providing robust features to fortify businesses against digital threats. With AI-powered defenses against phishing, spoofing, and BEC attacks, seamless encryption, compliance measures, and Smart Indexing Cloud Archiving, Trustifi offers a unified solution for unparalleled email security.

360° Email Protection For Ultimate Peace of Mind Against Advanced Email Threats



Trustifi Products and Descriptions

Inbound Shield™

Advanced threat protection prevents the widest spectrum of sophisticated attacks before they reach a user's mailbox. Our comprehensive cloud-based email security solution acts as an email filter, using sophisticated AI to scan inbound emails, effectively identifying and blocking email threats.

- Text-based analysis using sophisticated AI– catches all types of impersonation, spoofing, spear phishing threats and BEC (Business Email Compromise)
- Full URL and files scanning (URL protection blocks malicious URLs from any device)
- AI filters to keep mailboxes clean of SPAM/GRAY emails to prevent phishing attacks (spam filtering)

Outbound Shield™

Mitigate human error and sensitive data leakage with easily enabled DLP to automate email scanning and 256-bit AES encryption.

- Set up outbound email encryption rules and threat protection policies for your entire organization in minutes
- Intuitively designed user experience – open encrypted emails with one click by selecting the best email security solutions from Trustifi
- Remain fully compliant with 10+ frameworks with one click

Account Takeover Protection

Detect anomalies in user behavior with contextual signals

- AI deeply learns the behaviors of every user profile
- Automatically alerts admins and end users of any suspicious account activity, offering robust protection against sophisticated email attacks
- Neutralize advanced threats in real-time by instantly blocking taken-over or compromised accounts

Smart Indexing Cloud Archiving

Easily preserve, retrieve, search, and share all email communications in a secure manner with a next-generation eDiscovery for a single-point-of-truth.

- Retention management
- eDiscovery
- Restore deleted emails
- Secure sharing
- Specific query-sharing capabilities
- Email status and tracking information display

Email Managed Detection and Response (EMDR) Service

Expertly-managed email security. Trustifi's team of cybersecurity experts can remove workload from your IT team by performing the necessary tasks to maintain your email security environment.

- Daily review of quarantined emails to identify potential false-positives or false-negatives
- Identifying potential weak points in your organization's security posture
- Updating and maintaining allowlists and blocklists
- Finding and fixing misconfigurations related to email security

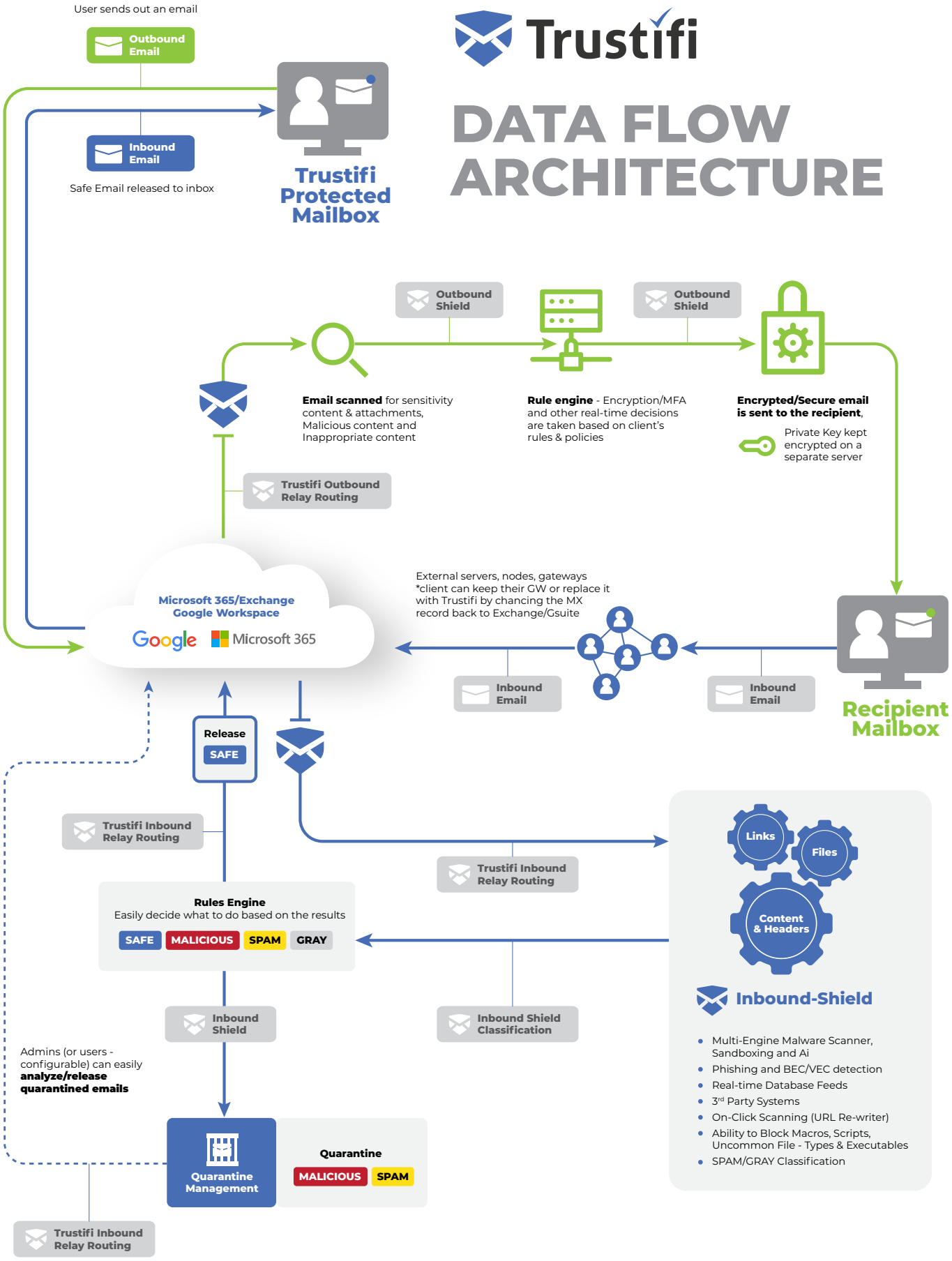
Security Awareness Training

Identify users who are most vulnerable to phishing attempts, allowing IT administrators to apply warning banners and training strategies to users who fall prey to mock phishing attacks.

- Send realistic-looking threat simulation campaigns to test security awareness
- View real-time advanced analysis of user engagement with the campaign
- Gain insights into the organization's overall security awareness level, and identify risky users
- Educate users on how to successfully detect and avoid phishing attacks

Trustifi

DATA FLOW ARCHITECTURE



Target Personas

	CISO	Midlevel
Job Titles	CTO, CISO, CSO, VP of Security, VP of Network Security or senior-level executive of security	Security analyst, IT Director, IT manager, security engineer, security manager, systems architect
Responsibilities	• Protection of the organization's enterprise-critical assets • Selection of security tools that are within budget and work with existing security tools • Reporting on the successes and failures of cybersecurity objectives	• Plans and executes cyber operations, gathering cyber intelligence • Implements phishing prevention strategies • Secure critical network assets and sensitive information • Keep current with new cyber threats and tools available to help prevent them
Challenges	• Increasing cyber threat landscape, ransomware, and phishing attacks • There are many security tools available on the market and selecting the best ones • Failure to detect and prevent a cyberattack could lead to a breach or loss of sensitive data	• Keeping users and company safe within their email inbox • Securing sensitive data in transit and at rest • Providing end users with user-friendly security tools
Cares about	• Return on investment on security tools • Ability to prevent cyberattacks on critical assets • Protecting shareholder interest and brand	• Making an error that could cause the network to be breached • Learning and working with useful new tools available in the market • Keeping up to date with the latest cyber threats
Why Trustifi	**Company and brand protection, and cost** Trustifi empowers organizations to bolster their email security, fortifying the most crucial communication channel for businesses. Safeguarding against sophisticated email attacks, it not only enhances the overall security posture but also upholds the brand's reputation.	**User-friendliness and keeping the network safe** Trustifi empowers users to navigate email with absolute peace of mind. Its user-friendly capabilities distinguish Trustifi from legacy systems, ensuring the organization remains resistant to the most sophisticated phishing attacks.

Common Objections

On The Demo

Q: I already have Microsoft Defender

A: MS Defender can catch and detect many threats, however, to get the full protection capabilities of Defender you will need to buy the E5 tier licenses for all of your users – which are very expensive. On the other hand - the basic E3 licenses are not expensive but fail to catch many advanced threats (see Trustifi vs. Microsoft battle card).

By keeping (or downgrading to) the basic MS E3 licenses and adding Trustifi, you can save a lot of money and be more protected against all threats compared to just using MS E5. We even have a cost-savings calculator for this purpose: https://trustifi.com/microsoft-cost-savings-calculator.

Q: I have an email gateway in place

A: There are many kinds of threats that SEGs today cannot catch. Specifically, SEGs are more focused on catching threats carried by "active payloads" like known phishing links and malware distributed through files, while being vulnerable to threats like zero-day attacks and content-based attacks without active payloads.

Most importantly, SEGs do not scan or protect internal traffic – since the gateway is set up at an MX level, and internal traffic goes through internally without passing through the gateway. If an internal mailbox is compromised, or if an employee goes rogue, a SEG offers no protection against malicious emails being sent from within.

Trustifi's email relay solution protects both external and internal traffic, while also being much easier and quicker to set up. If you want to keep your SEG, Trustifi deployed as a relay can work perfectly fine alongside a gateway, and can help stop any threats that the SEG fails to catch initially.

Q: I'm just looking for information (pricing), I don't need anything right now

A: Don't think this requires a technical answer, it's more salesmanship to emphasize the need for an email security solution and create urgency in making a decision.

Q: How long does it take to deploy? /I don't have the manpower to install something like this right now.

A: Each of Trustifi's protection modules takes mere minutes to set up, and the process is very easy. We have an automated deployment wizard to create the necessary connections with Trustifi, detailed step-by-step documentation and our team is available to walk you through the entire onboarding process including customizing and configuring the solution.

In terms of manpower on your end, it really takes just one person to provide access to your mail server in order to create the connection. The Trustifi platform is very easy to use, but if you don't have any manpower available to operate day-to-day operations, we offer an EMDR (Email Managed Detection and Response) service, performed by veteran professions in the cybersecurity field who can personally take care of your daily email security operations.

Q: How do you migrate from another solution?

A: It's possible and easy to migrate to Trustifi from another solution thanks to a couple of key features in Trustifi:

- Trustifi is very easy to set up, and can even be installed alongside an existing SEG for a trial period if needed
- Trustifi allows importing your existing allowlists, blocklists, contact lists, and archives easily through our management platform
- The deployment of Trustifi is very flexible if you want to set up a limited scope POC that will only apply to certain people or groups in your organization

Q: How is Trustifi different from xyz

A: If you're looking for a direct feature comparison, see the relevant battle card for that system. If the question is more general, there are a couple of distinct things that make Trustifi unique:

- **Extremely easy to deploy, configure, and manage**. Our relay deployment is very quick and simple: we offer step-by-step documentation for the onboarding process, a dedicated onboarding wizard in the Trustifi platform, and an automated deployment wizard that can create via API the relay connection itself in a few clicks. Our team is happy to help with the process as well, though many clients just go through the onboarding process by themselves because it's so simple.
- **Strong AI threat detection accurately detects spam, graymail, or content-based attacks that are becoming more frequent every day**. Many competitors focus on threats carried by active payloads such as phishing links and malware, but today more and more phishing attacks are carried out via impersonation and text-based attacks that can only be caught by a strong AI engine like Trustifi's.
- **A truly complete email security suite.** Trustifi offers a complete email security package including: encryption and MFA, automated DLP, look & feel customization, protection against all inbound threats, sandboxing, DMARC analyzer, account takeover protection and monitoring, secure file transfers, archiving, e-discovery, security awareness training, and more.
- **Trustifi's RND team is extremely agile and flexible, and very open to requests and suggestions from our clients and partners.** Many of the features in Trustifi have been added as a result of requests and suggestions from clients and partners.

Q: I have m365, hybrid, on-prem, dedicated server, google

A: Trustifi is fully compatible with all of these environments for outbound and inbound protection.

Q: How does a Trustifi POC work?

A: There are many ways to execute a POC, and Trustifi's deployment flexibility supports this process. Typically a POC would work like this:

A POC group is selected within the organization to test out Trustifi, while the rest of the organization remains unaffected. Trustifi's outbound and/or inbound modules are deployed as a relay to this POC group only, and you may choose to add or remove people from the group as you go along the POC and onboarding process.

You can choose during the POC if you'd like Trustifi to actively protect your mailboxes, either by blocking inbound threats or by encrypting outgoing traffic, or if you want to deploy Trustifi in "Monitor mode" – where traffic goes through Trustifi and data is collected but no changes are made to mail flow.

Trustifi can also be deployed in "Journaling mode" – where only a copy of your outbound/inbound traffic is sent through Trustifi for the purpose of monitoring.

A typical POC lasts 1 - 2 weeks once deployment is finished, and after this time period there should be enough data gathered in the testing process to show the impact (potential or active) of Trustifi protection on your tested mailboxes. Trustifi offers extensive reporting and data visualization to help show this impact in a clear way.

Q: do you integrate with third-party systems like awareness training, ticketing systems

A: The general answer here is that we do, though to provide more details on how we do this we would need to know which systems are being used. For some systems, we offer this integration pretty much out of the box, and for others, an integration would need to be created via development work.

Worth mentioning that in most cases, whatever service this 3rd party system is doing – Trustifi probably offers the same service as a built-in part of the full suite.

Q: Can Trustifi ingest our allow/block list

A: Absolutely, Trustifi can easily import any existing allow/blocklist from other solutions.

Booking a call

Q: I have a solution in place

- **A:** Mr. Customer, I completely understand your position and I wouldn't be calling you and not expect you to already have a solution in place. However, when you see how we are able to identify phishing and spoofing attacks that your current solution is missing through our dynamic AI scanning, I am confident you will be interested in taking a further look. Are you available on Thursday at 1?
- **A:** Mr. Customer at this point all I am asking you to do is take a look into Trustifi if you think your current solution is better I will respect your decision and make sure no one from the org ever contacts you again. How does Wednesday at 2 work for you?

Q: I do not have the budget for this right now

- **A:** Mr. Customer, at this point I am not asking you to buy anything, I am just asking you to look at the solution. We are a fast fast-growing company, and we value the feedback from leaders in the space like yourself. How does Wednesday at 2 work for you?
- **A:** Mr. Customer I understand you don't have the budget for any new technology at this time however I understand that you are an experienced professional in the space and part of your job is to be aware of the leading solutions in the market I am only asking if we could schedule some time to look at the platform and get your general feedback. How does Wednesday at 2 work for you?

Q: Not interested

A: I agree I would have to say that if I speak to 10 people they have the exact same response, However after looking at our solution and seeing how we are able to (insert value prop) protect the company from malicious phishing attacks 7 out of the 10 companies actually take a demo and become customers after seeing how our solution is able to highlight the malicious emails your current solution is missing. Would you prefer Wednesday or Friday at 11?

Q: Send me an email / follow-up at a later date

- **A:** I would be more than happy to send you an email; is your best email still: however what other customers have told me in the past is that an email doesn't properly demonstrate the value of the platform. They told me they were much better served by taking 20 minutes to look at the platform and speak with a technician. How does Monday at 1 work for you?
- **A:** I will send you an email with further information and after your review, I am sure there will be additional questions, what we can do is put together a calendar invite for (date and time) and I will include my Trustifi contact to answer any additional questions you may have after you had a chance to review the information