Trustifi

WHITE PAPER

Microsoft Email Security Is Not Enough.

Why experts are saying businesses need to add a layer of security.

www.trustifi.com

As the adoption of cloud email systems continues to grow, security and risk management leaders are forced to evaluate the native capabilities offered by providers.

In the absence of an additional layer of protection, legacy email systems or secure email gateways often cannot prevent sophisticated social engineering attacks and malicious emails.” *

“The pandemic and the upsurge of remote work has led to an increased reliance on email as a communication method that requires more than simple gateway data protection.” *

“Ransomware, impersonation and account takeover attacks are increasing and causing direct financial loss, as users place too much trust in the identities associated with email. The evolution in these types of threats has led to an increased demand for new techniques and services.” *

> Continued increases in the volume and success of phishing attacks and migration to cloud email require a re-evaluation of email security controls and processes. Security and risk management leaders must ensure that their existing solution remains appropriate for this changing landscape.”

Gartner’s Market Guide for Email Security October 2021

*Gartner®

Microsoft Protection Features Are Outdated

Out-dated technologies, such as legacy email systems and secure email gateways (SEGs), are complex and expensive. Microsoft lacks advanced anti-phishing and other latest threat protection capabilities.

Gartner analysts say that, "Microsoft's default email security capability (Exchange Online Protection (EOP)) lacks advanced anti-phishing and other threat protection capabilities. ... **You should evaluate Microsoft's built-in email security solution and consider augmenting or replacing it with a third-party solution if it doesn't meet your requirements**."

What Does Microsoft Provide?

Gartner reports state that: "SEGs are still the most common deployment of email security" and that "By 2023, at least 40% of all organizations will use built-in protection capabilities from cloud email providers, rather than a secure email gateway (SEG)–up from 27% in 2020."

SEGs have traditionally protected incoming and outgoing emails for on-premise systems, whether they were local appliances, virtual appliances, or cloud solutions. Microsoft Defender for Office 365's management console is part of the Microsoft 365 Defender portal. A Microsoft Office 365 SEG offers two email security options, the most basic of which is Exchange Online Protection (EOP). EOP provides the bare minimum level of protection against spam, malware, phishing and other email threats. Advanced Threat Protection (APT) provides a somewhat higher level of protection.

Customers who purchase Enterprise licenses of Office 365, Windows 10, and Windows 11 get Defender's features and its portal at no additional cost.

Without the use of AI engines and text analysis, SEGs can't stop phishing, spoofing and have literally zero detections of any spam emails that do not contain links or attachments.

Adoption of ICES and CAPES

The rapid adoption of cloud email infrastructure like Microsoft O365 and Google G Suite is forcing enterprises to move away from traditional secure email gateways and on-premises hardware. Microsoft and Google cloud email security services are quite popular because of their built-in native features.

But these easily deployed solutions are now recognized as insufficient so that an additional layer of email security that uses API access to the cloud email provider is increasingly being deployed as Integrated cloud email security (ICES) and Cloud-native API-enabled email security (CAPES).

"Initially, these solutions were deployed as a supplement to existing gateway solutions, but increasingly the combination of the cloud email providers' native capabilities and an ICES is replacing the traditional SEG.", says Gartner.

Gartner suggests to check out "Email security solutions that include API-based ICES …", as well as "anti-phishing technology for Business Email Compromise (BEC) protection that use AI to detect communication patterns and conversation-style anomalies."

Trustifi's relay-based security uses sophisticated anomaly detection techniques like natural language understanding (NLU) and natural language processing (NLP). It is specifically designed to address BEC by leveraging AI-powered features that identify these challenging new ongoing conversation phishing attacks, which standard security email gateways can't detect.

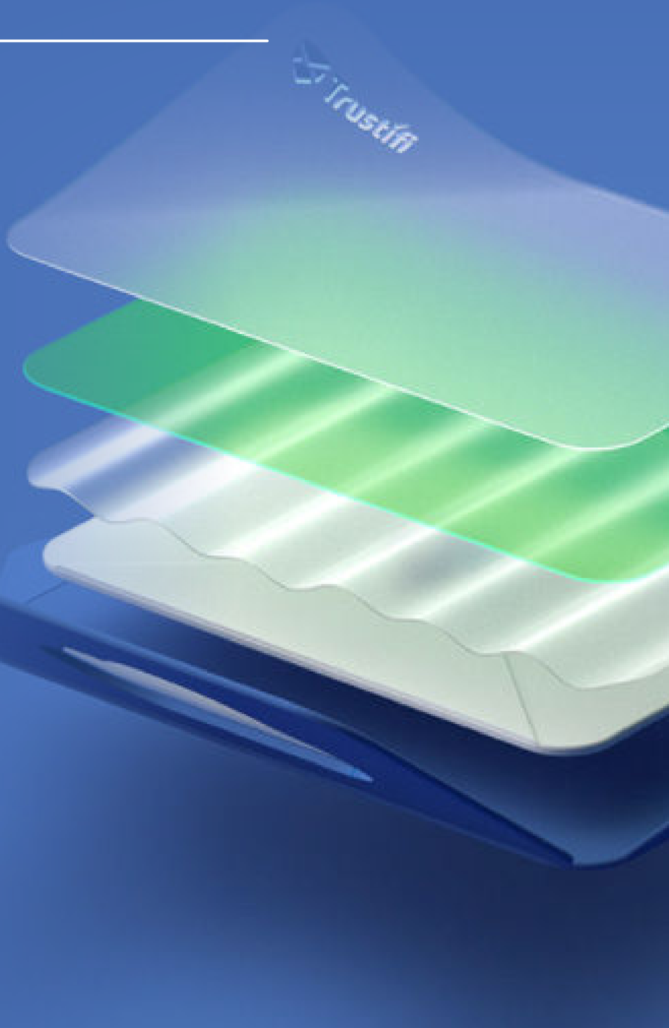
Trustifi – As an Additional Layer or on Its Own

Trustifi provides the best of all worlds!

Trustifi is recognized in multiple categories of email security as a representative vendor in 2021 Gartner® Market Guide with its products –

- ✓ Trustifi Outbound Shield
- ✓ Trustifi Inbound Shield
- ✓ Trustifi Email Account Compromise Detection

Trustifi provides more protection and lower costs in a simpler straightforward interface that can be deployed on top of Microsoft or on its own to get the best of all scenarios in terms of security, ease-of-use and price.



Trustifi Catches What Microsoft Misses

> *"Microsoft is missing so many attacks that are picked up by Trustifi – and we can prove it! We have so many examples of Microsoft letting things through. The architecture works like this – when Trustifi is deployed as an additional layer on top of Microsoft, Microsoft scans the emails first. This means that Trustifi gets all the emails that Microsoft lets through, so we know for a fact that they missed them."*, says **Maor Dahan**, Chief Technology Officer at Trustifi.

Internal Study Shows What Was Missed by Microsoft but Caught by Trustifi

76%

Spam – Microsoft misses ~76% of the spam emails.

65%

Malicious Links (**primarily Phishing**) – Microsoft misses 65%.

--

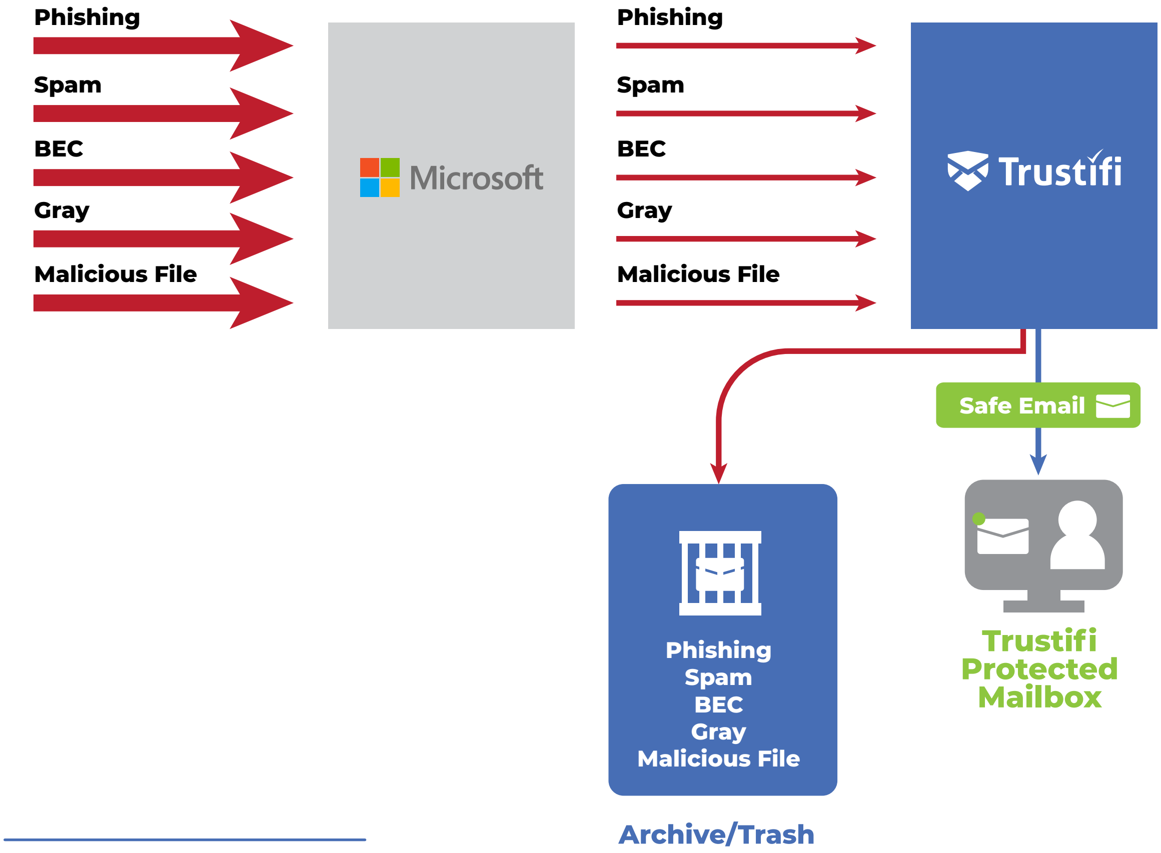
Gray – Microsoft does not have GRAY mail classification.

38%

Malicious Files – Microsoft misses 38%.

93%

BEC/VEC Emails – These emails are usually just text and do not contain any links/or files – Microsoft misses 93%.



Shocking statistics! – Microsoft misses 76% percent of the spam emails, 65% of malicious links, which are primarily phishing, and 93% of BEC/VEC emails.

Traditionally, malicious emails, might contain viruses, trojans, bad attachments and so on. Microsoft is okay for handling these, which currently only constitute about 5 or 10% of the new types of malicious emails that are landing in your email boxes.

Without the use of an AI engine and advanced text analysis for spam, Microsoft is unable to handle the new phishing methods.

Customize Your Unique Solution in A Few Quick Clicks

Microsoft

Activating Microsoft 365 Defender is easy, but configuring and managing it is an extremely complicated challenge that most companies find insurmountable and thus don't or can't take it on. As a result, they suffer the consequences of severely deficient protection.

The Microsoft security solution has a variety of systems that must be configured, such as Microsoft 365 Defender, ATP, EOP (Exchange Online Protection) and more. Without being a trained Microsoft engineer who knows all the ins and outs of setting up proper data loss prevention policies and rules, there is no way to get the protection that Microsoft promises.

In addition to being extremely complicated, they lack a wide variety of security finetuning options, such as the definition of policies and rules. For example, you can't define that a specific email detected from a specific sender to a specific recipient should trigger a specific action.

Trustifi

Every company has their unique email security problems. Legacy SEG solutions are not built for this. With Trustifi a single click enables you to resolve the specific challenges that your company faces. Trustifi's simplicity and flexibility makes it very easy to protect, address and deploy protection from a rich variety of security risks, while easily configuring Trustifi to protect the specific requirements of your organization.

Trustifi is a much more flexible and simple-to-configure product that enables a company's security representative to achieve optimal results without any learning curve. This enables them to focus on handling the bigger problems.

Trustifi also enables you to easily roll out a policy to your entire organization or a group in a single click, while providing significantly more flexibility, options and actions.

Customizing Your Email Brand Identity

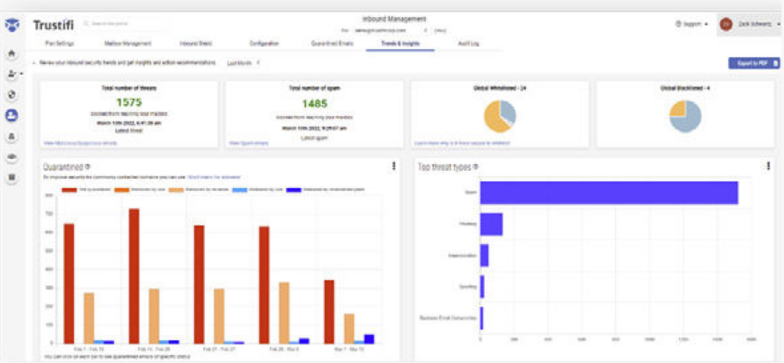
With Trustifi, it is simple to build customer trust and loyalty by creating a consistent corporate brand identity for all outbound emails. You can easily set up and send highly customized emails with dynamic fields to suit any recipient or purpose from your code (no complex third-party apps). Microsoft doesn't provide this simple functionality.

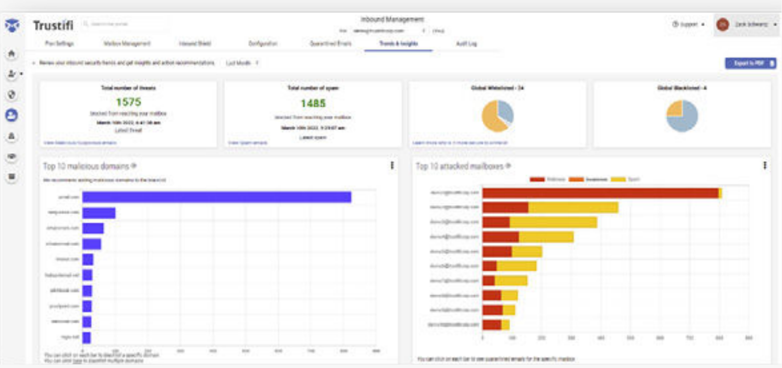
Single Pane of Glass

You can see the big picture and drill down into the details in a single click.

Microsoft

Microsoft 365 Defender, ATP, EOP and the other Microsoft systems don't communicate each other. Each of its services has a different dashboard, so that it is extremely difficult to get a report or understand why an email was quarantined.



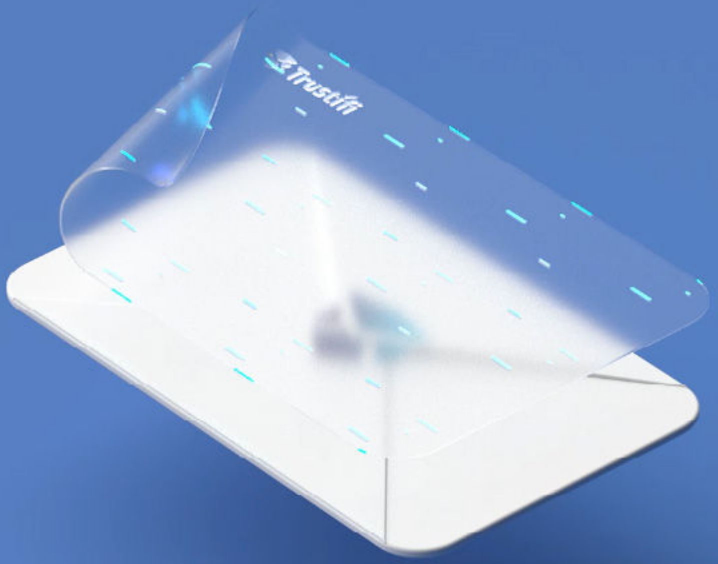


Trustifi

Here's a look at some of our single-click dashboards that provides an at-a-glance view of trends and insights and single-click actions in a single pane of glass.

These dashboards not only show the organization's security incidents and detections, but also **enable you to implement new security policy actions in a single click.** For example, to click on one of the malicious domains to automatically blacklist it or to click on a bar in the chart to see all the quarantine emails of a specific status or for a specific mailbox.

Inbound Protection



Microsoft

Gartner's analysts say "that Microsoft has two offerings for inbound email filtering: Exchange Online Protection (EOP) and Microsoft Defender for Office 365. … Email security requires more than the basic protection provided by EOP, and Gartner client inquiry data reveals that EOP does not meet the requirements for most of our clients. Therefore, it is highly recommended not to use EOP as the only email security service.

"Microsoft Defender for Office 365 (MSDO) offers a wide set of email security capabilities, but due to the rise in Business Email Compromises, account takeovers and other sophisticated attacks, many times malicious emails are actually missed by MSDO, and in fact by other email gateway solutions as well. Therefore, organizations should strongly consider integrating third-party solutions to strengthen their email security capabilities."

Trustifi

Trustifi's Inbound Shield keeps your organization safe from targeted threats that have powerful multi-layered scanning technology, as well as ML- and AI-based anti-phishing technology for BEC protection that analyzes conversation history in order to detect anomalies. In this way, Trustifi enables analysis, detection and classification of the most advanced phishing, malicious, spam and even gray emails. It imposes a layer of protection between your email system and the outside world by using artificial Intelligence and dynamic engines. Inbound Shield readily identifies and blocks suspicious inbound emails.

In addition to scanning and eliminating malicious content, the Inbound Shield addresses a variety of aspects, including –

- ✓ Imposters sending messages from falsified domains
- ✓ Requests for money transfers and confidential information
- ✓ Links to impersonated websites
- ✓ Phishing
- ✓ Spoofing
- ✓ Reputation
- ✓ Impersonation
- ✓ Business Email Compromise (BEC)
- ✓ Malware
- ✓ New Threats, like Zero-Day

SEGs Can't Catch Phish.

Microsoft

Imposter emails that don't appear to be malicious cannot be blocked or quarantined by SEGs. In a phishing attack, the attacker spoofs an identifiable sender, vendor or website to trick the secure email gateway into believing they are a trusted source. SEGs are built to detect high-volume spam. Phishing attacks, on the other hand, tend to be low volume, targeted and slow, which facilitates their penetration through the SEG. The purpose of secure email gateways is to prevent active, ongoing attacks. In the latest incarnation of phishing threats, however, the attacks are initiated and terminated instantly, before their profiles can be detected by the SEG.

Trustifi

Trustifi's Inbound Shield protects your inbox from malicious links, files, BEC attacks and spam by using dedicated AI and implementing a series of dynamic and comprehensive engines.

But real protection actually starts with a sophisticated email solution that can truly understand the content and context of each email and its user's behavior in order to detect sophisticated attacks.

Trustifi uses its dedicated AI (Artificial Intelligence), ML (Machine Learning) and NLP (Natural Language Processing) to monitor emails in order to detect key phrases, such as requests for credentials, wire transfers, confidential information, Amazon gift cards and so on. Upon detecting suspicious messages, Trustifi flags, warns and notifies relevant administrators regarding such emails.

Business Email Compromise (BEC)

> One of the most common challenges that top level execs tell me about is that they were impersonated. They recognize that they need something more.” says Maor Dahan, Chief Technology Officer at Trustifi.

Business Email Compromise (BEC) and account takeover threats continue to rise, with significant financial losses as a result. These are often very difficult to detect because they don’t contain links or attachments. They rely on social engineering to defraud recipients. In the case of account takeover, there isn’t even any indication in the message headers, so, for all intents and purposes, it’s a legitimate email.

Microsoft

The first stage of a BEC email chain arrives in an executive’s inbox as a simple text email (without links and attachments). These are not handled by Microsoft at all because Microsoft doesn’t have AI-based text analysis. For these types of emails, Microsoft has literally zero detection.

Gartner’s analysts say that. “With the rise of Business Email Compromise-type phishing, no secure email gateway (SEG) is 100% effective in blocking all attacks. This increase requires an additional email security solution for organizations.”

Gartner recommends that security and risk management leaders responsible for email security should, “Use email security solutions that include anti-phishing technology for Business Email Compromise (BEC) protection that use AI to detect communication patterns and conversation-style anomalies.”

Trustifi

To combat BECS, Trustifi uses a variety of advanced detection techniques, including natural language understanding (NLU), natural language processing (NLP), social graph analysis (patterns of email communication) and more.

Business Email Compromise is a multistage attack, which requires multistage protection as follows –

1

Step 1 – Protecting your outbound email

This is the first step in securing enterprise inboxes from BEC attack. Hackers use unsecured outbound emails to learn how your users communicate and with whom, as well as to capture the keys to the castle. They employ a variety of multistage email ploys containing sophisticated stories and buildups. They often start with targeted phishing emails.

Trustifi starts off its BEC protection by encrypting outbound emails, thus preventing hackers from accessing your organization's emails. Trustifi's automated data loss prevention (DLP) encryption ensures that confidential information is protected from the prying eyes of hackers.

2

Step 2 – Inbound Phishing

Once hackers know with whom your users communicate, they will impersonate those known contacts with the intention to perform sensitive actions, such as money transfers and information exposures.

Trustifi's Inbound Shield protects your inbox from malicious links, files, BEC attacks and spam by using dedicated AI and implementing a series of dynamic and comprehensive engines. It can truly understand the content and context of each email and its user's behavior in order to detect sophisticated attacks.

3

Step 3 – Email Compromise

After a user clicks on a malicious link or attachment, hackers can gain access to mailboxes in order to monitor, change and steal data and to secretly use this mailbox to generate more BEC attacks while remaining undetected.

Trustifi's machine learning technology creates baseline profiles of all users in order to detect an anomaly in user access or behavior. Trustifi gives administrators real-time notifications when an account has been compromised.

Outbound Encryption and Data Protection

Gartner says, "*Although email encryption has been available for many years, the workflow is often very poor, meaning open rates of encrypted emails are historically low.*"

Microsoft

Only a trained Microsoft engineer with years of experience is able to set up proper data loss prevention policies and rules in Microsoft.

Trustifi

Trustifi's Outbound Shield provides peace of mind knowing that emails are automatically sent secured and compliant with easily enabled Data Classification and Data Loss Prevention Rules.

Implementation takes minutes with automated integrations for Microsoft Office 365, Exchange on-premise, and Google Workspace. Trustifi provides –

- ✓ Email encryption
- ✓ Data loss prevention
- ✓ MFA methods for recipient authentication
- ✓ Compliance management with one-click compliance
- ✓ Tracking & postmark proof
- ✓ Secure storage and back-up system

Email Encryption and Data Loss Prevention services keep your company ahead of the criminals.

Emails are automatically sent securely and compliant with easily-enabled Data Classification and Data Loss Prevention rules.

With Trustifi, simple guided if-then statements enable you to easily select from a rich variety of options in dropdown menus. Afterwards, you can achieve total compliance in a one-click roll out of your new policy to the entire organization or a group. The Trustifi engine is much more flexible and provides significantly more options and actions.

Trustifi's systems automatically scan and encrypt outgoing email messages according to administrators' policies so any emails that contain sensitive information are automatically secured. This includes emails with sensitive attachments (such as those containing social security numbers), emails containing financial information or credit card numbers, and emails containing sensitive company intellectual property. If an email is sent to an incorrect recipient, the EDP prevents the information from being leaked.

This process is completely automated and markedly reduces the likelihood of human error causing data breaches. In addition, Trustifi allows end users far more control over email than otherwise possible. End users can recall email messages, revoke access to attachments, and prevent email forwarding.

You also have access to full reporting of encrypted emails so you can identify people with risky email behaviors and mitigate against data loss in the future.

Conclusion

Microsoft

Legacy SEG systems are no longer able to keep up with the four pillars of email security –

- **Inbound** – Advanced threats like BEC and phishing, impersonations and account take overs are being missed and labeled as false negatives.
- **Outbound** – Outbound emails containing sensitive data are being sent unsecured BEC because of misconfigurations of DLP/classification. When emails are encrypted, a significant percentage are abandoned without being opened because recipients can't be bothered with the cumbersome processes (usernames, passwords) required to start using encrypted emails.
- **Archiving** – Storing data for ediscovery and compliance requires a vast amount of storage and is very difficult to search and share.
- **Account Take Over Detection** – Cyber criminals can spend weeks or months inside an organization's infrastructure, while monitoring, stealing and changing data without system admins having any knowledge of a breach.

Trustifi

By encrypting email, providing an Inbound Shield that filters malicious email and preventing data loss, Trustifi enables customers to stay one step ahead of their attackers.

- **A Single Platform** – Trustifi addresses all pillars of today's email security requirements in a single pane of glass as an additional layer to Microsoft or on its own.
- **Reduce Latency** – Trustifi's unique architecture utilizes API and email relay technology and thus enables centralized deployment and management that is agnostic to the number of seats or email volume.
- **Increased Productivity** – Trustifi's one-click solutions make it simple to send and open encrypted emails without portals, usernames, or passwords, thus increasing productivity.
- **Mitigating Sophisticated Attacks** – Trustifi utilizes ML -and AI-technology to diagnose natural language patterns and identifies BEC impersonation where others can't.
- **The Simplest Email Security Solution** – Trustifi integrates easily with standard email servers, such as Outlook and Gmail. Even without subscribing to Trustifi's software, the click of a single button encrypts outgoing messages and recipients can open encrypted messages with a single click.

"In a world where it is common place to send and receive sensitive client information, it is vital to have an email security platform that does not make sending this information cumbersome. Trustifi is the best solution I have used to make sending private data easy." a Trustifi customer review.

Trustifi

Contact

Trustifi offers industry-leading solutions for email security, including email encryption, data loss prevention, and advanced threat protection. Request a free demonstration of Trustifi's secure email solution. Connect with Trustifi and see how easily and affordably you can protect your digital assets and keep your employees—and your company—from becoming victims.

☎ **+1 844-249-6328**

@ sales@trustificorp.com