Email Security as a Service (ESaaS)

PROTECT YOUR DATA. FORTIFY YOUR EMAIL COMMUNICATIONS

METCLOUD

GET CONNECTED • CYBER SAFE

Cloud Email Security

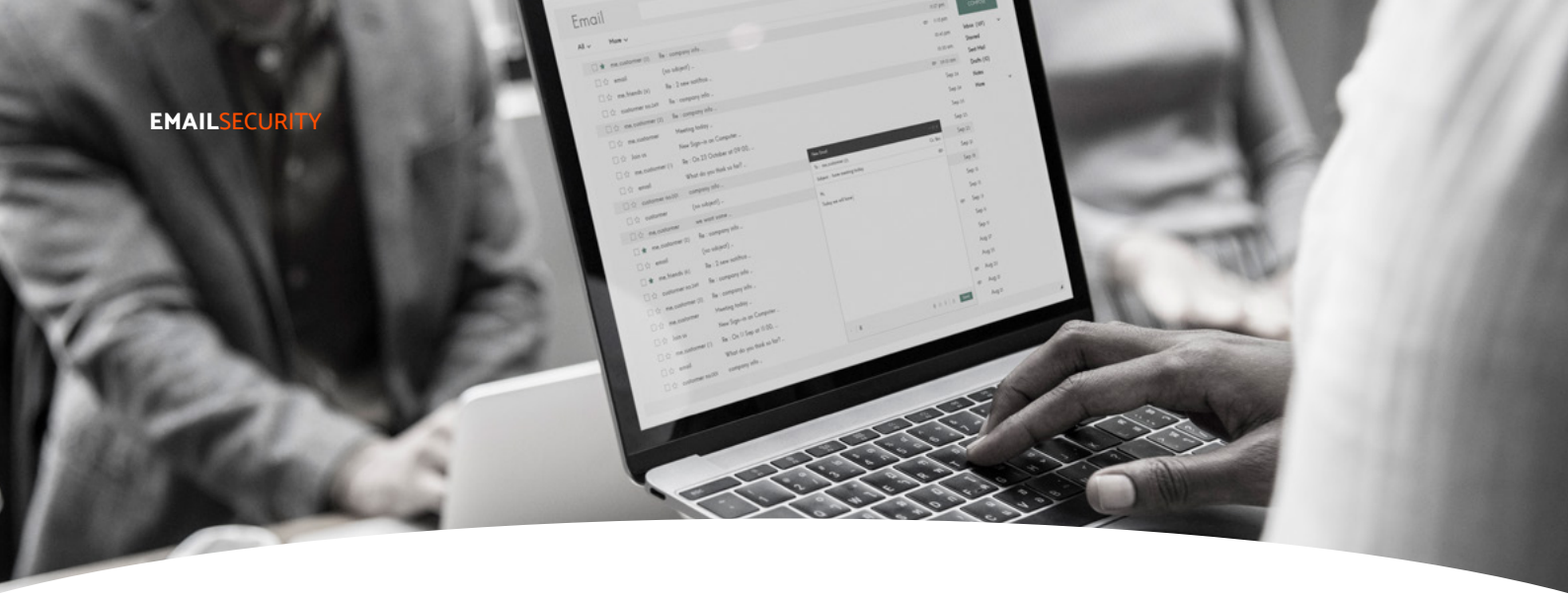
PROTECT YOUR DATA. FORTIFY YOUR EMAIL COMMUNICATIONS

Using cloud email security can protect your systems from unwanted emails or malicious email threats. Cloud email security helps detect and quarantine unwanted emails including those containing spam and bulk emails, malware, ransomware, spyware, and other viruses in malicious links or attachments.

Phishing and spear-phishing attempts, C-level executive impersonation attacks, advanced targeted attacks and more. Cloud email security may also provide other features such as email archiving, email encryption, and data loss prevention functions for outgoing email.

KEY BENEFITS OF CLOUD EMAIL SECURITY SOFTWARE

- Offer a cloud-based, rather than on-premises, email security solution
- Include anti-spam, anti-malware, and anti-phishing capabilities
- Detect and quarantine suspicious emails, including links and attachments



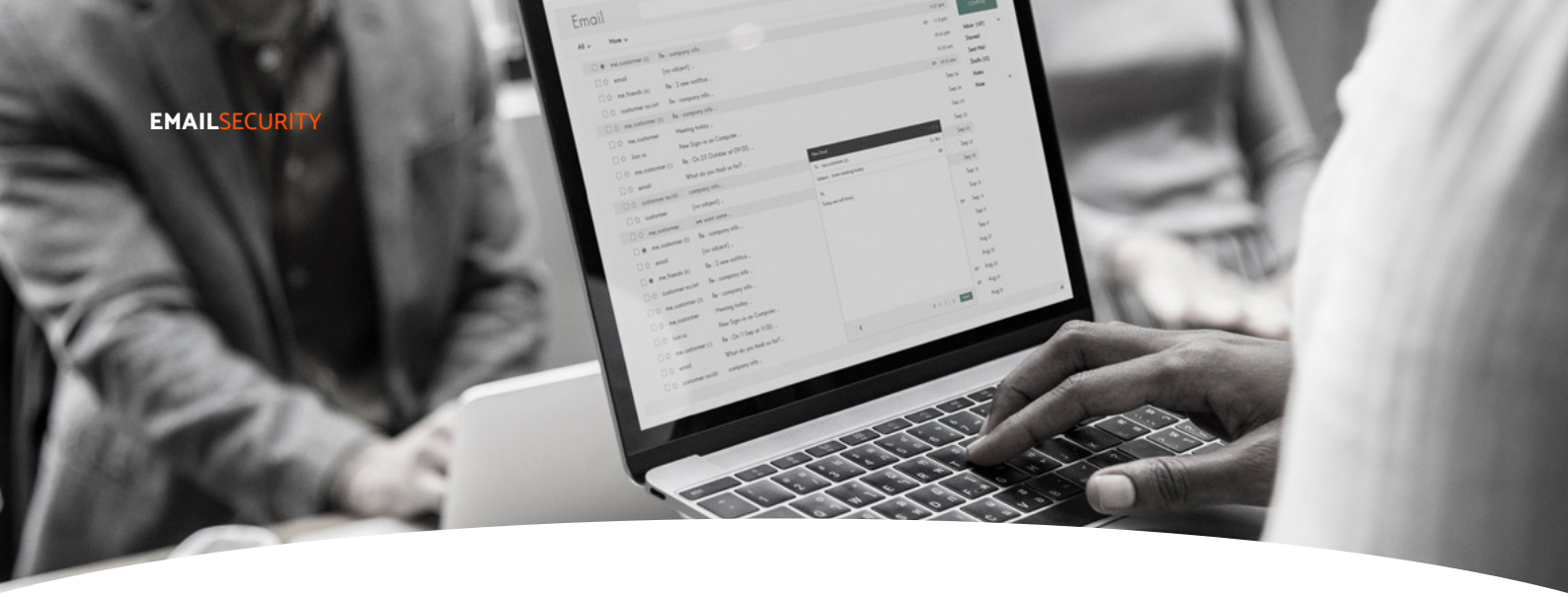
Why you need Email Security?

Cloud email security helps companies protect their cloud-based email communications. Email is one of the most used points of entry for hackers to gain access to corporate systems or to trick recipients into divulging sensitive information. Often, these attacks lead to information or financial losses and reputational damage. Cloud email security software protects against email-focused attacks by blocking or quarantining suspicious emails.

Cloud email security protects against spam, malware, and phishing attacks. Malware attacks, which often originate from emails with malicious links or attachments that unsuspecting users click or open.

- Malware can include ransomware, spyware, or other viruses.
- Ransomware encrypts company files and demands a random to decrypt them.
- Spyware usually sits silently on company systems stealing sensitive information such as intellectual property or trade secrets.

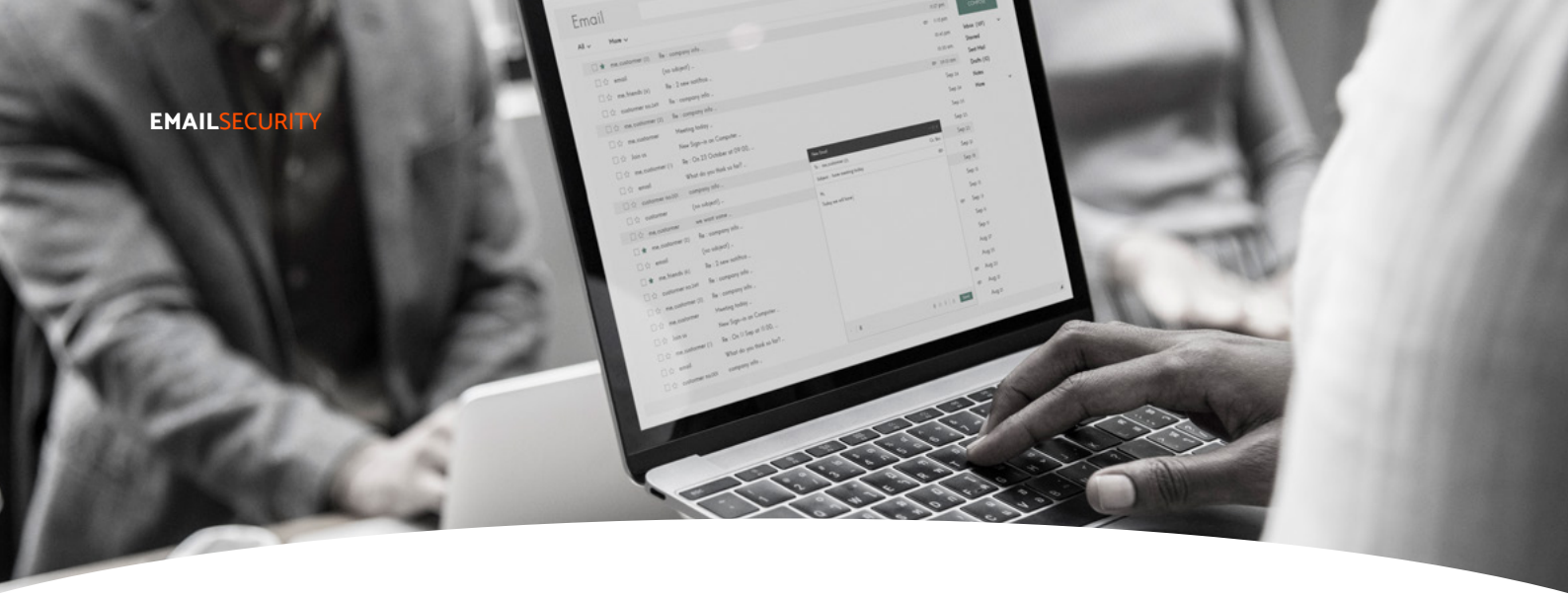
Other viruses seek to embarrass companies and can damage a company's brand and reputation. For example, a virus that sends an email to all the user's contacts, would fall in this category.



Cloud email security software also protects against social-engineering attacks such as phishing, spear-phishing, and c-level executive impersonation attacks.

Phishing attacks are emails sent in bulk aiming to get employees to divulge information, such as sensitive financial information. Spear-phishing is a type of phishing that is targeted to a specific individual. In spear-phishing attacks, hackers spend time getting to know the targeted employee's habits and preferences to send a personalized malicious email. The newest kind of phishing attacks are known as "impersonation attacks," which are often emails sent to company employees impersonating C-level executives which ask employees to make large financial transactions or purchases.

Additionally, companies use cloud email security software to meet regulatory compliance regarding data protection. Most notably, data loss prevention functions in cloud email security solutions help prevent data leakage on outgoing emails. For example, hacked email accounts (known as account takeover) can email out sensitive information. A less sinister example would be when a legitimate employee mistakenly sends out sensitive information such as personally identifiable information (PII), Social Security numbers, credit card numbers, and other confidential data. Additionally, when a breach occurs, reporting functions in the cloud email security platform can assist IT administrators in understanding which accounts were impacted in the incident.



Cloud Email Security Features

At minimum, cloud email security software offers advanced filtering functionality and rule-based actions to prevent email-based spam, malware, viruses, and phishing attempts. Many cloud email security platforms include additional functionality including advanced threat protection, encryption, and data loss prevention tools, among others.

ANTI-SPAM

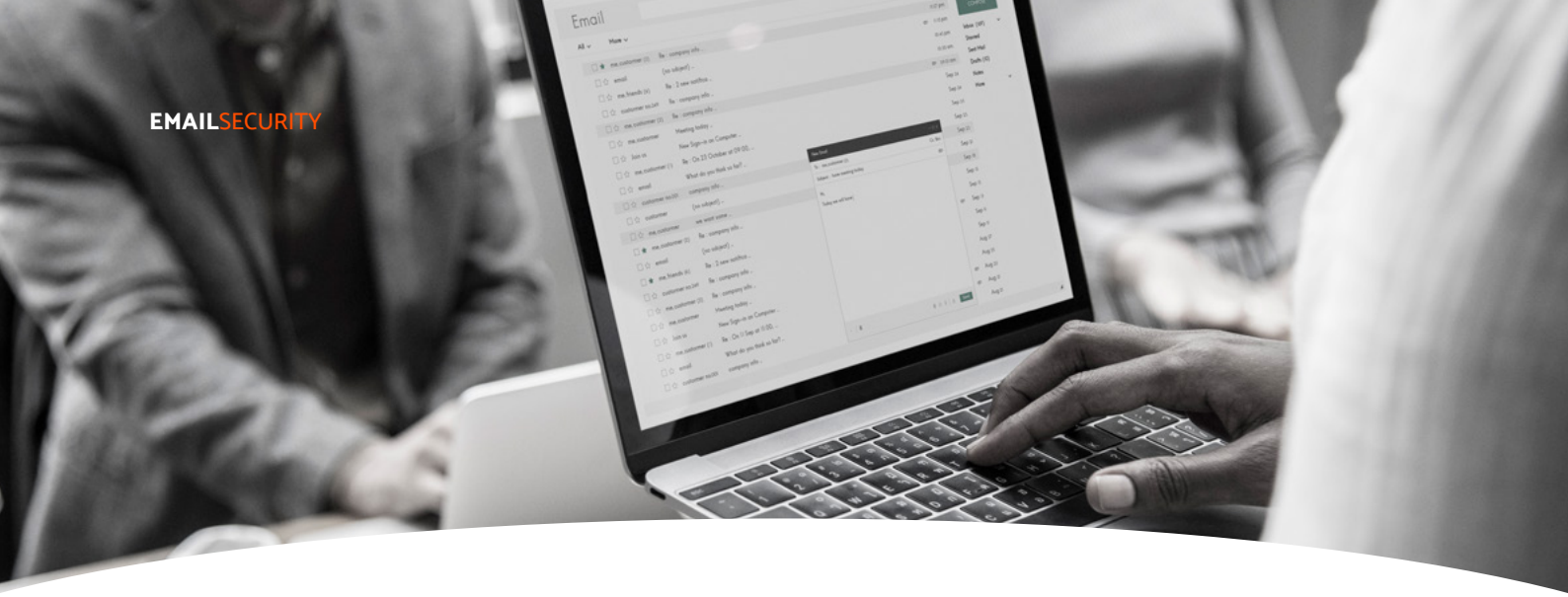
This functionality prevents unwanted emails (bulk, mass, or other junk emails) from reaching recipients mailboxes. Filtering out spam emails can improve employee productivity because employees are not sifting through unwanted emails.

ANTI-MALWARE

This feature prevents emails with malicious links or attachments embedded with malware (ransomware, spyware, other viruses, etc.) from reaching email recipients.

ANTI-PHISHING

This functionality helps prevent social engineering attacks such as phishing, spear-phishing, and C-level executive impersonation attacks.



FILTERING FUNCTIONALITY

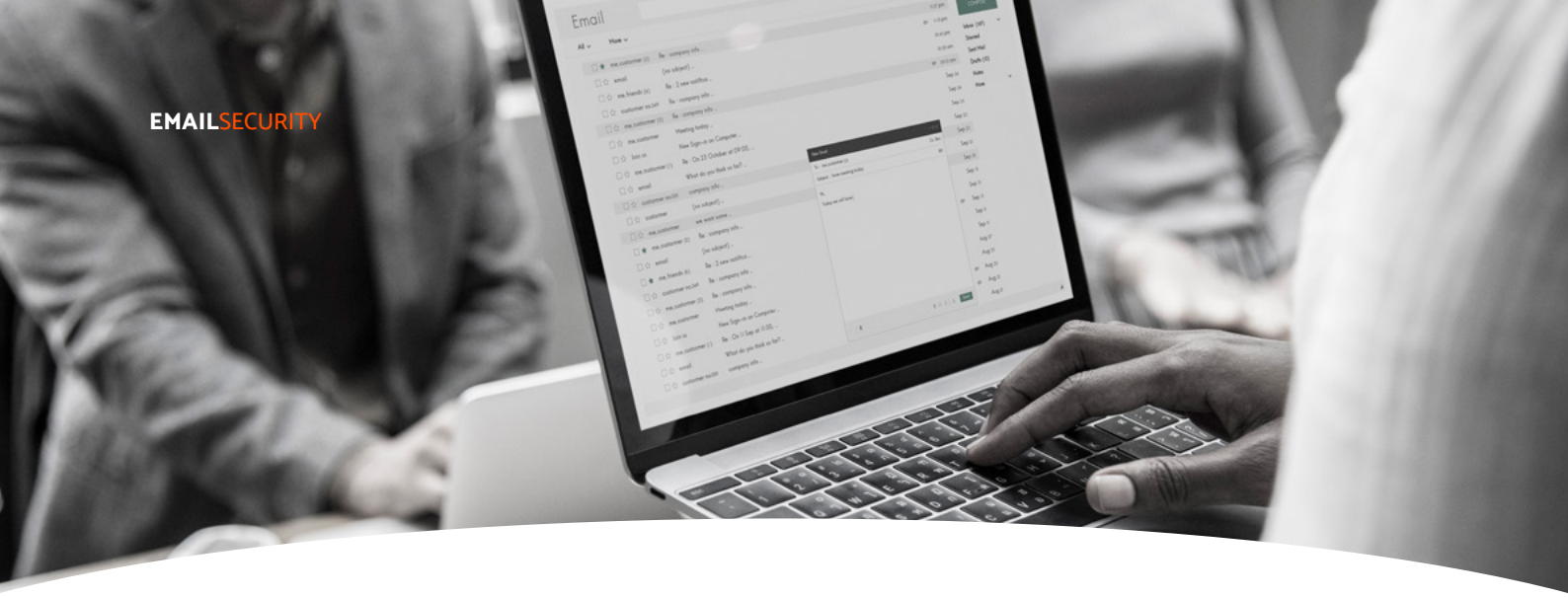
With filters, IT administrators can allow and prevent the delivery of certain kinds of emails to end users. Filters can include approved senders, approved lists, grey lists such as bulk emails that may not be malicious, blocked senders, blocklists, IP reputation, content (such as profanity, credit card numbers, password protected files, and other sensitive information), virus detection, redirects and malicious URLs, newsletter detection, attachment size, and invalid recipients.

RULE-BASED ACTIONS

Using rule-based actions, the cloud email security platform can automatically block, delete, route to tag a subject, copy an administrator, and redirect emails to another email address, among other actions.

GRANULAR SEARCH FUNCTIONALITY

Cloud email security solutions enable IT administrators to locate specific emails using granular search functionality. Users can narrow emails down from sender, recipient, content, and many other factors.



USER GROUPS SETTINGS

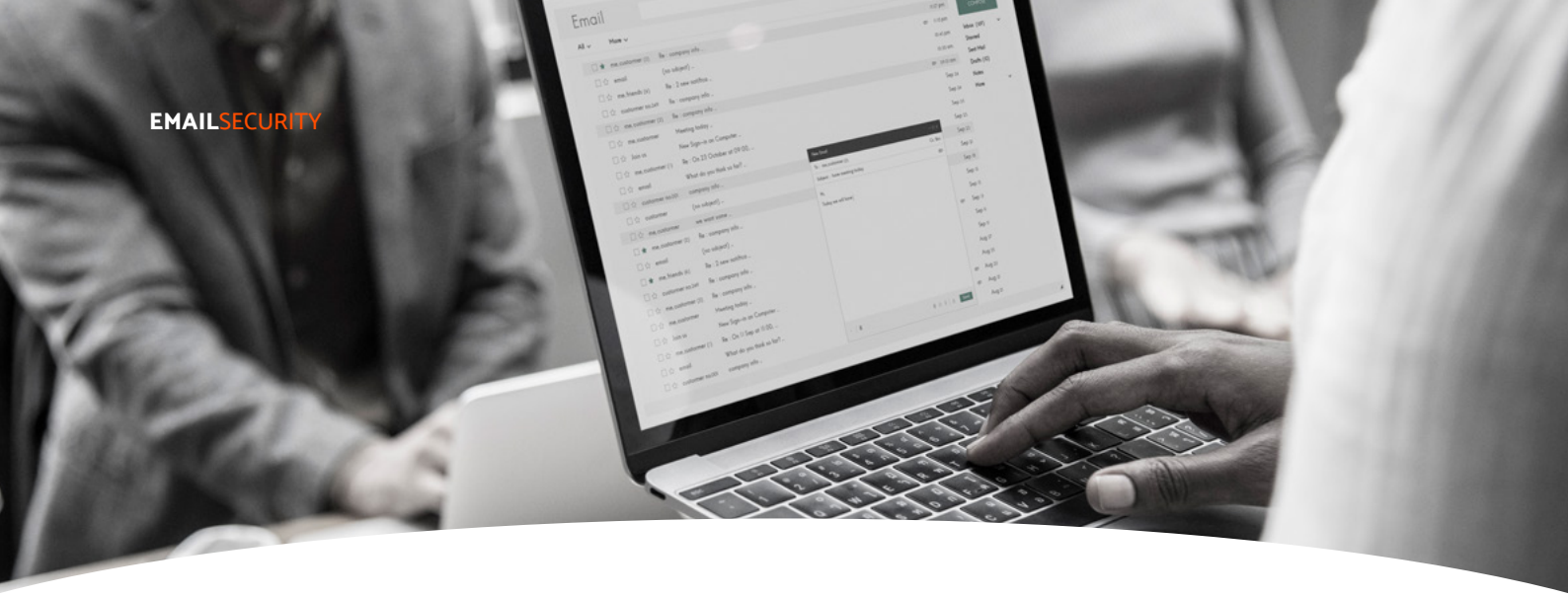
With user group settings, IT administrators can easily manage users by assigning them to groups and applying group settings.

REPORTING

One of the major benefits of using cloud email security is the ability to create reports to understand unique threats over time. Many cloud email security platforms provide incident logging with granular detail, which is required for regulatory compliance.

DASHBOARDS (ADMINISTRATOR AND END-USER)

Cloud email security platforms offer dashboards for administrators to manage their company's email security, as well as quarantine dashboard for end users to review suspicious email activity related to their user account.



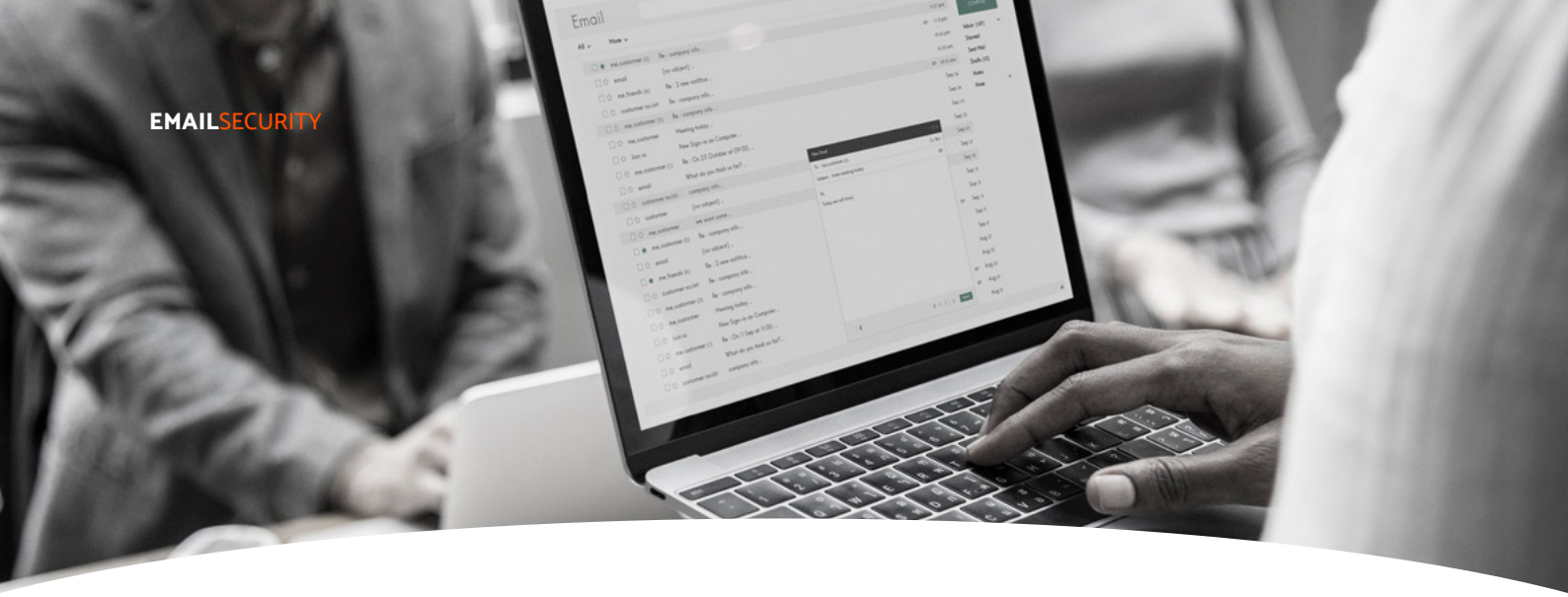
Additional Cloud Email Security Features

ADVANCED THREAT PROTECTION

As email-borne threats become more sophisticated, so must the security tools needed to thwart these attacks. Many cloud email security solutions include further security tools, providing an additional layer of protection on top of standard anti-spam, anti-malware, and anti-phishing functions. Advanced threat protections often include machine learning to conduct abnormal behavioural analysis, display name spoof detection (especially regarding C-level impersonation attacks), detecting lookalike email domains that are visually confusing (such as the letters “rn” looking like the letter “m” when in lowercase. Example, “name@ernail.com” visually looks like “name@email.com”), compromised email account detection, and other anomalies.

EMBEDDED DATA LOSS PROTECTION

While cloud email security is mostly concerned with ensuring the safety of incoming mail, some tools monitor outgoing mail, as well. Monitoring can prevent employees from sending sensitive information externally via email. Monitoring can also include things such as ensuring employees do not use profanity or other non-approved language in their emails to prevent reputational damage.



MULTI-LANGUAGE

Some cloud email security platforms support email analysis in multiple languages and allow custom dictionaries.

EMBEDDED ENCRYPTION

Some cloud email security platforms offer embedded encryption functions, which apply encryption to a company's outgoing emails based on specific policies.

ARCHIVING

Some cloud email security platforms also offer archiving solutions, which are helpful for companies in regulated or legal industries to properly store, secure, and search emails as needed.

'ONE SIZE DOES NOT FIT ALL'

There are dozens of Cloud Email Solutions so how do you pick the right one for you? At METCLOUD we view Email security as just one component of your overall cybersecurity.

Why METCLOUD?

Award winning company for cybersecurity, innovation, and excellence. Our vision is to be the global brand of choice for next generation cybersecure cloud services. Our services have been architected with security by design. Ransomware, Cloud vulnerabilities, Phishing attacks Social engineering and vulnerability management are the five top global security threats. METCLOUD's portfolio of cyber security and cloud services will ensure that you protect, defend, and mitigate any potential cyber attack irrespective of how it was carried out.

Let's get connected.

Call 0121 227 0730
and speak to one
of our experts.

Email the team.
hello@metcloud.com

Visit our website for
more information.
metcloud.com

METCLOUD

GET CONNECTED • CYBER SAFE