LAYERED EMAIL PROTECTION

AN APPROACH DOCUMENT

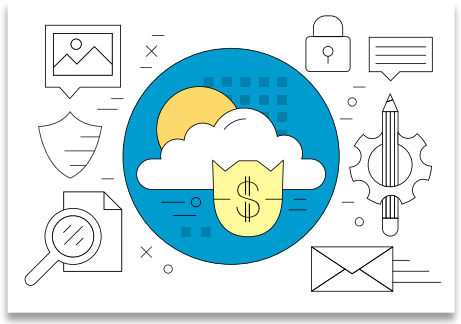
SYNOPTIQ
Infosolutions

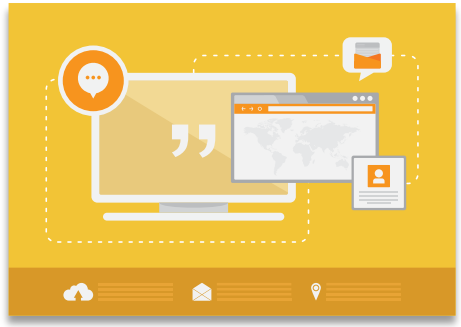
SECURITY SOLUTIONS FOR NON-STOP BUSINESS.

Typical Email Delivery Process

Email Gateway

Email User





Emails are sent for users

They arrive at the gateway

They get validated at the gateway

Emails get delivered to the intended users

Common Misconception

MYTH

Deploying Secure Email Gateway solutions is enough to protect your Business-Critical application: Email

REALITY

In reality, there are multiple layers of protection that you need to deploy in order to secure your Emails and make them always available.

Why Secure Email Gateway is NOT enough

Gateway security is most effective for known threats

Phishing emails always find a way into your setup

Spoofing of domains cannot be stopped by gateway solutions

Email deliverability visibility is a problem

DMARC services from Gateway Security vendors are costly & not their core focus

Email backup and archival must be done in a structured manner

Hence, complete protection can be achieved only with a 5-layered approach

Layered Protection of your Email Infrastructure

1 Secure the Email Gateway

- Stop advanced threats
- Stay Compliant and Productive
- Granularity of security and filtering

2 Post-delivery Security

- Taking remediation action once a potentially harmful email gets delivered through SEG and mail server to end users
- AI based technologies to detect BEC attacks and reporting

3 Making Humans your firewalls

- Create Human layer defense to stop phishing at end-user level
- Providing email assistant which can help them to find the good or bad emails by just looking at email

4 DMARC, BIMI & VMC

- DMARC is a stepping-stone to your Email Authentication; depends upon SPF and DKIM to perform actions
- A proper configuration & alignment of these components are key to DMARC enforcement success
- BIMI and VMC ensure that your branding is visible on all authentic emails.

5 Email Backup & Archival

- Overcoming the restrictions set by cloud email providers by architecting archiving rules
- Being able to granularly restore emails when required

Some Email Security Terms: Explained

DMARC - Domain-based Message Authentication, Reporting, and Conformance

What it aims for: DMARC helps make sure emails from a domain are genuine and secure.
What it does and why it's important: DMARC stops cyber tricksters from faking emails from trusted domains, like banks or shops. It boosts email safety and prevents scams and phishing.
How it can help mitigate: By setting up DMARC, you block bad actors from pretending to be you. It shields your reputation and stops your emails from being wrongly flagged as suspicious.

BIMI - Brand Indicators for Message Identification

What it aims for: BIMI lets email services display your logo next to your emails.
What it does and why it's important: BIMI is like a visual stamp of approval. It helps people recognize legit emails and gives a professional touch to your messages.
How it can help mitigate: With BIMI, people trust your emails more as they can spot your logo. This deters scammers who try to imitate your brand and safeguards recipients from fraud.

VMC - Verified Mark Certificates

What it aims for: VMCs are digital certificates confirming the authenticity of your email.
What it does and why it's important: VMCs validate that you are who you claim to be, reinforcing your email's reliability. They show your email is genuinely from your brand, not a scam.
How it can help mitigate: By attaching a VMC to your email, you prove its legitimacy. This blocks spammers who often send fake emails and ensures your recipients receive trustworthy messages.

We can help you

Synoptiq can help you deploy these best of breed solutions coupled with continuous support for the whole stack.

Call us today!

SYNOPTIQ
Infosolutions

THANK YOU!

contact@synoptiq.biz
www.synoptiq.biz

SYNOPTIQ INFOSOLUTIONS
#164, V Mall, Asha Nagar, Thakur Complex, Kandivali East.
Mumbai – 400101. Maharashtra. India.