NSP
SECURE YOUR FUTURE

# SECURE EMAIL

## Background

Email is mission critical, but email-based threats, including ransomware and business email compromise (BEC), are growing exponentially, and it's challenging to keep up.

Email was initially designed without security in mind and is involved in more than 80% of all attacks through tactics such as phishing and BEC.


Even savvy employees can mistakenly click malicious links and expose the organisation to cybercrime. Therefore, training users and encouraging the correct behaviours is as important as the technical settings.

## SECURE EMAIL - PART OF THE NSP LAYERED SECURITY MODEL

### Stop phishing and spoofing

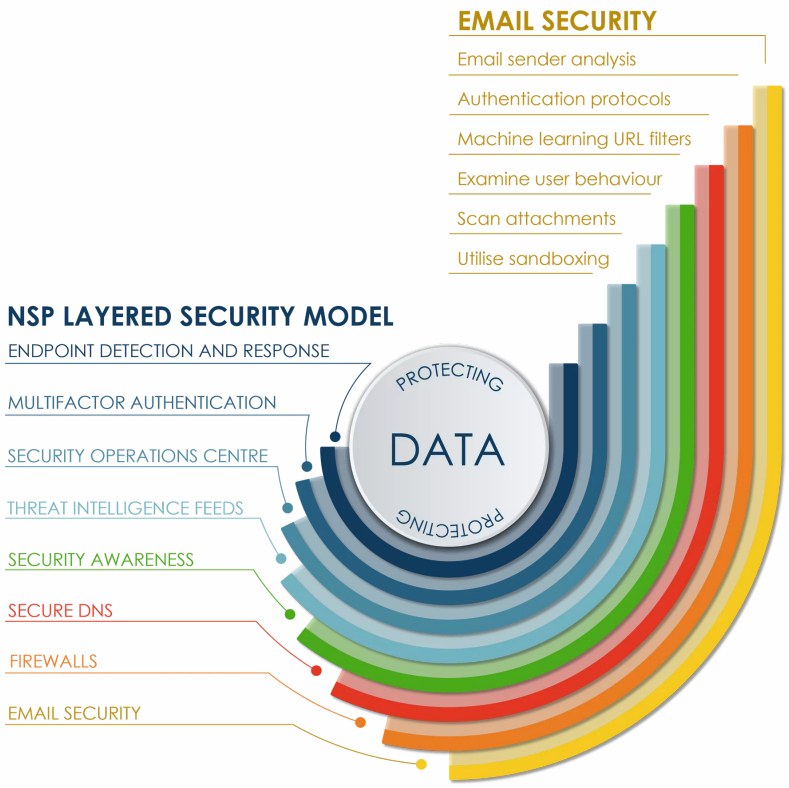
- To prevent email based cyber threat it is imperative to enable email sender analysis and authentication protocols i.e. SPF, DKIM and DMARC.

### Detect and block threats

- Stop zero-day malware by using machine learning URL filters
- Stop malware by scanning attachments and utilising sandboxing

### Protect against BEC

- Increase security for high-profile users by examining email behaviour, intention and writing style



### What you get

While email security is simple in concept, it can be challenging to set up correctly. NSP deploys in following a 3-phased approach:

- Set up tooling and configuration
- Eight-week monitoring and finetuning exercise to prevent inadvertent blocking of legitimate email traffic
- After mutual agreement, 'policy enforcement mode' is activated to block malicious traffic

### Cost

| ONE-OFF | MANAGED SERVICE | HOURLY RATE |
|---|---|---|
| • Set up tooling and configuration<br>• Enablement towards enforcement mode | • Platform management<br>• Monthly threat reporting<br>• Releasing blocked or quarantined emails | • Policy changes and feature requests<br>• Incident investigation and response |