ACDS
ADVANCED CYBER DEFENCE SYSTEMS

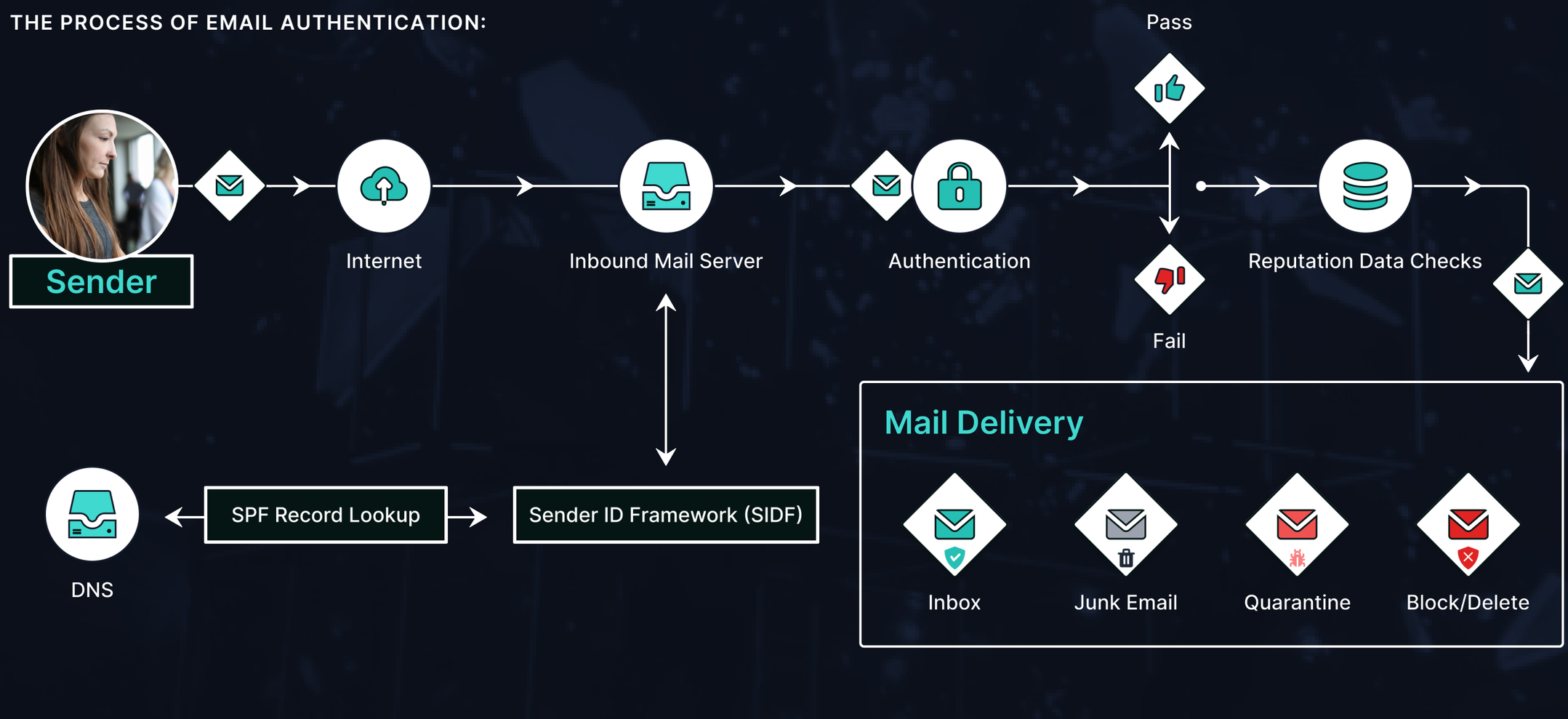
Email Guard

Ensure your organisation is compliant with the latest standards in email encryption and authentication.

Email fraud is on the rise, and organisations must protect themselves from this top attack vector. Companies without fully configured email authentication are vulnerable to criminals impersonating their brands and spoofing their customers and staff. This is known as Business Email Compromise (BEC).

The adoption of available email authentication standards is growing but still below 50% in many sectors [1]. Beyond the threat of impersonation, businesses risk their brand losing credibility as major consumer email providers have started flagging non-compliant messages from companies. This affects both the open rate of email to clients and customers and has the potential to decrease delivery success rates if companies don't take proper action.

THE PROCESS OF EMAIL AUTHENTICATION:



Email Guard is a tool for assessing compliance with email security technologies. Email spoofing is much harder if email domain owners implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to ensure that their email addresses are not successfully used by criminals in their campaigns. Email Guard provides guidance for correctly configuring these controls, which will help protect an organisation against attacks such as spoofing.

Email authentication is based on DNS records. Three kinds of records need to be set up to establish email authentication: DMARC, SPF, and DKIM. Each of them provides a different purpose—DMARC sets up reporting, SPF identifies approved email senders, and DKIM sets up cryptographic authentication of senders.

[1] DMARC and Email Statistics 2022, GoDMARC

Email Guard helps you set up and maintain good **DMARC**, **SPF**, **DKIM** and **TLS** configurations. It also collects, processes and analyses DMARC reports.

Monitor:

- Monitor your email security for any number of domains and sub-domain configurations.
- Gain visibility of all emails sent from your organisation and from third parties.
- Monitor the configuration of anti-spoofing controls (DMARC, DKIM and SPF) to ensure they are configured correctly.

Analyse:

- Present complex aggregate reports via clear, human-readable dashboards to help solve email authentication issues quickly.
- Reports will highlight if any of your organisation's domains are being abused.

Recommend:

- Identify configuration gaps to help you enhance your email protection protocols.
- Provide insights into your email confidentiality via the dashboard to track progress over time.

Benefits:

- Protects your email recipients by making it more difficult for cybercriminals to spoof your email address.
- Increased email deliverability by ensuring emails sent from your domains pass the recipient's email authentication.
- Compliance with anti-spoofing and email authentication standards helps provide protection against email fraud.
- Helps protect brand integrity and customer trust as cybercriminals cannot impersonate your domains.

ACDS
ADVANCED CYBER DEFENCE SYSTEMS