SYNAQ ITP BROCHURE

SYNAQ SECUREMAIL
IDENTITY THREAT PROTECTION

WHAT IS SECUREMAIL IDENTITY THREAT PROTECTION?

Identity Threat Protection (ITP) is a set of tools designed to combat and further reduce the risk of email phishing attacks on Securemail customers.

This toolset was designed to further address major phishing vectors such as domain spoofing and whaling (also known as spear phishing). It utilises existing email security standards namely the Sender Policy Framework. It extends its capabilities to further secure the identity of email domains protected by the Securemail Inbound service, significantly reducing the threat of spoofed email being delivered to your domain.

An added benefit of ITP is cross-domain security, which means that if you have more than one domain under ITP protection they will all be protected from spoofing each other.

A USER EMPOWERMENT DESIGN PHILOSOPHY

Greater user control is at the heart of ITP's design. It's important for users to understand their email environment with regards to the origins of the emails they receive. ITP caters for this learning and discovery process, allowing you to become more confident in your ability to secure your email domain(s) from spoofing without the worry of incorrectly rejecting or quarantining legitimate mail.

In the testing mode, you can monitor ITP reports to correct your SPF record or bypass trusted domains before enabling a protection command.

THE ITP TOOLSET

- **Domain Anti-Spoof management (DAS)** The DAS tool is designed to combat client domain spoofing and allows for enabling Header-From and Envelope-From checks to verify both senders against a domain's published SPF record. Spoofing is identified by a mismatch between these two senders.

- **Secured networks** due to multiple concurrent virus scanners automatically updating themselves with the latest malware and virus signatures, preventing viruses from reaching your network.

- **Executive Fraud Protection management (EFP)** The EFP tool is designed to combat whaling and applies additional checks on the Header-From

display name against a list of configured names, consisting of executives or important functionaries in the client's business when DAS is detected.

- **Protection Bypass management** This tool allows you to designate a trusted "affiliate" when sending domains to bypass DAS and EFP checks. For instance, a marketing mailer service or financial service which is send from their own Envelope-From domains but represent the client domain in the Header-From.

- **What you need to use ITP?**

- Domain(s) must be provisioned and protected by the SYNAQ Securemail inbound service.
- A published and valid SPF record must exist for each domain under ITP protection.
- Protection Bypass domains must have their own valid SPF record.