SECURE MAIL

With advanced spam and URL threat detection, 100% virus protection, Identity Threat Protection (ITP), Data Leak Prevention (DLP) and the only 100% punitive phishing protection SLA against leading banks in South Africa, SYNAQ Securemail is the ultimate line of defence in protecting businesses against spam, viruses and phishing attempts.

Delivered as an integrated cloud service and supported 24x7 by local SYNAQ engineers, your business can start to benefit from the peace of mind of having a spam, virus and phishing free inbox.

To become a SYNAQ client, contact us on:
(011) 262 3632 or email sales@synaq.com

SYNAQ
BE EMPOWERED.

FIRST LINE OF DEFENSE IN EMAIL THREATS

First generation email security solutions, desktop software, servers and gateway applications are not capable of an effective pre-emptive response to the aggressive tactics virus propagators and spammers use to infiltrate corporate networks and email servers.

SYNAQ Securemail incorporates an array of anti-virus, antispam, content control and anti-phishing technologies that act as the first line of defence between the public Internet and your company's email servers.

With our proactive Software-as-a-Service approach to email security, SYNAQ Securemail is a counter against new viruses and spamming tactics as they emerge around the world, and filters email-borne spam and viruses before they reach corporate networks, 24x7x365.

WHAT IS LINKSHIELD?

LinkShield, our native threat detection feature for URL-based phishing attacks, is powered by LUCA (LinkShield URL Classification AI), our own proprietary machine learning technology. LUCA's advanced algorithms anticipate and neutralise zero-day phishing threats for enhanced threat detection accuracy, reducing false positives for unparalleled protection against URL-based threats.

LINKSHIELD BENEFITS

- **Defend your business against URL-based phishing with LinkShield's** proprietary Machine Learning algorithms that detect and prevent attacks with greater accuracy.
- **Custom Policy Settings** configure and manage policies to suite your business context through an intuitive interface.
- **Powered by LUCA** custom-built artificial intelligence to identify zero-day or discretely targeted phishing URLs, reducing false positive and ensuring more accurate and performant security environment.

WHAT IS 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).

WHAT IS DATA LEAK PROTECTION?

Securemail's DLP helps IT managers who want to prevent sensitive and confidential information leaking out of the organisation via email. DLP reduces the opportunities and therefore mitigates the risk of such information leaking out through both employee ignorance, or criminal intent.

END-USER BENEFITS

- Email protection ensures that end users are safe from spam, phishing and email-borne viruses.
- Additional risk mitigation against phishing attacks, specifically domain spoofing and whaling, using the ITP toolset, namely: Domain Anti-Spoof management, Executive Fraud Protection management and Protection Bypass management.
- No installation and easy to set up with simple DNS mail record (MX) changes, businesses are set up and protected in less than 24 hours.
- Secure, powerful and user-friendly administration interface provides detailed management reports and statistic.
- Mitigates the risk and impact of URL based phishing, ransomware and malware attacks in emails using LinkShield (URL threat protection).
- DLP introduces business rules and policies that effectively prevent the transmission of emails that contain sensitive and confidential information leaking out of the organisation via outbound email.

ADMINISTRATOR BENEFITS

- **Advanced detection techniques identify** 99.95% of spam using multiple techniques, including highly advanced heuristics, Optical Character Recognition (OCR) and other sophisticated methodologies Administrators have full control to manage user accounts, email aliases, calendar resources, archive and discovery access and distribution lists through a full-featured web-based administration interface.
- **Enhanced control** with the ability to specify multiple mail routing destinations.
- **Advanced diagnostics** allow administrators to quickly detect where possible breakages in the email chain exists for faster issue resolution.
- **Quick and easy mail quarantine administration** that saves quarantined emails for up to 30 days for later analysis.
- **Added redundancy** ensures that even if your infrastructure is down, email is spooled on SYNAQ servers for 14 days.
- **IT managers can measure** the number of bad URL's blocked across a domain and block threats from affecting the companies devices and infrastructure.
- **Integrated Azure Active Directory (AD)** module means you can deploy Securemail for your Microsoft 365 mail solution for a more comprehensive line of defence. Ingest your existing Azure AD accounts quickly and easily and enhance Access and Identity Management (AIM) with centralised password management and Azure SSO integration.
- **Secured networks** due to multiple concurrent virus scanners automatically updating themselves with the latest malware and virus signatures, preventing viruses from reaching your network.
- **Highly configurable service** allows for the use of thousands of different rules and configurations for any combination of users or domains
- **Hassle-free administration** means no more patches or downloading software. SYNAQ takes care of the software and services while IT enjoys the protection provided.
- **Insights Module** designed to empower and proactively enhance client email security posturing and performance through access to contextualised, high-level security metrics, and the ability to drill down into the details.
- **Ability to enforce policies on outbound email for the purposes of restricting, or monitoring, the transmission** of certain classes of personal or company sensitive information as proscribed by either legislation or internal company policy.

To become a SYNAQ client, contact us on:
(011) 262 3632 or email sales@synaq.com

SYNAQ
BE EMPOWERED.

FINANCIAL BENEFITS

- **No upfront investment** as SYNAQ Securemail is delivered as a cloud service. No additional software or additional infrastructure investment is required.
- **Network compatible** as SYNAQ Securemail works with all mail infrastructure regardless of the operating system and hardware.
- **Save bandwidth costs** by eliminating virtually all wasteful and potentially harmful traffic that overloads company networks before reaching your gateway.
- **Highly scalable** as it processes millions of emails per day and allows you to pay as you grow.

SECUREMAIL IN BRIEF

- **99.95% spam detection** accuracy and 99.9% uptime guarantee.
- **Innovative mail queue** and destination management technology.
- **SMTP transmission log view** to quickly diagnose potentially problematic emails.
- **Identity Threat protection toolset.** Domain Anti-Spoof management, Executive Fraud Protection management and Protection Bypass management.
- **Automatically corrects messages** on the fly and quarantines dangerous sections of mails.
- **Mitigation of URL based phishing,** ransomware and malware attacks in emails using LinkShield.
- 100% **virus protection** SLA.
- 100% **phishing protection** SLA against leading banks in South Africa.
- Over 2500 different **spam checks**.
- **Scans for attacks** against known and unknown security vulnerabilities
- Organisational and domain **level management**
- **Full audit trail** of interface operations
- **Whitelist and blacklist** administration **Enforces business rules and policies using DLP** to effectively prevent the transmission of outbound emails that contain sensitive and confidential information.