PROTECTION

Good news for your email server

More than 90 out of 100 cyberattacks are carried out via email

Cyberattacks have become part of everyday life for companies all over the world. The possible consequences of such an attack range from complete paralysis of your business to damage claims by affected customers to reputational damage. With the conventional email still being the main entrance gate for cyberattacks, there is reason enough to always keep your email communication absolutely secure.

NoSpamProxy® Protection rejects problematic emails categorically

NoSpamProxy Protection scans emails as soon as they are received, ensuring complete protection against spam, ransomware, spyware and malware. NoSpamProxy classifies inbound emails using a variety of anti-spam filters and rejects spam emails reliably. Only non-hazardous emails are allowed to pass. Furthermore, in case a trusted email is blocked, NoSpamProxy Protection will inform the sender about its rejection. This makes NoSpamProxy one of the few anti-spam solutions compliant with the challenging German laws (particularly in accordance with §206 of the StGB [Criminal Code] and §88 of the Telecommunications Act).

NoSpamProxy Protection eliminates malicious content

Email attachments in Word, Excel or PDF format can be converted or mitigated into safe PDF files based on rules, thus guaranteeing that only harmless attachments are delivered to the recipient. The „click out of curiosity" no longer threatens your entire IT infrastructure.

NoSpamProxy Protection meticulously inspects sender addresses

The automated sender identification allows NoSpamProxy to clearly determine whether an email originates from the specified sender. To do this, NoSpamProxy uses a Sender Reputation Management system based on SPF, DKIM and DMARC checks. To protect against phishing and CxO fraud attacks, a comprehensive check of the Header-From, i.e. the header of an email, is performed. This prevents, for example, attackers from impersonating your superiors or colleagues in emails.

NoSpamProxy Protection learns about your communication habits

With the help of the Level of Trust technology, NoSpamProxy constantly learns who you or your company's employees are communicating with. Trust points are assigned on the basis of numerous features. However, these characteristics are more than a dynamic allowlist: NoSpamProxy Protection also scans outbound emails and assigns trust points for the recipients of these emails. In this way, desired communication relationships are learned and your system grows intelligently.

No quarantine trap with NoSpamProxy Cloud

A problem common to all spam protection solutions is that the software decides whether an email is classified as spam. In many cases, not all spam emails are detected, or uncontaminated emails are accidently blocked. These false positives are a huge threat for companies and a weakness in many conventional anti-spam solutions. If such emails are deleted or stored in a quarantine folder, it is nearly impossible to locate them once they have been quarantined.

Virus Bulletin confirms 0 % false positive rate for NoSpamProxy

"With a score of 99.99 out of 100, NoSpamProxy has earned the prestigious VBSpam+ rating for IT security. NoSpamProxy scored an excellent strike rate of 99.99 % in the anti-spam test carried out by Virus Bulletin. In addition, it also impressed with its 0.00 % false positive rate.
Not only does NoSpamProxy perform brilliantly in terms of spam protection but it also offers cutting-edge protection from malware and ransomware, which we have started testing for in the latest version of our tests.

Martijn Grooten,
Senior Editor, Virus Bulletin

SecurITy made in Germany

Complete and retraceable spam protection

With the reporting functions of NoSpamProxy Protection you have a constant overview of your email traffic. Thus, the data volume as well as the email and spam volume can be analysed in detail down to the user level. Integrated message tracking logs every single email as well as information about how it was processed. Rules and all anti-spam filter activity are fully retraceable. Administrators can use the logs and reports of NoSpamProxy Protection to keep all messages in constant view and to answer questions easily.

Optional Sandbox Service

The optional NoSpamProxy Sandbox Service increases the probability of the detection of new viruses significantly. This is possible because files are scanned not only in a single sandbox, but in a sandbox array.

Perfect synergy between NoSpamProxy Protection, Encryption and Large Files

If you use NoSpamProxy not only for protection against spam and malware, but also for email encryption and for the secure transfer of large files, you will gain added security:

- Thresholds for rejecting messages suspected of being spam or malware can be increased if regular communication with business partners is encrypted and signed.
- Spam and malware scanning can be efficiently performed at the same gateway used to decrypt emails. If other solutions are used, re-routing is required, resulting in loss of time and performance.
- The same Web Portal is used for smart attachment management, Content Disarm and the Large Files module. This allows for great flexibility in configuring the handling of large files and different file types.
- NoSpamProxy Protection also builds on the Level of Trust technology: You can easily specify whether attachments from known communication partners are directly sent to the recipient and only attachements of unknown communication partners are added to the attachment quarantine.
- Additional benefits result from the coordination of the functionalities of the NoSpamProxy modules.

Real-time virus protection

NoSpamProxy Protection integrates the zero-hour technology of our technology partner Cyren. For this purpose, the patented technology examines large parts of the global internet traffic in real time and analyses up to 100 billion messages per day, of which up to 88 billion are contaminated with spam and viruses. The solution scans the Internet proactively and identifies potential virus outbreaks particularly quickly. Unlike signature-based methods, this solution detects new virus outbreaks as they occur. Your Exchange server as well as your entire email infrastructure are protected within the first seconds.

> The Level of Trust filter is excellent. It is reliable to stop known spammers and guarantees that emails from our business partners and customers are delivered.
>
> Jürgen Lalla,
> Head of IT at Swiss Life Select

SwissLife Select

All highlights at a glance:

- ✓ No quarantine
- ✓ Relief for the administrators
- ✓ Level of Trust technology
- ✓ Content Disarm and Reconstruction
- ✓ Sender Reputation Management
- ✓ Cyren Anti-Spam and Anti-Virus Engine
- ✓ Optional Sandbox Service