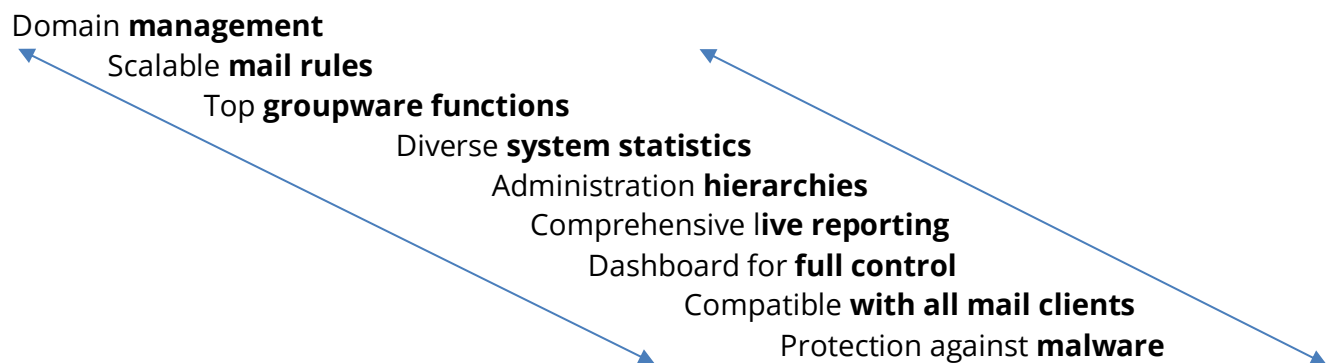# groupios

secure.
simple.
open.
clever.

The E-Mail-Security and Groupware of the future

As part of an **e-mail and groupware security solution**, TUXGUARD combines the protection of a **security gateway** with **easy-to-use groupware** - and adds a **multi-client capable administration console**.

groupios is **100% GDPR-compliant**.

groupios at a glance

Domain **management**
Scalable **mail rules**
Top **groupware functions**
Diverse **system statistics**
Administration **hierarchies**
Comprehensive l**ive reporting**
Dashboard for **full control**
Compatible **with all mail clients**
Protection against **malware**

The Gateway – Security „Made in Germany"

The groupios gateway reliably eliminates all forms of malware and provides effective protection against cybercrime. Threats such as spyware, malware or ransomware, but also annoying time-wasters such as spam do not even reach your e-mail inbox.
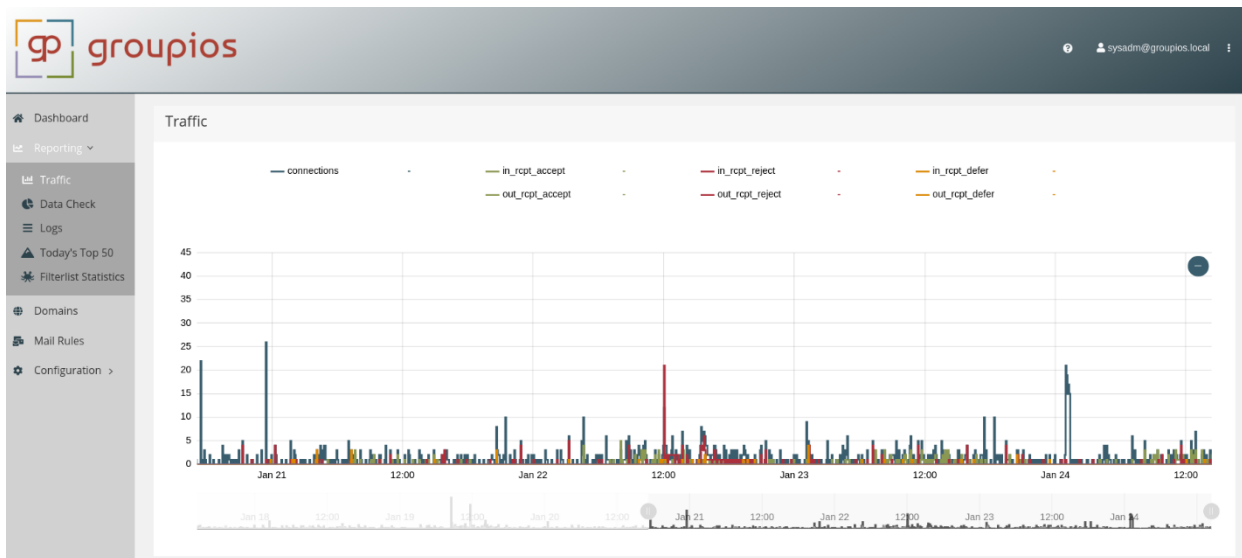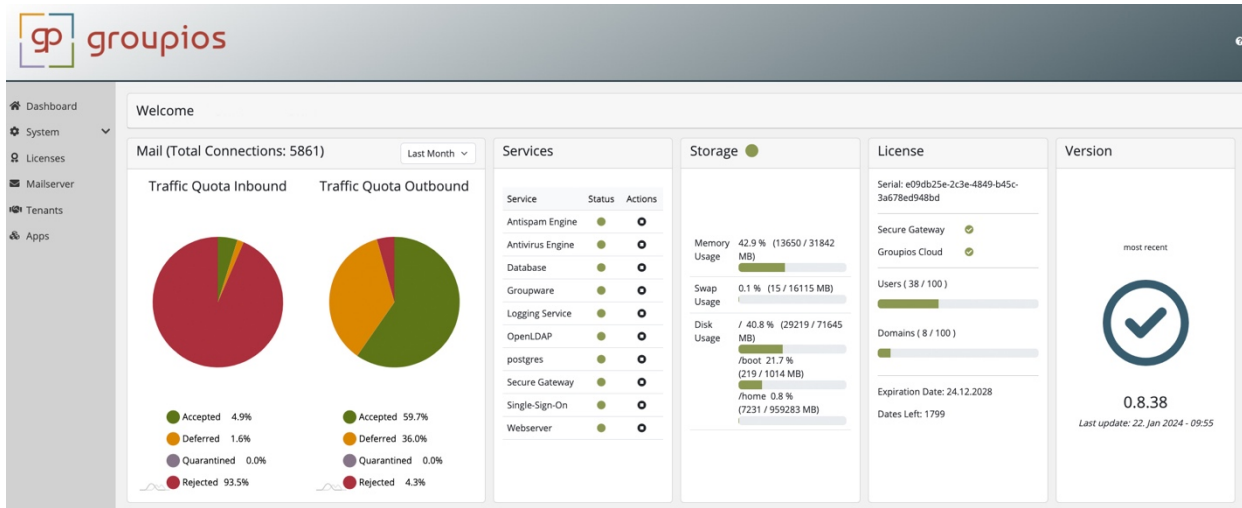

Comprehensive e-mail rules
for all-round protection

Powered by

TUXGUARD
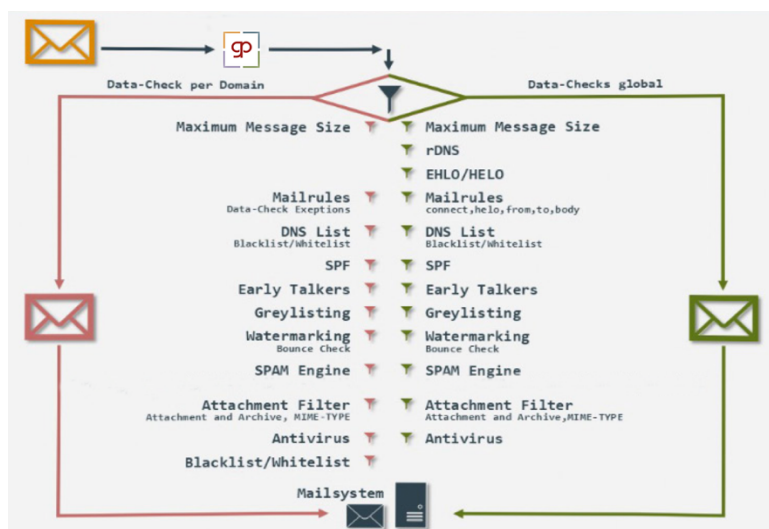
groupios – for companies of any size

In your dashboard, you have a live view of all network activities like in a cockpit and you can navigate, act and react in a targeted manner.


In your dashboard, you control the **system utilisation**, assign **administration rights**, manage your **domains** and control **extensive email rules**.

The admin console provides information about the **utilisation of the mail systems**, the **priority setting** for incoming and outgoing emails, the **configuration and management** of emails, provides an **overview of the data check** of network activities and **shows locations and administration levels.**

With a wide range of functions such as **individual white and black lists**, **greylisting, sender authentication, EHLO checks, watermarking and attachment filtering**, groupios offers effective all-round protection for your communication.

Assign and fix administration rights

Assign administration rights for different administration levels and give the respective user access to relevant system information.
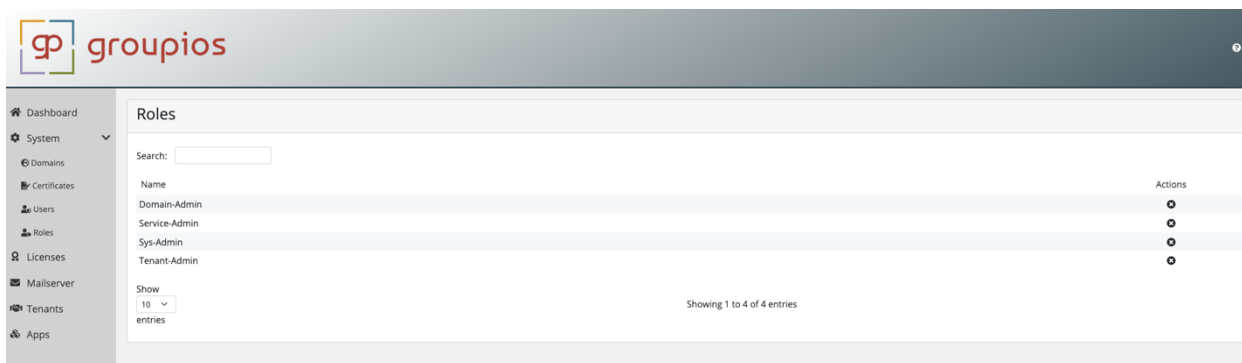
groupios – Groupware with Kopano Cloud inside

The groupios EGA (Extended Groupware Application) has integrated the **Kopano Cloud as an OEM solution**, creating a broad functional basis with standardized administration that is suitable for **"on premises"** use.
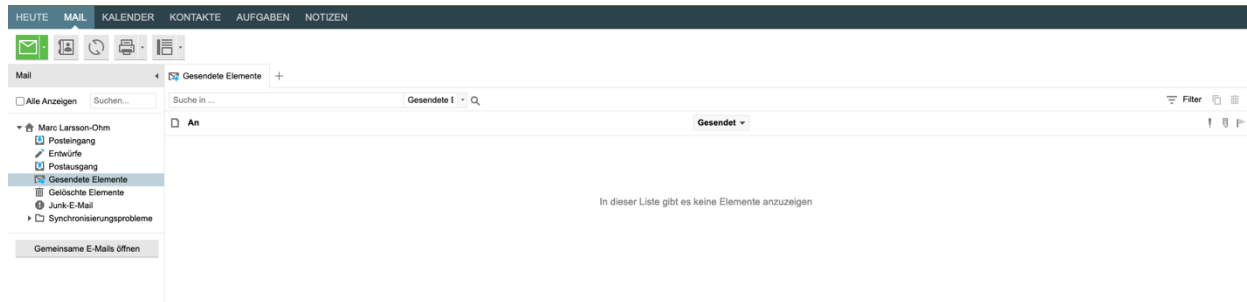
groupios offers a **native Outlook connection** without the help of plug-ins or add-ons, including autodiscover functionality.

The following **clients** are supported by groupios: WebApp, Microsoft Outlook (from 2016, incl. MS 365), alternative clients via IMAP/POP3 (e.g. Thunderbird), Android and iOS via ActiveSync.

With the EGA, groupios provides familiar functions such as **mail, calendar, contacts, tasks and notes**; shared folders, aliases for users and domains as well as an extended global address book across several domains of an organisation are also possible. All **data always remains user-related** - even at the same hierarchy level.

groupios Security features

Dashboard (multi-client management console)

Dashboard start page	Display of system loads for web interface and users - CPU-Utilisation - Memory-Utilisation - HDD - Inbound- and Outbound-Traffic
Dashboard access and management via page navigation for network administration	Reporting Domain-Management Various E-Mail-Rules Assignment of rights to administrations, hierarchy locations Configurations

Powered by

TUXGUARD

groupios

System-Statistics

**Display of current
status of all services**

System-Utilisation Webinterface and User
Traffic-Display: Inbound- and Outbound-Utilisation
Display of performed Logs
Top-50-Activities

Administration hierarchy

Administrative levels

Role-based release of authorisations and
assignment of privileges

Domain-Management

Check of Data traffic

Pre-Check of Data traffic:
- Backscatter Filter, Backscattering of
  received bounce messages (e-mail
  cannot be delivered) or automatic replies
  to unsent messages
- Bounce-Messages
- Greylisting

Post-Check of Data traffic:
- Watermarking for reduction
  of „False Positive"
- Incl. Spam- and AV-Engine
- Checking file attachments
- Report and alarm planning

Varoius Mail-Rules

Global Message Size Limit

Global limitation of the message size
Optional restrictions on mail traffic

White- and Blacklists

White- und Blacklisting with optional adjustments
and deletions

Smart Host Support

Use of the mail gateway as an "intelligent" host for
SMTP Auth

Recording of all email addresses with activated user
address book

Increase scanning efficiency and reduce false alarms

Pre-Check of Data traffic

Pre-Check   Data check before message text is sent

                            Rejection of messages until the recipient of the
                            message is determined

                            Request and inclusion in white and black lists

SPF (Sender Policy Framework)/   Review of broadcasting licenses
Anti-Spoofing

rDNS   Checks and filters reverse DNS lists for generic
                            and invalid rDNS doms

Bounce Messages   Help with sender identification and delivery errors

DNS Lists   Optional integration of DNS blocklists for incoming
                            connections and URLs in mails

Watermarking   The mail gateway flags both incoming and outgoing
                            messages with watermarks

                            Reduction of system load and false positives

Sender- Authentication   Heuristics for sender identification

EHLO/HELO-Checks   Identification of the qualified host name of the
                            sending system

Reliable protection against malware

Antispam Protection   Rspamd
                            groupios DNS Blocklists
                            optional additional Blocklists
                            Greylisting
                            rDNS
                            Early Talkers

Virus & Malware Protection   ClamAV is license-free integrated (incl.
                            Unofficial Signatures)

Attachment Filtering   Prevents unwanted attachments in the mail system

Check of Attachments   Retention of unrecognised senders and protection
                            from infected attachments

                            Block mails with unwanted attachments
                            (f. e. .doc, .docx, .xls, .xlsx etc.)

Powered by

⌐TUXGUARD

Comprehensive Reporting

Analyses
Real-time analyses of:
- System utilisation
- Status of all basic services involved
- Spam volume

System requirements

AlmaLinux 9
Hard- and Software compability:

- All virtual environments

- All hardware components including servers

Do you have any questions? Please contact us!

TUXGUARD GmbH
Wilhelmstraße 9, D-24534 Neumünster
sales@groupios.com
+49 4321 / 87 26 7-0

Visit us on **www.groupios.com**!

About TUXGUARD

TUXGUARD GmbH has stood for IT security "Made in Germany" for over two decades. A team of innovative developers develops customised cybersecurity infrastructures that are, of course, GDPR-compliant and free of backdoors. Threats are recognised at an early stage and eliminated immediately. TUXGUARD's perfectly harmonised portfolio, based on the revolutionary Intelligence Cyber Management (ICM) technology, connects people and technology and offers reliable protection of sensitive data against any threats from the network.