

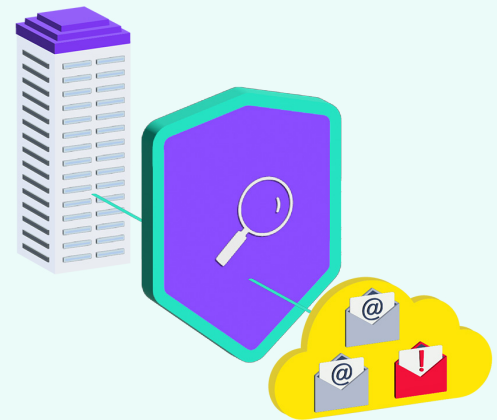
genumail

Facts & Features



Secure E-Mail Gateway

genua.



Definition

The e-mail gateway genumail is a solution that filters incoming e-mails and protects your company against spam, malware, phishing, and false identity fraud. Implemented as a gateway in front of the mail server, it filters unwanted e-mails before they reach the mail server. This protects e-mail as a communication channel and reduces the workload of your mail server.

Typical Use

- Filtering spam, malware, and phishing, eliminating a critical attack surface
- Providing a quarantine workflow
- Implementation of an e-mail security strategy: pattern and anomaly detection
- Dialog with end-users regarding quarantine status

Throughput Volume

genumail is based on a Kubernetes infrastructure and can scale flexibly: Depending on the e-mail type and attachment size, it has a throughput of at least 50,000 incoming and outgoing e-mails per hour.

Reasons to Choose genumail

- Modern scalable on-premise e-mail filtering solution based on Kubernetes
- Sovereign operation through the possibility of hosting and operation by the user
- GDPR readiness for compliant operations in German data centers
- IT Security made in Germany

Customer Service

- Customer service directly from the manufacturer
- Hotline service
- Comprehensive training courses

SecurITy
made
in
Germany

E-Mail Filter Components	
E-mail evaluation	Incoming e-mails are evaluated using a bonus/malus system. Based on the result, e-mails are delivered, quarantined, greylisted or even deleted.
Server mail security parameters	<ul style="list-style-type: none"> Evaluates SPF, DKIM, and DMARC configurations and rates incoming e-mail accordingly if the sending mail server supports these settings Deviations from the senders communicated configuration lead to devaluation or even rejection of the e-mail
Mail server IP and domain	When the connection is established, the IP address and domain of the foreign mail server are compared against a dynamic list of known spammers and "bad" mail servers and the e-mails are devaluated or rejected
Malware detection	E-mail attachments are transferred to a virus scanner via the ICAP interface, and the result of the scan is included in the evaluation of the e-mail
Phishing	Links in incoming e-mails are checked against a dynamic list of known phishing servers and can cause the e-mail to be devaluated
"Bad" Links detection	Links in incoming e-mails are checked against a dynamic list of known malware distributors, cracked websites, and "bad" e-mail reply addresses and can cause the e-mail to be devaluated
Spam content detection	Spam e-mails are identified and devaluated based on the e-mail content

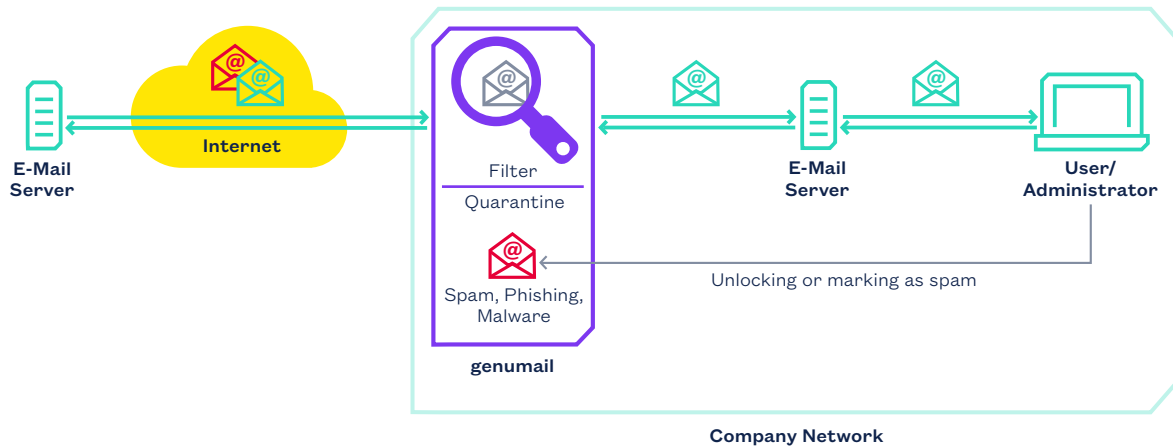
Monitoring	
Logging	Standard Kubernetes logging into the log system connected to your K3s
Metrics	All product metrics are provided in the Prometheus industry standard

Administration	
Web GUI	Powerful and modern web GUI (https)
Inline Help	In addition to the manual, inline help for many of the configuration options offered
Convenient upgrades	Easy installation of patch versions and new releases using the Kubernetes Helm installation scripts

More product information



Use Case



Reliable Protection of the Corporate Network

E-mail traffic is one of the main attack vectors in companies. genumail protects your business from e-mail-based attacks that can cause security breaches, data loss, and identity theft.

Safeguarding the user mailbox against dangers allows for trouble-free e-mail communication and minimizes the risk of security incidents. All of genumail's protective functions work automatically in the background and enable smooth business processes.

Further Information:

www.genua.eu/genumail

genua GmbH

Domagkstrasse 7 | 85551 Kirchheim | Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu