Welcome

heinlein

Linux höchstpersönlich.

heinlein

04.02.2024 / Carsten Rosenberg, Manu Zurmühl

Enterprise grade mail-cluster with open-source?

heinlein

04.02.2024 / Carsten Rosenberg, Manu Zurmühl

Enterprise grade mail-cluster with open-source?

yes ;)

Who we are

Carsten Rosenberg
Linux-Consultant
Mail Security Expert

Manu Zurmühl
Linux Consultant
Mail Security Expert

heinlein

- Consulting
  - Linux
  - Storage
  - Monitoring
  - **Mail Infra**
    - **Rspamd**
    - **Postfix**
    - **Dovecot**
    - **…**
    - **(Groupware)**
- IT Academy
- Hosting / ISP
- mailbox.org
- Opentalk

How-to Enterprise Mail-Security -

we had a look at some vendors

- Adaptive Ratelimiting
- Advanced Anomaly Detection
- Advanced Malware Protection and Threat Grid
- Advanced Multi-layer Attack Vector Detection
- Advanced Multi-layer Malware Detection
- Advanced Threat Protection
- Artificial Intelligence (AI) Spam Detection
- BEC and CEO Fraud Detection
- Cloud-driven Reputation
- Content Disarm and Reconstruction
- Domain Fraud Protection
- Email Data Loss Prevention
- Identity-Based Encryption (IBE)
- Impersonation Analysis
- Local and Cloud Sandboxing
- Mailbox Safeguard
- Recipient dependent Transport Layer Security and Encryption
- SIEM Vector Export
- Typosquatting Detection
- URL Click Protection
- Web Interaction Tracking
- Secure Message Delivery
- Virus Outbreak Protection

Advanced Threat Protection

- *Alias: Advanced Anomaly Detection, Advanced Malware Protection and Threat Grid, Advanced Multi-layer Attack Vector Detection, Advanced Multi-layer Malware Detection, Virus Outbreak Protection*

  Recognition of malicious E-Mail content or attachments

  Multilayered: Filename Extension, hash, anti-virus, file-analysis, cloud-query, sandbox

- Rspamd: Multimap, RBL, Oletools/PDF, PeekabooAV (Sandbox)
- Antivirus

Artificial Intelligence (AI) Spam Detection

- *Alias: Cloud-driven Reputation*

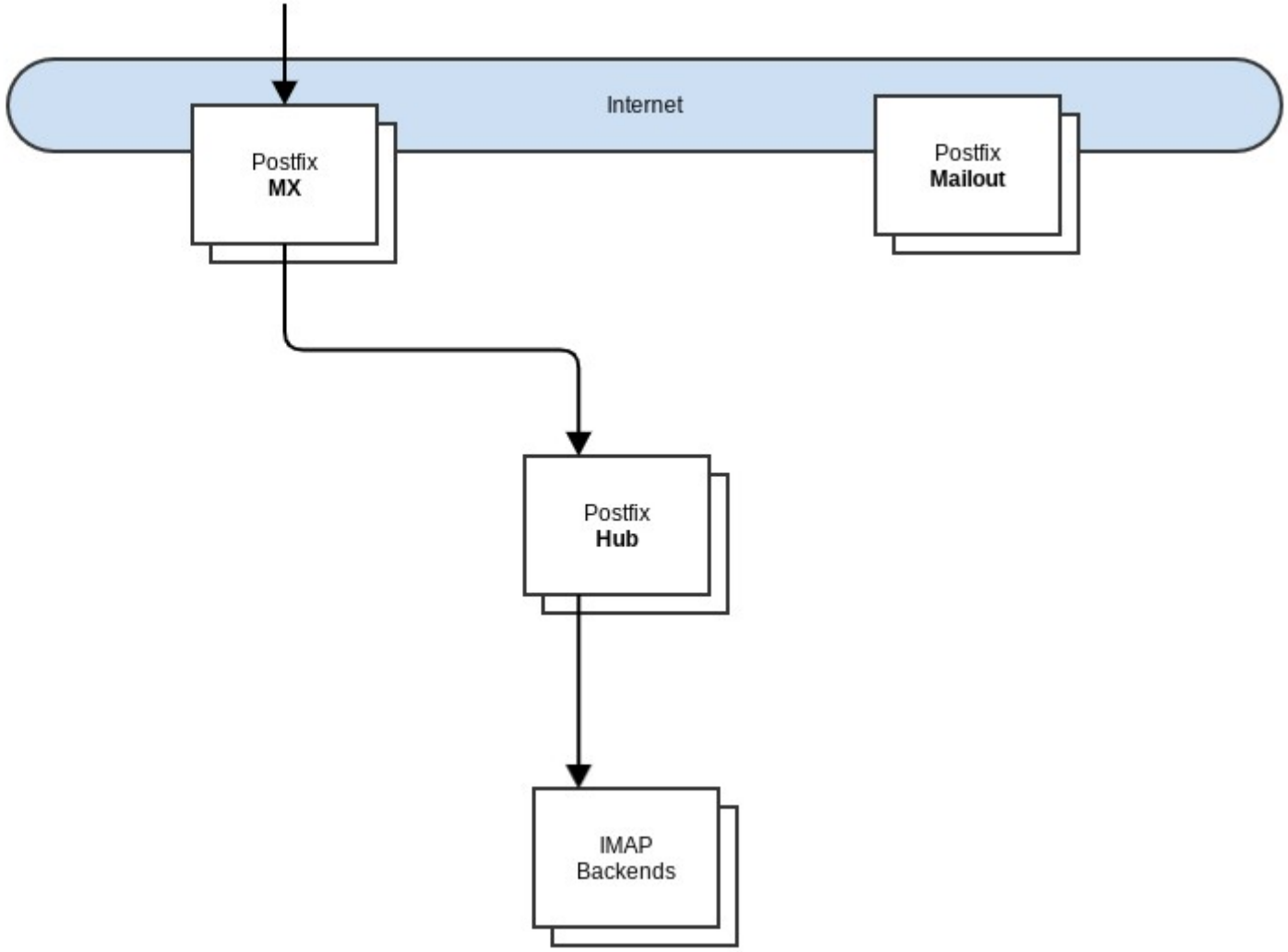
  Insights by learning different sets in neutral networks
  retrieval or querying data from the manufacturer cloud

- Rspamd: local Neural Network, local and remote Fuzzy
- Cloud data and some neural networks

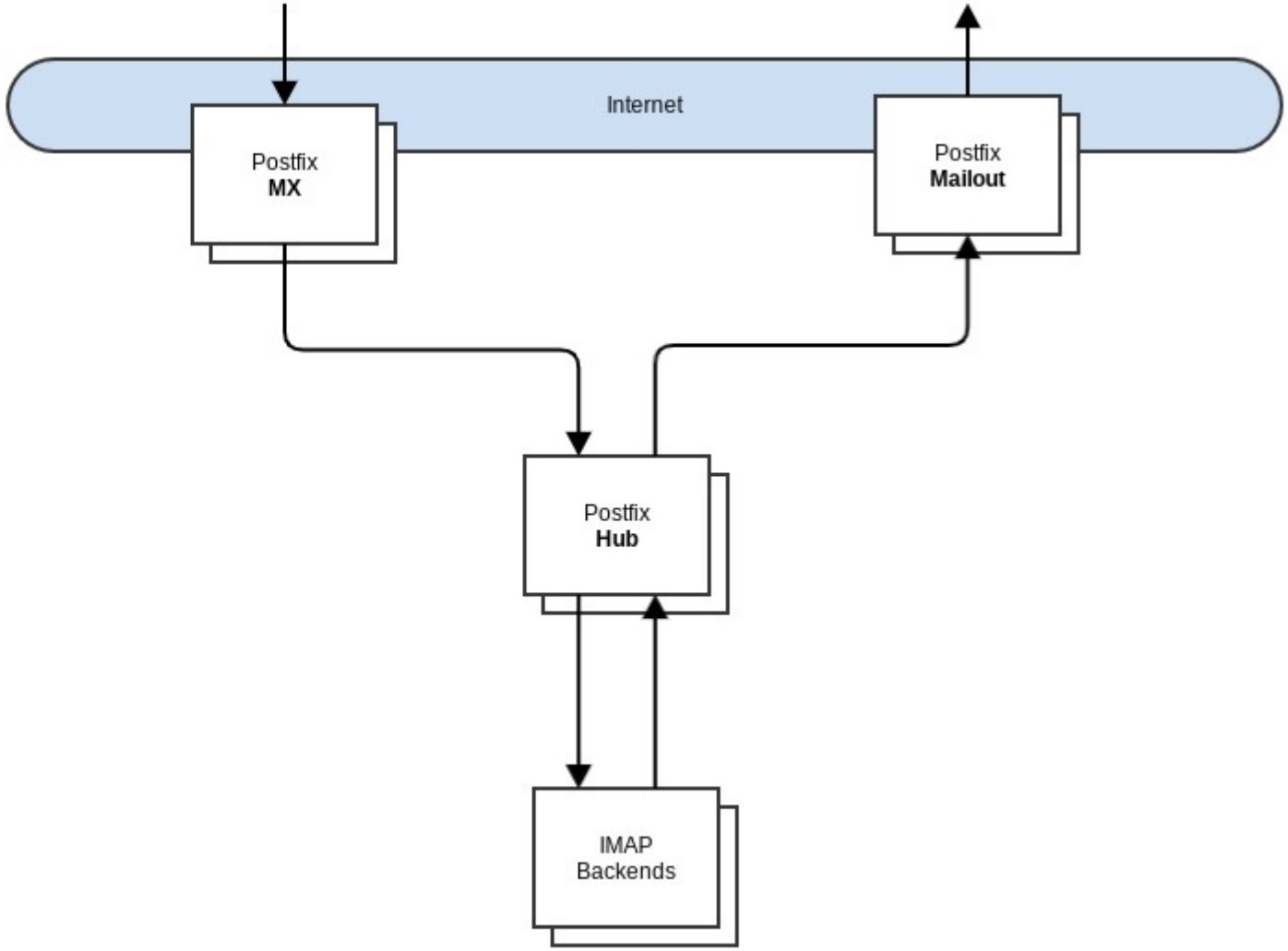
Our current Stack for Mail-Security

- Rspamd
- Postfix
- Redis / KeyDB
- extra Services: AntiVirus, File Analyzers, RBLs, Hash DB (Razor, Pyzor, DCC),
- User specific Profiles (Databases)

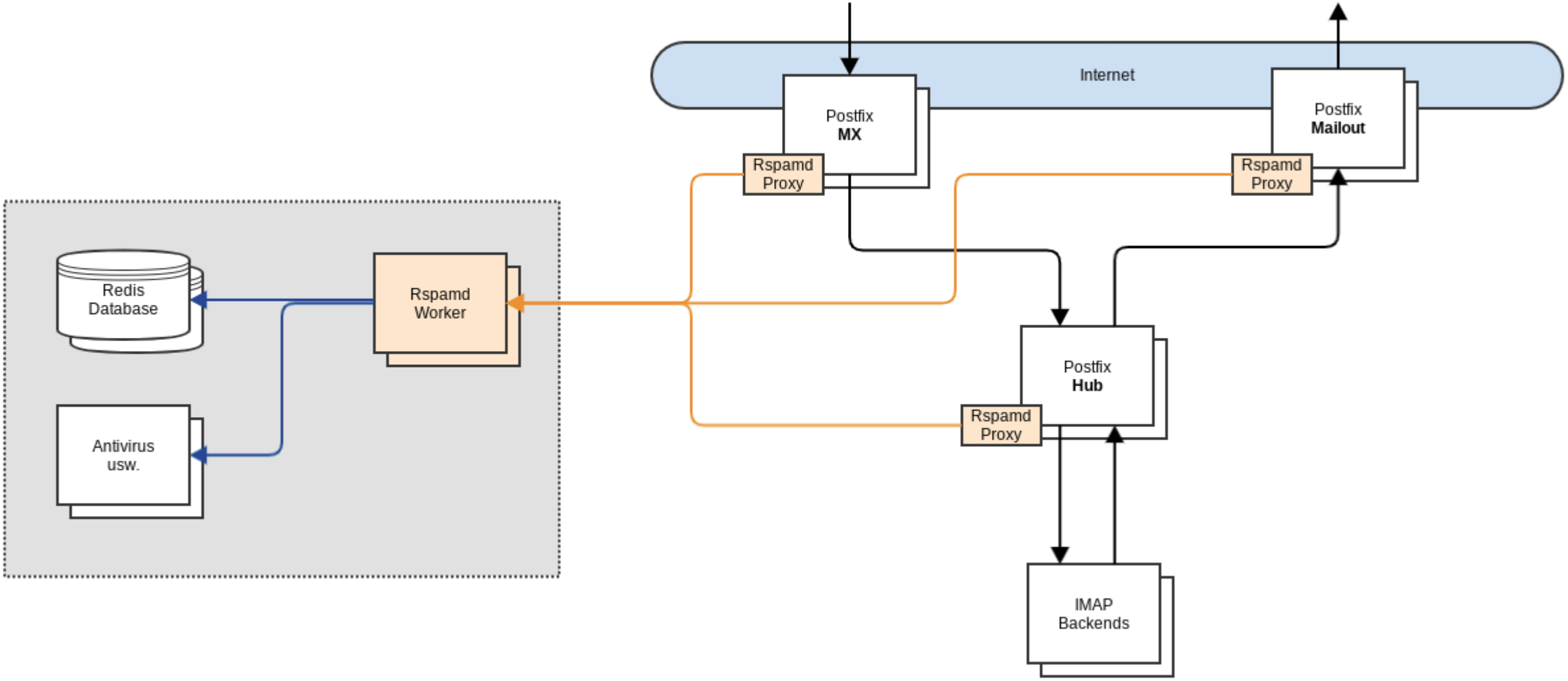
How we build Mail Infrastructure



How we build Mail Infrastructure



How we build Mail Infrastructure



Why Rspamd as central Mail-Security Controller?

- Very flexible redundant Mail-(Content-) Framework
- Self-learning and highly customisable reputation
- Text-analysis with Bayes (Statistical) and Fuzzy algorithm (text shingles)
- Powerful flexible pattern matching to query lists, APIs or DNS zones (RBL)
- helpful plugins: Ratelimit, URL Redirector, Neural Network (for scan reports)
- Proof-of-Origin: (Sign and) verify SPF, DKIM, DMARC, ARC, BIMI
- Easily extendable with new functions and plugins (Lua)
  - integration of external services (e.g. sandboxing or APIs)
  - e.g. write a rate-counting plugin with Redis caching in 200 lines of code

Rspamd - Log

Feb 01 12:26:45 srv.example.com rspamd[4137084]: <1190ef>; task; rspamd_task_write_log: id: <q1aWo8J54nOoq1aWo8J54nOoq1aWo8J54nOo@iaeti.org>, qid: <E9972200407>, mta: 127.0.0.1 (localhost), ip: 198.251.80.254 (mail10.iaeti.org), from: <Valee@iaeti.org>, subject: "h mustermann, Erektionsprobleme?", (default: T (reject): [36.13/15.00]

- [**HS_RS_BAD_FAKE_SHOP**(12.00){},**RBL_SH_ZEN_XBL**(9.00){198.251.80.254:from;},**BAYES_SPAM**(5.07) {99.93%;},**HS_HEADER_1519**(5.00){},**RCVD_UNAUTH_PBL**(2.00){},**R_DKIM_ALLOW**(1.52) {iaeti.org:s=root;},**IP_REPUTATION_SPAM**(1.22){asn: 53667(0.40), country: US(0.01), ip: 198.251.80.254(0.00);},**SUBJECT_ENDS_QUESTION**(1.00){},**MX_INVALID**(0.50){},**DKIM_REPUTATION**(0.49) {0.99933343079923;},**SPF_REPUTATION_SPAM**(0.49){0.99933343079923;},**MIME_HTML_ONLY**(0.20) {},**LOCAL_FUZZY_AUTOLEARN**(0.11){type 2 (weight: 2);},B**AD_REP_POLICIES**(0.10){},**LOCAL_RCPT**(0.10) {example.com;},**NON_LOCAL_IP**(0.10){198.251.80.254;},**SPAMD**(0.10) {HTML_MESSAGE;MIME_HTML_ONLY;SPF_HELO_NONE;},VALID_RCPT(0.10){h.mustermann@example.com;},**ARC_NA**(0.00) {},**ARC_SIGNED**(0.00){example.com:s=arc:i=1;},**ASN**(0.00){asn:53667, ipnet:198.251.80.0/24, country:US;},**DEFAULT_INCOMING**(0.00){},**DKIM_TRACE**(0.00){iaeti.org:+;},**DMARC_POLICY_ALLOW**(0.00) {iaeti.org;reject;},**FROM_EQ_ENVFROM**(0.00){},**FROM_HAS_DN**(0.00){},**GROUP_RBL_FROM_REJECT**(0.00){},**HAS_URL**(0.00) {},**INCOMING**(0.00){},**IXHASH_TEST**(0.00){38e264a10145a17e1488c4e276486a90;},**MID_RHS_MATCH_FROM**(0.00) {},**MIME_TRACE**(0.00){0:~;},**PROXY_INFO**(0.00){E9972200407;srv.example.com;1190ef;},**RCPT_COUNT_ONE**(0.00) {1;},**RCPT_DN_IN_SUBJECT**(0.00){dn mime: h mustermann;},**RCPT_USER_IN_SUBJECT**(0.00){rcpt mime user: h mustermann;rcpt smtp user: h mustermann;},**RCVD_AX_COMB_GEN_RDNS**(0.00){82.211.222.158:received;},**RCVD_COUNT_ONE**(0.00) {1;},**RCVD_SH_ZEN_PBL**(0.00){82.211.222.158:received;},**RCVD_TLS_LAST**(0.00){},**R_SPF_ALLOW**(0.00) {+ip4:198.251.80.0/24;},**TO_DN_ALL**(0.00){},**TO_MATCH_ENVRCPT_ALL**(0.00){},**UID_ROUNDTRIP_VERIFY_FAIL**(0.00){no_hdr;}])
- , len: 2605, time: 2552.095ms, dns req: 69, digest: <e2ac0d9e945a1b6d643c992836c9025e>, rcpts: <h.mustermann@example.com>, mime_rcpts: <h.mustermann@example.com>, settings_id: default_in

Is just running Rspamd enough?

- Not out of the box!
- Rspamd needs to be configured for your infrastructure
- Additional reputation data or internal resources to generate them yourself (monitoring, spamtraps)
- There are plenty of free or paid resources you could use
  - RBL e.g. Spamhaus, Abusix and many more
  - Fuzzy Database instances (Rspamd – paid/free)
  - Look for modern Blocklist types like Email-hash, URL-hash, Bitcoin hash (e.g. abuse.ch)
  - Antivirus Signatures
  - Threat intelligence feeds – ask your snakeoil provider ;)

Build your own Reputation Service

(and maybe share it)

- It’s the best you can get for your own infrastructure without vendor lock-in
- learn detected incoming spam mails
  - Text Matching Algorithms
  - Reputation: IP, Domain, Headers, URLs etc
  - Local neural network Learnings
- Use weighted results instead of static rules
- One word to Rspamd Fuzzy Plugin
  - Weighted, distributed -> shingle hashes based text matching
  - Fuzzy Database learning and querying can be shared
    - open public groups
    - closed groups
    - or can even be a commercial service

Are commercial Mail-Security Appliances better?

- Marketing and Sales
- Fancy and powerful web-interfaces
  - But limited to predefined configuration option
- Maybe the amount of data aggregated from all appliances worldwide

- *But in our opinion - never in functionality*

heinlein

questions and discussion

Linux höchstpersönlich.

Die Heinlein-Gruppe: Gemeinsam für digitale Souveränität

Heinlein Support

- Akademie: Für die oberen 10% des Wissens – unsere Linux-Schulungen für IT-Experten.
- Consulting: Security- und Strategieberatung, Projektumsetzung und umfassender Support für IT-Administratoren
- Services: SLA-Verträge, Hosting und Lizenzen als Unterstützung & Absicherung Ihrer kritischen IT-Infrastruktur

Weitere Marken

- mailbox.org: E-Mail, Online-Office, Cloud-Speicher und Videokonferenzen nach neuesten Sicherheitsstandards und mit grüner Energie.
- OpenTalk: Videocalls, wie sie sein sollten – mit unserer sicheren, benutzerfreundlichen und skalierbaren Videokonferenz für Behörden, Provider, Unternehmen und Schulen.

CompetenceCall

Das Backup für Ihre Server-Administration.

Nutzen Sie unsere SLA-Verträge und sichern Sie sich den 24/7-Support unserer Linux-Consultans.

- Kontimuierliche Absicherung mit garantierten Reaktionszeiten und festen SLAs
- Rückendeckung im Notfall: mindestens LPIC-2 zertifizierte Profis mit jahrelanger, täglicher' Admin-Erfahrung
- Projektunterstützung: maßgeschneiderte Lösungen, die Flexibilität, Sicherheit, Administrierbarkeit und Hochverfügbarkeit vereinen
- Services: Performanceanalyse, Serverhärtung, Netzwerkanalyse, Konfigurationshilfe, Datenrestaurierung

Werde Teil des Teams

- Du bist neugierig, voller Tatendrang und überzeugt von Linux, Open Source und sicherer, freier Kommunikation?

- Wir freuen uns über Unterstützung im Team:
  www.heinlein-support.de/jobs

Bleiben wir im Kontakt

Carsten Rosenberg

Tel. +49 30 40 50 51-46
c.rosenberg@heinlein-support.de

Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de

Bleiben wir im Kontakt

Manu Zurmühl

Tel. +49 30 40 50 51-51
m.zurmuehl@heinlein-support.de

Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de