From Surveillance to Security: In-House Mail Servers for Email Privacy

Presented by:

Matteo Pasotti

ITC passionate, hacker, devops (by need)

linkedin.com/in/mpasotti

mastodon.uno/@devrandom

Every Device Needs an Account

- Today, every smartphone or tablet requires a user account to fully function.

- - Apple (iCloud)

- - Android (Google Account)

- - Windows devices (Microsoft Account)

- This account is almost always tied to an email address.

Big Tech's Dominance in Email Services

- In 2024, most users rely on free email services from big tech companies:

- - Google Gmail

- - Microsoft Outlook

- - Apple iCloud

- These services are fast, reliable, and heavily integrated into the devices' ecosystems.
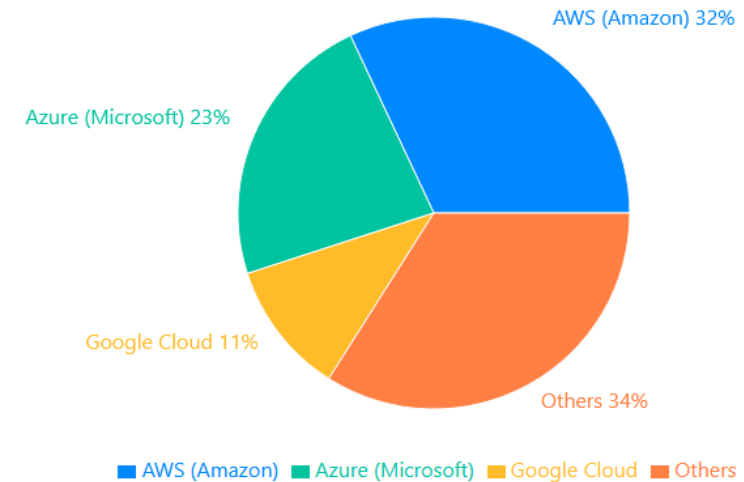
Synergy Research Group's report for Q4 2023 cloud infrastructure market share

https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/
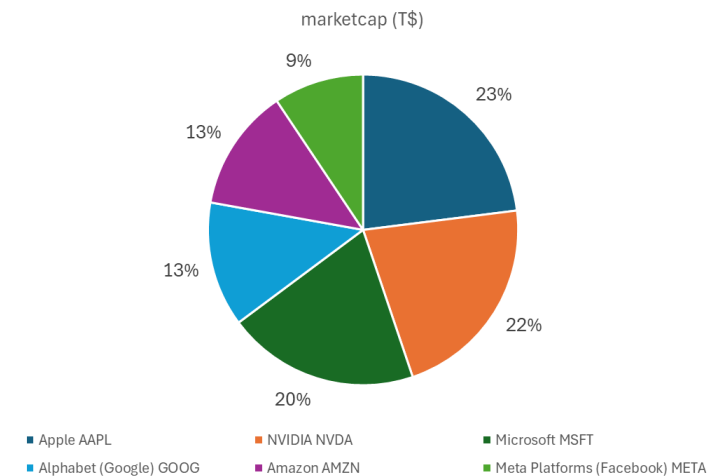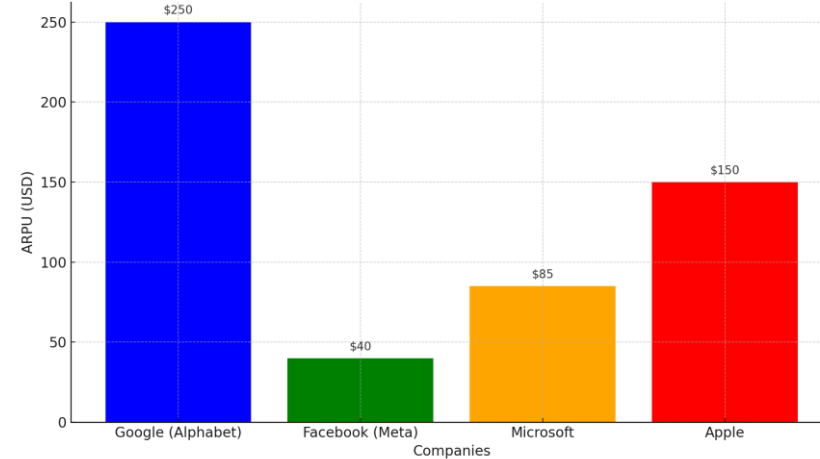
Why Configure Your Own Email Server in 2024?

- What's the point of setting up your own mail server?

- - **Privacy**: Control your data and avoid surveillance

- - **No ads** neither **data mining**

- - **Customization**: Full control over your email infrastructure
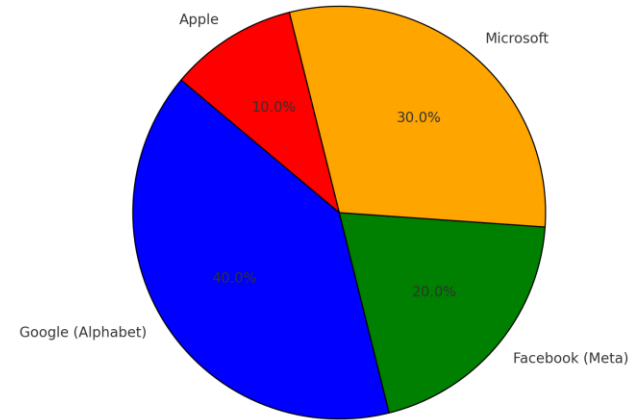
Source: Gartner, Statista and IDC

ARPU (year) = Total Revenue / Total User

Estimated Yearly Cost:

SBC

- RPI4 (no in idle): ~20€

PC

- Avg PC: ~200€

VPS or cloud instance

- €100 - €500 (depending on your needs)
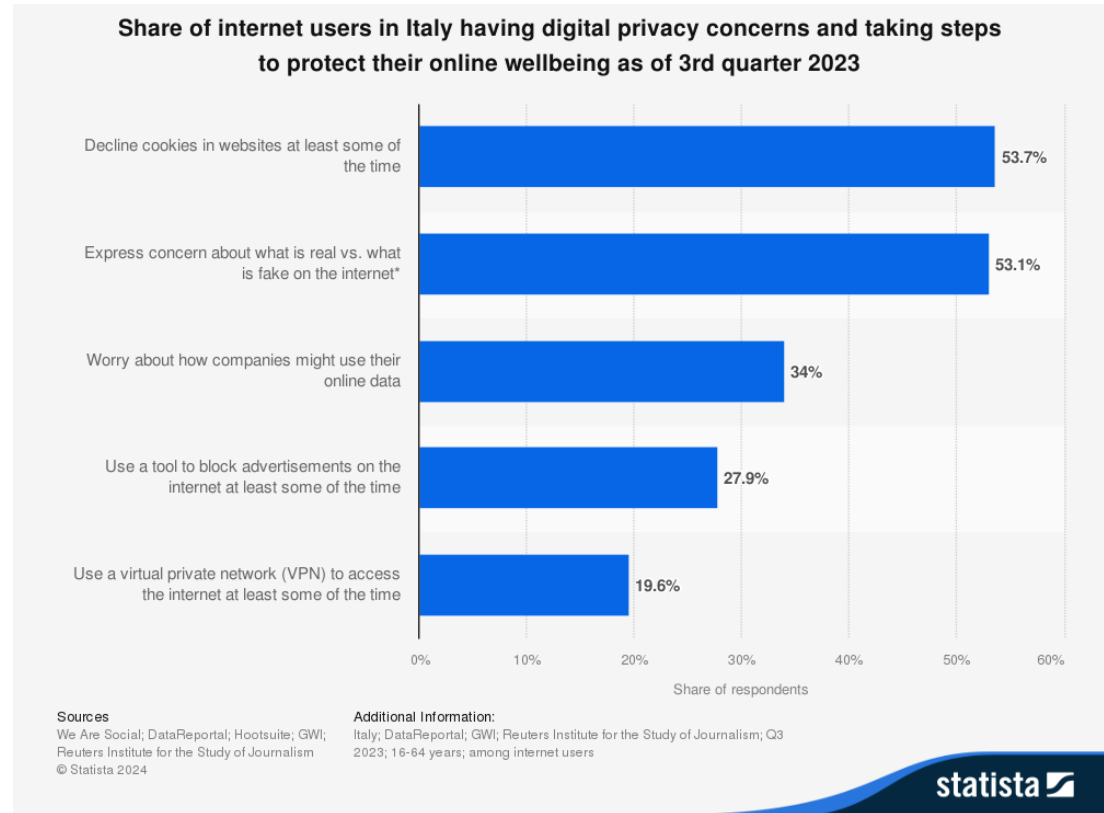
Surveillance in Italy

Sources

We Are Social; DataReportal; GWI; Hootsuite; Reuters Institute for the Study of Journalism

Digital 2024: Italy

Published by

We Are Social; DataReportal; Hootsuite

Share of internet users in Italy having digital privacy concerns and taking steps to protect their online wellbeing as of 3rd quarter 2023

Decline cookies in websites at least some of the time	53.7%
Express concern about what is real vs. what is fake on the internet*	53.1%
Worry about how companies might use their online data	34%
Use a tool to block advertisements on the internet at least some of the time	27.9%
Use a virtual private network (VPN) to access the internet at least some of the time	19.6%

Share of respondents

Privacy: A Right, Not a Privilege

"I've got nothing to hide" – A Common Misconception

Privacy isn't about hiding; it's about protecting **our fundamental rights** as citizens.

Privacy Protects Everyone

In a democratic world, privacy enables **freedom of thought, expression, and association** without fear of unjust scrutiny.

Privacy: A Right, Not a Privilege

Personal boundaries	Safeguards the details of everyday life that shape our identity and relationships.
Security	Helps prevent misuse of information for identity theft, discrimination, or exploitation
Freedom of opinion	Allows open discussion and political beliefs without surveillance chilling free speech.

Remember: Privacy is not about hiding wrongdoings; it's about preserving our freedom, dignity, and autonomy in an interconnected world.

Mail server main requirements

Setup a fully functional mail server on a SBC (RPI or similar), on a personal computer or on a VPS

Required: DNS already working
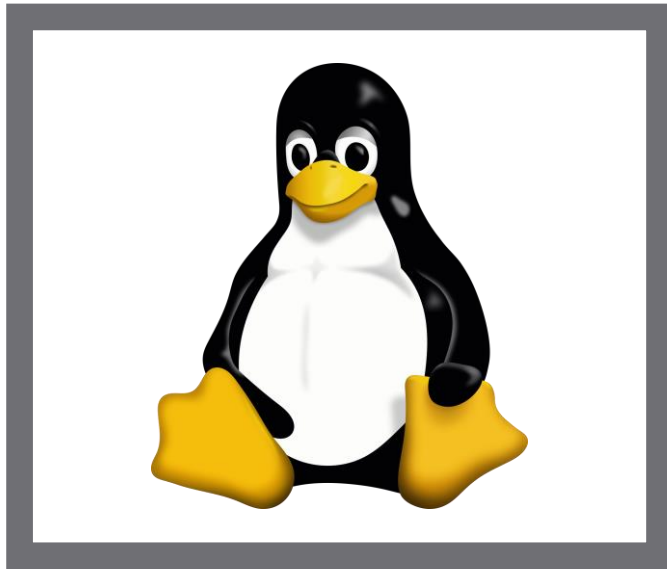
Choosing the Right OS: Why Linux Over *BSD for Mail Servers

- **Linux** Pros:

- - Wide community support, security patching, and software compatibility

- Linux Cons:

- - Higher attack surface, resource-intensive

- ***BSD** Pros:

- - Security and stability, lightweight

- *BSD Cons:

- - Limited software support, smaller user base
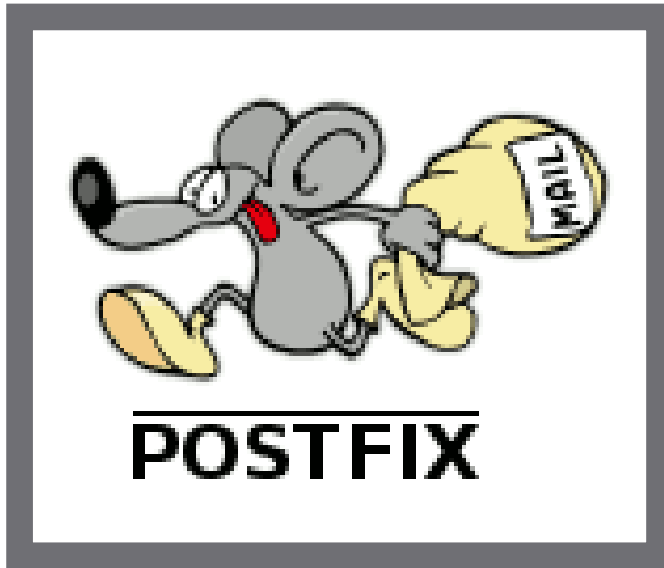
Postfix and Dovecot: The Gold Standard for Mail Servers

- **Postfix** Pros:

- - Secure, modular

- Postfix Cons:

- - Complex initial setup

- **Dovecot** Pros:

- - Fast, secure

- Dovecot Cons:

- - Limited to IMAP/POP3

Postgrey

Apache SpamAssassin™

Effective Antispam: greylisting policy server, SpamAssassin, and Blocklists

- **postgrey** Pros:

- - Reduces spam, easy to manage

- postgrey Cons:

- - Delays legitimate emails

- **SpamAssassin** Pros:

- - Highly customizable, open-source

- SpamAssassin Cons:

- - Resource intensive

Firewall Security: (ip|nf)tables and fail2ban

- **Iptables / nftables** Pros:

- - Customizable, integrated with Linux

- iptables Cons:

- - Complex syntax (nftables is relatively simpler)

- **fail2ban** Pros:

- - Automated defense, configurable

- fail2ban Cons:

- - Limited to log monitoring (evaluate NIDS alternatives alongside a greater resources consumption)

Keeping an Eye on Things: Monitoring with Zabbix or Centreon

- **Zabbix** Pros:

- - Feature-rich, free

- Zabbix Cons:

- - Complex setup

- **Centreon** Pros:

- - User-friendly, good integration

- Centreon Cons:

- - Limited free features

Securing Your Emails with OpenDKIM and OpenDMARC

- **OpenDKIM** Pros:

- - Enhances trust, improves deliverability

- OpenDKIM Cons:

- - Requires precise DNS configuration

- **OpenDMARC** Pros:

- - Domain protection, customizable policies

- OpenDMARC Cons:

- - Reporting challenges

DNS Done Right: Key Steps for Mail Server Setup

- DNS Setup:

- - MX Records for mail routing

- - SPF to define permitted senders

- - DKIM to encrypt email signatures

- - DMARC to prevent spoofing and phishing

Intrusion Detection with AIDE, AUDITD, and Wazuh

- **AIDE** Pros:

- - Lightweight file integrity monitoring

- AIDE Cons:

- - No real-time alerting

- **AUDITD** Pros:

- - In-depth system monitoring

- AUDITD Cons:

- - Complex configuration

- **Wazuh** Pros:

- - Comprehensive SecInfoEventMgmt and FileIntegrityMonitor solution

- Wazuh Cons:

- - Resource intensive

A working example

Mail server running

Do not want to configure every single piece of software? Some alternatives

Modoboa

Mail-in-a-Box

iRedMail

Mailcow

Zimbra

Happy Hacking & Secure Sending!

Key Takeaways:

- [cit.] *When something is free you are the product*
- Running your own mail server is a powerful step toward true privacy (*not sufficient by the way*)
- Though setup has its challenges, the benefits of security and control are priceless
- Whether you're a tech enthusiast or privacy advocate, every small step helps push back on data centralization

Thank you & Keep your data safe! 👾 💻 ✉️