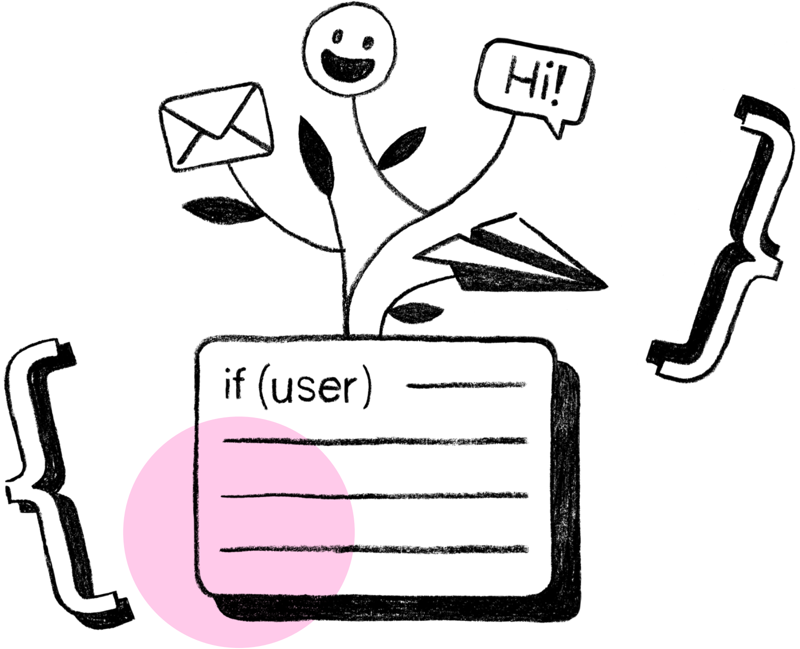
halon

Epost-säkerhet

Fredrik Poller
Product Manager

Securing email worldwide since 2006

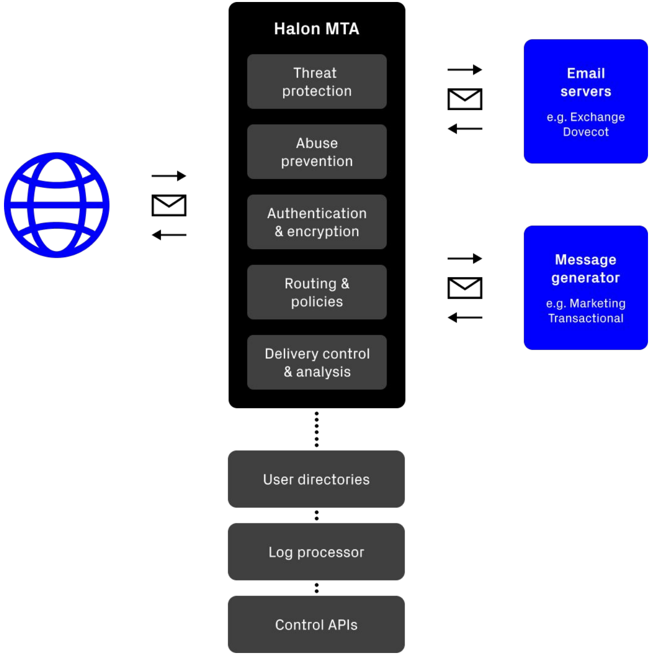
- Halon Security AB was founded 2006 in Sweden
- HQ in Gothenburg, Sweden with offices in San Francisco and Washington D.C, USA
- 250 clients on four continents



The Halon MTA at a glance

Security functionality

- State-of-the-art advanced threat protection
- Supporting the future of encryption and authentication



Deliverability functionality

- Enable best-in-class deliverability via adaptive and granular controls
- Industry leading throughput
- The developers’ choice: scriptable and container-ready

halon

Email security

Vad menar vi med det?

- Encryption standards (TLS, DANE, MTA-STS, DKIM)
- Other security standards (SPF, DMARC, reporting etc.)
- Traditional filtrering (Anti-spam, Anti-virus, rate-limiting)
- Transaction safety and deliverability (especially important together with quarantine)
- Advanced threat protection

halon

Encryption standards

TLS

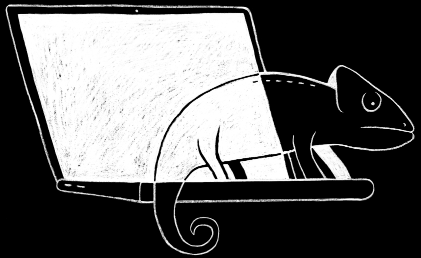
- Version 1.2 and 1.3 are the only ones currently not deprecated
- Ensures proper and safe encryption for messages in transit *

* DANE / MTA-STS

- Solves enforcement and authentication issues by allowing a receiving domain to indicate how a sender should communicate with them

DKIM

- Cryptological signing of messages to prove the identity of the sender, typically used together with DMARC



halon

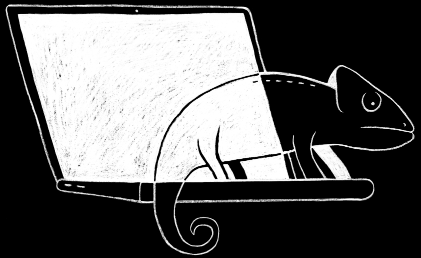
Other security standards

SPF / DMARC

- Enables a sender to dictate how a receiver should validate them

Reporting

- DMARC reporting
- TLS reporting



halon

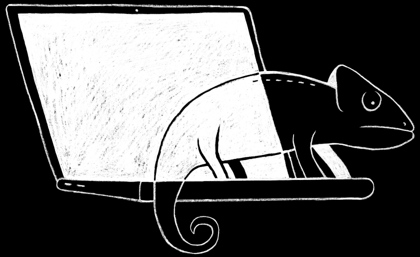
Traditional filtering

Anti-spam / Anti-virus

- Typically a combination of commercial and open source solutions
- Can be both “offline” and “online”
- Can leak personal information to third parties if configured improperly

Rate limiting

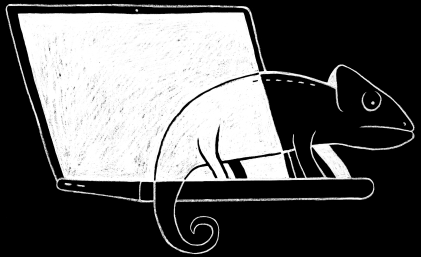
- Most commonly used for outbound flows to mitigate the effects of compromised accounts
- May be used in combination with IP pooling to limit the effects of blocklisting



halon

Transaction safety and deliverability

- In-line scanning prevents a lot of issues
- Extra care must be taken when considering quarantines



Advanced threat protection

Kärt barn har många namn

- Email attachment sandboxing
- Time of click protection

Sandboxing

CYREN

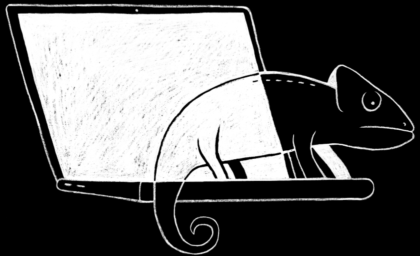
Lightweight sandboxing *

- Uses AI analysis approach
- Fast - can be run inline
- Cheaper than real sandboxing
- Runs on-prem

SOPHOS

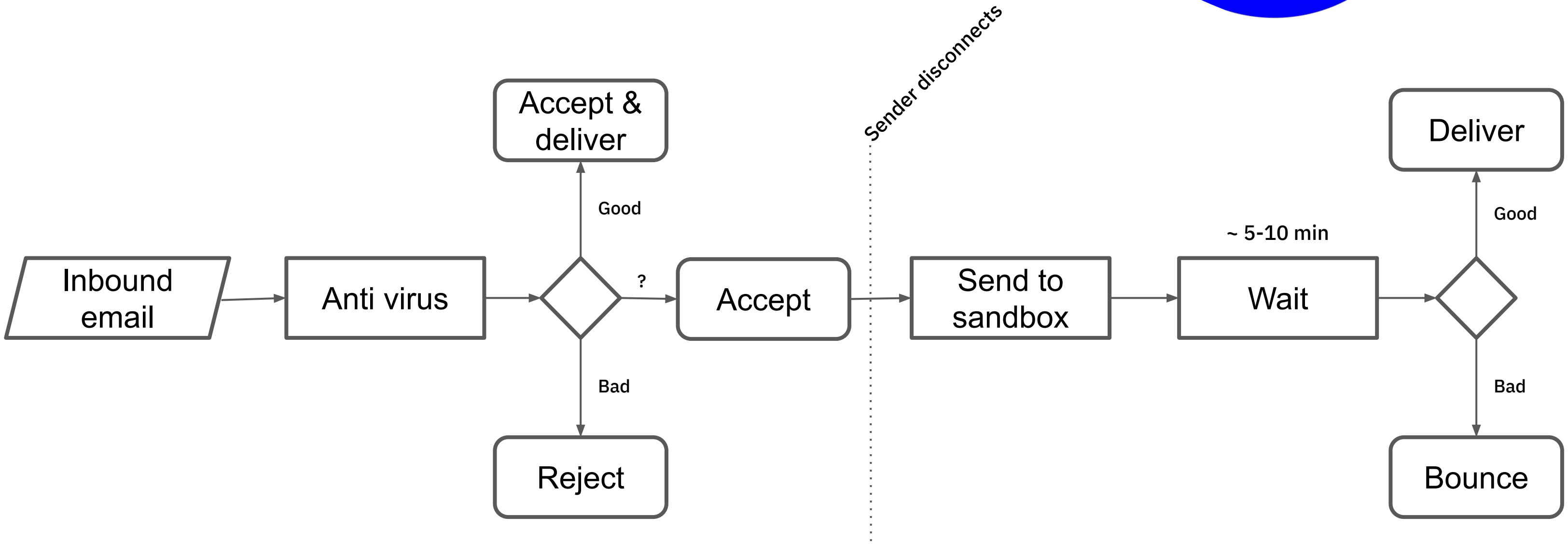
Real sandboxing

- Supports pre-scanning with Sophos anti-virus
- Executes files in a real environment



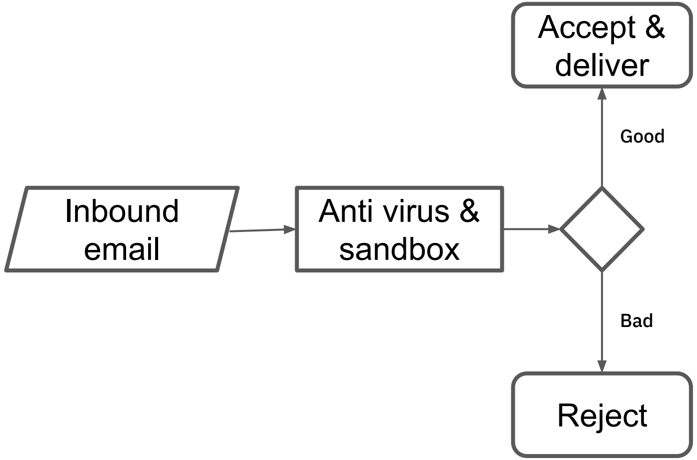
Typical sandboxing workflow

Real sandboxing with execution



In-line sandboxing workflow

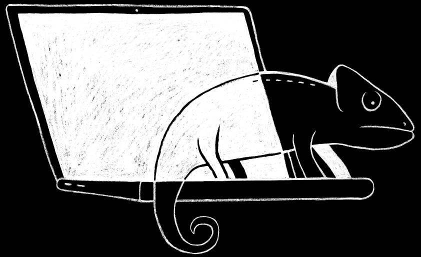
AI analysis, no real execution



halon

Time of click protection

- Content of websites are sometimes changed after delivery
- Does scanning in real time when opening links
- Typically together with a commercial provider



halon

Thank you!