

CronLab



STOP THE THREAT

- Threat stopped before reaching network
- Prevents spam, viruses and phishing attacks

POWER AND AVAILABILITY

- Sweden based clustered servers
- Filters above 99.95% of spam

AS SIMPLE AS IT GETS

- Up and running in minutes
- No user changes required

NO LOST EMAILS

- Severe spam and viruses stopped
- User notified by uncertain spam through quarantine
- Search through all emails up to 30 days old
- Track email delivery stages in detail

A COST EFFECTIVE SOLUTION

- Low prices saving you money without sacrificing quality

INNOVATIVE ADD-ONS

- Email Attachment Saver allows sending/receiving large emails
- Outgoing filtering prevents blacklisting and reputational damage
- Customized layout for improved marketing

DEPLOYMENT

- Hosted (SaaS): point the domain straight to CronLab's servers
- Appliance: Install your appliance in only 10 minutes

KEY FEATURES

- **Virus scanning:** Scans emails and attachments (including zip files)
- **File type blocker:** Blocks dangerous file types and content
- **Blacklists:** Checks sender against lists of known spammers
- **Address validation:** Verifies receiving address to be valid
- **Local whitelist generation:** Automatic generation of whitelists based on sender reputation
- **Statistical analysis:** Bayes analysis of emails to identify spam
- **Experience based training:** Known legitimate senders get improved reputation to ensure email deliverability
- **Multilingual system:** Available in English, Swedish and French
- **Quarantine:** Secured user-level quarantine for uncertain emails
- **Customized rules:** Proprietary rules to improve filtering rates
- **Post processing:** Quarantined emails are re-processed several times for optimal hit rate
- **User based training:** Users can train the filter to improve accuracy
- **Anti-Virus engine:** Commercial Anti-Virus available as an add on





OUTGOING SPAM FILTERING

PROTECT YOUR BUSINESS PARTNERS

- All outgoing emails are scanned with CronLab's engines, fighting spam, viruses, malware and phishing attacks

UNPRECEDENTED AVAILABILITY

- Ensure safe delivery of your emails no matter where you are
- Works on all networks with all email servers and clients, including mobile phones

ALARMS WARN FOR POTENTIAL PROBLEMS

- An alarm is sent to the administrator if a computer attempts to send out spams or viruses

STRONG ENCRYPTION AND SECURITY

- All communication is handled through strong TLS or SSL encryption
- User-based accounts to ensure the validity of the sender
- Domain-wide accounts can be set up for authorized server relays

PREVENTS BLACKLISTING

- Minimizes the risk of your domain being blacklisted as a spammer as spams and viruses are removed before they reach the recipient

EMAIL ATTACHMENT SAVER

ATTACHMENTS ARE REPLACED BY LINK TO WEB INTERFACE

- If the email is over a certain size, it is stripped of all attachments. Instead a link to a website is added along with instructions
- Recipient simply downloads the attached files from a website, where files are stored for 100 days

NO TRAINING OR EXTRA PROGRAMS REQUIRED

- Uses a format known to users (email). No training or extra programs required

HANDLES LARGE FILES

- Files of up to 2GB can be handled by the system

SAVES NETWORK BANDWIDTH

- Avoids bouncing emails

REDUCES USER FUSTRATION

- Simplifies the sending of large files and avoids common error messages stating that the email is too large to be handled by the email server or the inbox



WHY A WEB FILTER?

ENHANCED SECURITY

- Protects the company against internal risks linked to unauthorised browsing.
- Protects the company against the external risk of information theft through phishing attacks.

ENHANCED PRODUCTIVITY

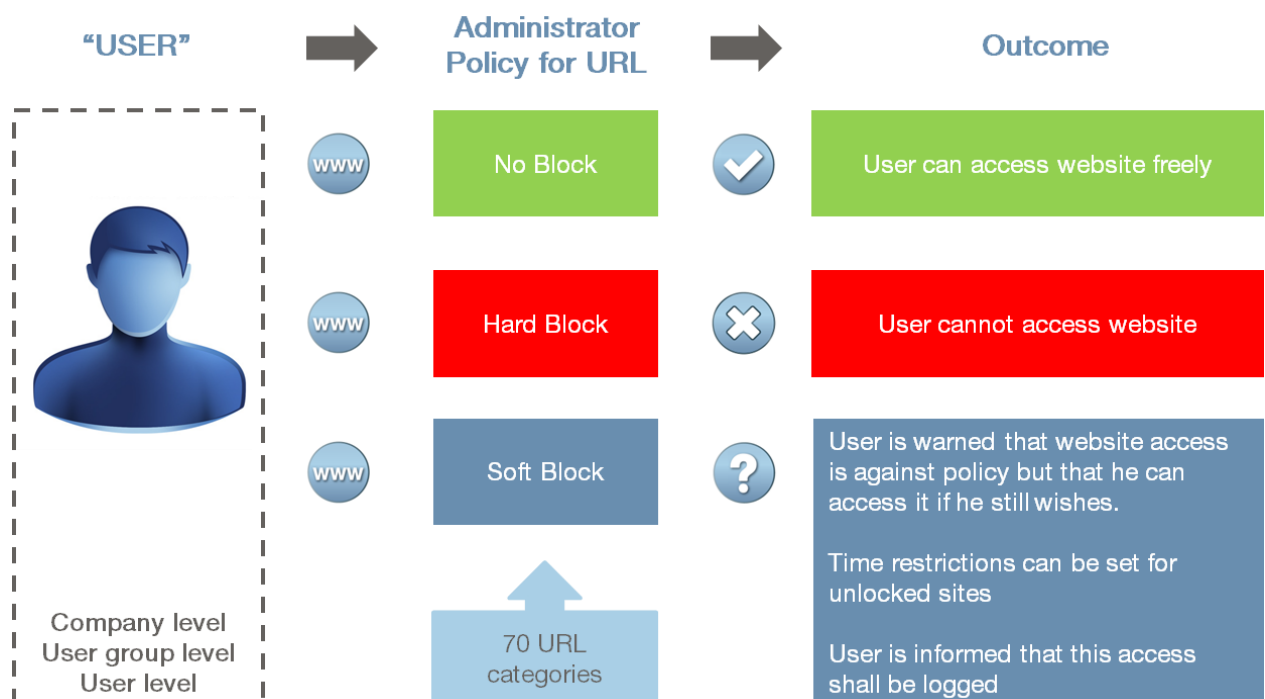
- Employees do not waste office time and company bandwidth on non-productive browsing.
- Enables control of internet traffic within the organisation.

HOW DOES IT WORK?

- The CronLab Web Filter is a SaaS (Cloud) based security service requiring no local software agent installation.
- All traffic is routed through CronLab's web proxy where it is thoroughly analysed. Actions are taken based on the web filter settings managed by the administrator representing the company or group policy.
- The filter block setting can be customised to be:
 - **Hard block** – completely blocking access to the site
 - **Soft block** – allowing site access for an unlimited or limited amount of time after warning message

SPECIFICATIONS

- **Compatible** with all major browsers and systems
- Prevents unauthorised browsing
- Protects against phishing attacks
- Over 70 different URL categories
- Protects stationary users
- Protects roaming users
- **Soft block** – access after validation
- **Time restrictions** can be set for unlocked sites
- **White labelling** available
- Extensive usage statistics and reports
- **Granularity** of policy setting from company level to the single user level
- European data centres



CronLab Ltd

Phone: +44 (0)208 123 38 26 / 43 46

info@cronlab.com

www.cronlab.com



UNITED KINGDOM & IRELAND

CiRRUS Management Solutions

www.cirrus-ms.co.uk

BENELUX

CRYPSSYS Data Security B.V.

www.crypsys.nl

GERMANY, AUSTRIA & SWITZERLAND

VNC - Virtual Network Consult GmbH

www.vnc.biz

ROMANIA

Provision Software Division SRL

www.provision.ro

Please contact CronLab directly for inquiries about regions.