HORNETSECURITY

FACT SHEET

WEB FILTER

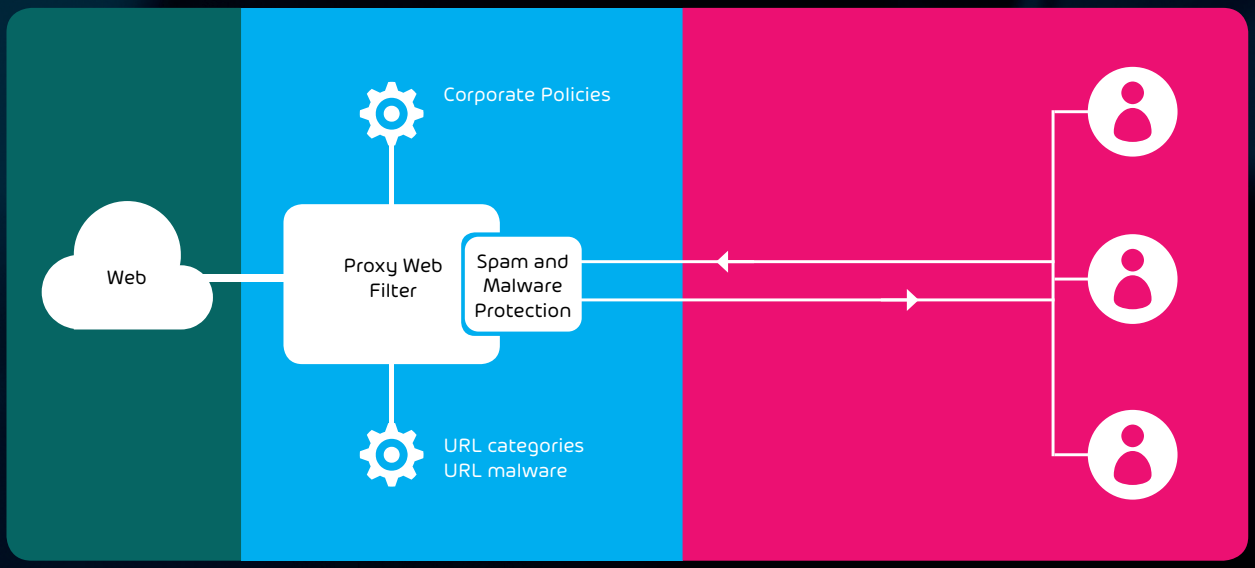
Block dangerous websites and harmful downloads with Web Filter.

Access to the Internet is essential for many companies worldwide. But this also makes it possible for cybercriminals to use hijacked or fake websites to try to steal access data, credit card details or personal information or to smuggle malware into the company system unnoticed. Web Filter reliably blocks dangerous Internet activities and prevents hacker attacks.

Protection from:

- Malicious file downloads
- Penetration of malware into the company network
- Drive-by downloads

INTEGRATION OF THE WEB FILTER INTO THE SECURITY MANAGEMENT SYSTEM



One of the essential tasks of the Web Filter is the protection of your own IT infrastructure against the dangers of the Internet. Controlling the use of the Internet is also important. The proxy Web Filter can be adjusted so that these two adjusting screws are set perfectly.

HORNETSECURITY

FACT SHEET

FEATURES FOR **SECURE WEB ACCESS:**

HTTPS scanning: Even encrypted websites are checked for viruses and other malicious software so that they cannot penetrate the company infrastructure.

Scan of FTP connections: FTP connections can be checked for the upload and download of corrupted files and if necessary blocked.

Ad blocker: Prevents the display of advertisements.

Application control: Certain versions of applications that access the Internet can be blocked or selectively released. Detects and blocks "hijacked" applications that spread malware.

Release request management: Processing of release requests by administrators via emails.

User authentication by login, LDAP matching or fixed IP address: Employees can be grouped into specific groups that share the same web filter settings (policies, settings and in logging).

Automatic authentication: The connector ensures that the user is always automatically logged on to the Web Filter Service.

Web threat management: Unknown websites are blocked and not displayed. Sites with known security loopholes can be blocked, as can the use of an anonymous proxy. Content available for download is analyzed in real time and prevented from downloading if there is a danger.

Company specific policies: Specific applications such as Instant Messenger cannot be used during working hours, illegal content cannot be visited or social media sites cannot be accessed.

Temporary release of websites: The user can visit a website that is actually blocked for a certain period of time and thus continue to work without delay. These releases are logged.

Data type detection of downloads: Prevent downloads of specific types of file (e.g. EXE or MP3 files).

Break times: Groups or users can be given specific time slots in which different web filter settings than the usual company defaults take effect.

Reporting of wrong categorizations directly from the browser: Fast, simple and efficient reporting allows for quick customization and improvement of the Web Filter.

Live monitoring: Receive a statistical evaluation of the surfing behavior. A detailed and anonymous overview of the web accesses of groups, individual users and IPS appears in the statistics area of the Web Filter module in the Control Panel.

Import of generally valid whitelists (also explicit whitelisting): Administrators can set up the web filter to meet the individual needs of the company.