HORNETSECURITY

FACT SHEET

WEB FILTER

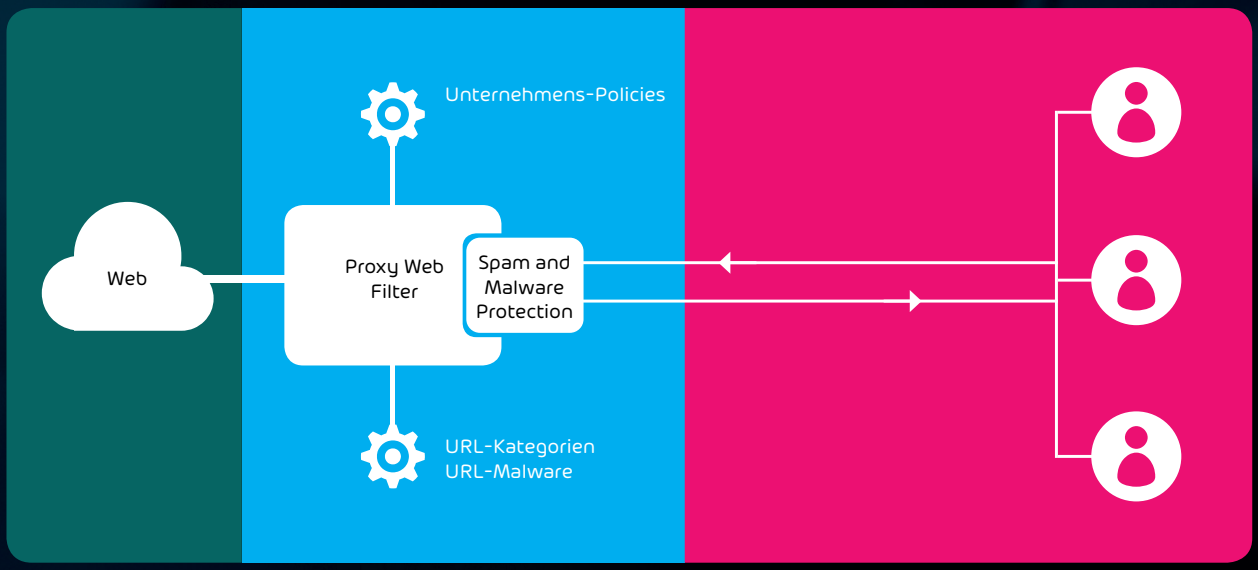
Blockieren von gefährlichen Webseiten und schädlichen Downloads mit dem Web Filter.

Der Zugriff auf das Internet ist für zahlreiche Unternehmen weltweit maßgeblich. Doch auch hier versuchen Cyberkriminelle mit gekaperten oder gefälschten Webseiten Zugangsdaten, Kreditkartenangaben oder persönliche Informationen zu stehlen oder unbemerkt Schadprogramme in das Unternehmenssystem zu schleusen. Der Webfilter blockiert zuverlässig gefährliche Internetaktivitäten und beugt Hackerangriffen vor.

Schutz vor:

- **Downloads von schädlichen Dateien**
- **Eindringen von Malware ins Unternehmens-Netzwerk**
- **Drive-By-Downloads**

INTEGRATION DES WEB FILTERS IM SECURITY MANAGEMENT SYSTEM



Der Schutz der eigenen IT-Infrastruktur vor den Gefahren des Internets ist eine wesentliche Aufgabe des Webfilters. Darüber hinaus ist die Steuerung der Nutzung des Internets von Bedeutung.
Der Proxy-Webfilter lässt sich so anpassen, dass diese beiden Stellschrauben ideal eingestellt sind.

HORNETSECURITY

FACT SHEET

FEATURES FÜR DEN **SICHEREN WEBZUGANG:**

HTTPS-Scanning: Selbst verschlüsselte Webseiten werden auf Viren und andere Schadsoftware überprüfen, so dass sie nicht in die Unternehmens-Infrastruktur eindringen können.

Scan von FTP-Verbindungen: FTP-Verbindungen lassen sich auf den Up- und Download von schadhaften Dateien überprüfen und gegebenenfalls unterbinden.

Ad Blocker: Verhindert die Anzeige von Werbeeinblendungen.

Application Control: Bestimmte Versionen von Anwendungen, die auf das Internet zugreifen, können gesperrt oder gezielt freigegeben werden. Erkennt und blockiert „gekaperte" Anwendungen, die Malware verbreiten.

Release Request Management: Bearbeitung von Freigabeanforderungen durch den Administratoren per E-Mail.

Benutzerauthentifizierung per Login, LDAP-Abgleich oder fester IP-Adresse: Mitarbeiter lassen sich in bestimmte Gruppen zusammenfassen, für die dieselben Web Filter-Einstellungen (Richtlinien, Einstellungen und im Logging) gelten.

Automatische Authentisierung: Mit dem Connector ist der Benutzer stets automatisch beim Web Filter Service angemeldet.

Web Threat Management: Unbekannten Webseiten werden blockiert und nicht angezeigt. Seiten mit bekannten Sicherheitslücken lassen sich ebenso sperren wie die Nutzung eines anonymisierten Proxys. Zum Download bereitstehender Content wird in Echtzeit analysiert und bei einer Gefahr am Herunterladen gehindert.

Temporäre Freigabe von Webseiten: Der Benutzer kann eine eigentlich gesperrte Webseite über einen bestimmten Zeitraum hinweg besuchen und so ohne Zeitverzögerung weiterarbeiten. Diese Freigaben werden protokolliert.

Unternehmensspezifische Policies: Bestimmte Anwendungen wie Instant Messenger sind während der Arbeitszeit nicht nutzbar, illegale Inhalte dürfen nicht besucht oder Social Media Seiten nicht aufgerufen werden.

Datentyperkennung von Downloads: Unterbinden von Downloads bestimmter Dateitypen (z. B. EXE- oder MP3-Dateien).

Pausenzeiten: Gruppen oder Benutzer können bestimmte Zeitfenster erhalten, in denen andere Webfilter-Einstellungen greifen als die üblich geltenden Firmenvorgaben.

Meldung falscher Kategorisierungen direkt aus dem Browser heraus: Die schnelle, einfache und effiziente Meldemöglichkeit erlaubt eine rasche Anpassung und Verbesserung des Web Filters.

Live Monitoring: Erhalten Sie eine statistische Auswertung des Surfverhaltens. Eine detaillierte sowie anonymisierte Übersicht über die Web-Zugriffe von Gruppen, einzelnen Benutzern und IPS erscheint im Statistik-Bereich des Web Filter Moduls im Control Panel.

Import von grundsätzlich geltenden Whitelists (auch Explicit Whitelisting): Administratoren können den Webfilter individuell auf die Unternehmensbedürfnisse einrichten.