Solution Brochure

RADICALIZATION BLOCKING

Protect Users from Terrorist Content on the Internet

The internet is seeing a rise in terrorist and extremist content with hate speech sites having more than doubled since the start of the pandemic. Our partner, the Counter Terrorism Internet Referral Unit (CTIRU) reported a 7% increase in 2020 in the amount of suspected terrorist content, compared to the year previous. Now more than ever, web filtering has become a necessity to protect users from radicalization content on the internet.

In their efforts of both radicalization and recruitment, terrorists, militias, and other illicit organizations have commonly used social media as a key piece of their calculated strategy.

Netsweeper provides controls for managing URLs and web applications, Enabling Radicalization Blocking:

- Lists include CTIRU, and terrorism related content. These lists are available through Netsweeper but need to be enabled as they are not active by default.
- Once the policy service list is reloaded and tested, custom reports can be set up, edited, and run.
- Contact Netsweeper Support (support@netsweeper.com) to enable the CTIRU list for your application.

Traffic Logging, Reports, and Analytics

Netsweeper can log all outgoing traffic on the network. Reports are customizable and can be generated on user internet traffic based on various categories and content.

If a user on the network attempts to access multiple terrorism sites within a set period of time, they will be flagged. An email alert will be sent once the report is generated.

Sharing Data with the Authorities

Law enforcement agencies can use anonymized meta data from the Netsweeper system to obtain warrants for investigation and/or prosecution.

We do not provide user identity information to authorities, but the time of access information can prove useful in correlating illegal activity as part of lawful intercept requests. .

About Netsweeper

Since 1999, Netsweeper has been a leading provider of online filtering and digital safety solutions worldwide. We protect over 1.2 billion users in our network footprint using hybrid AI technology to identify harmful content, contact, conduct, and commerce in real-time. Localized in 47 languages, and with over 90 filtering categories, we have accrued and strategically categorized 12 billion URLs to date and receive requests for over 50 million new URLs each day. We support educational institutions, government organizations, businesses, service providers, carriers, and OEM partners across the globe.

Ver 6.6.2023