CONCEAL

How ConcealBrowse is Different than a DNS Filter

ConcealBrowse and DNS filters are both vital tools in the cybersecurity domain, each designed with distinct objectives and functionalities. While both contribute to securing online navigation, understanding their differences is key to leveraging them effectively.

Primary Objective

ConcealBrowse: Conceal's AI-powered capabilities seamlessly identify emerging threats and proactively neutralise them, ensuring comprehensive protection in the ever-evolving cyber landscape.

DNS Filter: DNS filters focus on security by screening domain names to block or allow access based on preset criteria. Their primary role is to stop users from accessing malicious, inappropriate, or blacklisted websites.

Functionality

ConcealBrowse: Unlike traditional security solutions, which rely on static rules and predefined threat signatures, ConcealBrowse utilises the advanced capabilities of AI to provide dynamic protection. This ensures not just a reactive response to known threats but a proactive approach to potential future risks, allowing things to be caught more timely than traditional detection tools.

DNS Filter: Before a user accesses a website, the DNS filter checks the site's domain against a database of safe and unsafe websites. If the site is deemed unsafe, access is denied, effectively preventing potential threats.

Application

ConcealBrowse: By providing users with real-time feedback on their actions and potential threats, organisations foster a security-first culture, empowering employees to be the first line of defence - matter the industry.

DNS Filter: Ideal for organisations and educational institutions wanting to control internet access, protect users from malware, and maintain productivity by restricting distracting sites.

User Experience

ConcealBrowse: Security shouldn't come at the expense of user experience. ConcealBrowse ensures a seamless browsing experience by intelligently analysing URLs discreetly in the background, ensuring that genuine activities are never impeded while suspicious actions are promptly addressed.

DNS Filter: Does not typically slow down browsing speeds but can restrict access to legitimate sites if they are mistakenly categorised as unsafe, occasionally leading to over-blocking.

Customisability

ConcealBrowse: ConcealBrowse's AI-driven engine, SherpaAI, learns from each interaction, continuously updating its threat recognition patterns. This means that as cyber threats evolve, ConcealBrowse evolves with them, always staying a step ahead.

DNS Filter: Highly customisable. Administrators can set up whitelists, blacklists, and category-based filters to define what content is accessible.