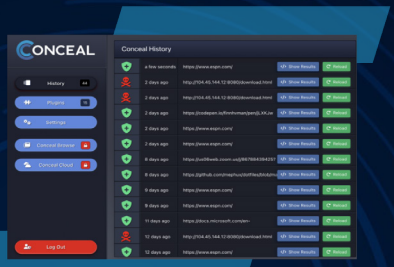
Conceal



Why Conceal?

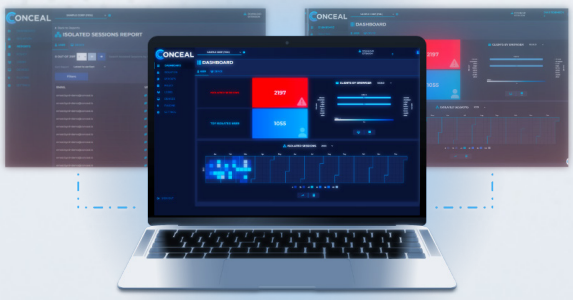
At any time, any employee can click a malicious link or access an unsecure website. This makes the web browser a major vulnerability.

ConcealBrowse stops those threats at the browser, delivering an enhanced layer of protection. Conceal's advanced features catch malware and data theft attacks that can slip through other security controls, blocking and isolating malicious activity to keep users protected.

The challenges Conceal solves

Conceal converts any browser into a zero-trust browser, catching some of the biggest problems in cybersecurity – ransomware and credential theft. When you browse the internet, threats can appear anywhere. Conceal's cutting-edge technology provides robust protection, working in the background to determine the risk of any browser activity.

When Conceal determines a request as malicious, blocks are put in place. If the risk is unknown, Conceal will isolate the activity. These steps enable users to continue browsing in a safe environment and avoid potential credential theft or ransomware attacks.



Benefits of Conceal

Protect sensitive data

Phishing links are actively blocked, protecting critical data.

Real-time threat analysis

Using AI, Conceal detects cyber threats early, significantly reducing the risk of data theft or ransomware threats.

Advanced phishing detection

Conceal's AI engine enables it to adapt quickly to rapidly evolving cyber threats and maintain robust threat detection.

Privacy for users

Conceal's browser extension does not upload or retain sensitive browsing history, maintaining user privacy.

Automatic endpoint protection

By proactively identifying and isolating malicious activity, endpoints remain protected.

No training required

Fast and seamless deployment requires no training meaning users are protected instantly.

Add company information here

Add company logo here