CONCEALBrowse™

Close Your Browser Security Gap

ConcealBrowse excels by delivering extensive, real-time protection across all web interactions through in-browser content analysis backed by threat isolation, offering seamless and comprehensive web security. It functions as an internal safeguard, proactively addressing threats from within the user's browsing environment. ConcealBrowse uses selective remote browser isolation to airgap users from suspicious sites, reducing risk to the corporate network.

Key Features

- Phishing Protection
- Real-Time in Browser Content Analysis
- Dynamic AI backed detection engine
- Content Filtering
- Selective Remote Browser Isolation
- Policy Enforcement
- Installation Enforcement
- Optional URL Classification Content Blocking
- Risky User Web Activity Monitoring & Alerting
- Chrome, Edge, Firefox and Chromium browser support
- Out of the box integrations with third party security tools: SIEM, Threat Intel, Network/Firewall and MDR/XDR/EDR
- Easy deployment options: device based via MSI with third party RMM/EMM or user based

Use Cases

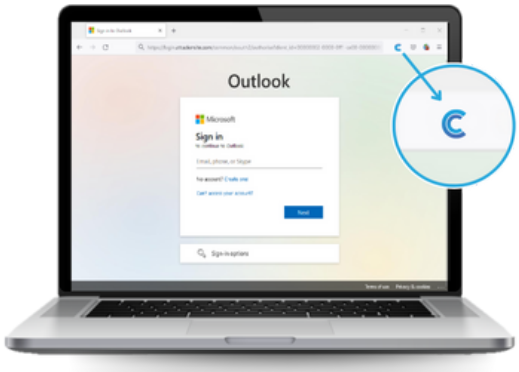
Phishing Protection for Employees: ConcealBrowse's phishing protection automatically detects the phishing attempt. It can either block the page entirely or isolate the user from the phishing site in a secure, remote environment, preventing any sensitive information from being compromised. IT administrators or security operations teams receive an alert about the attempted phishing event.

Real-Time Threat Detection and Mitigation: ConcealBrowse's Real-time In-Browser Content Analysis with Dynamic AI-Backed Detection Engine constantly scans and analyzes web content for threats, offering immediate mitigation. This allows security teams to focus on other critical tasks, knowing that web threats are being monitored and neutralized.

Secure Browsing through Remote Isolation: ConcealBrowse's Selective Remote Isolation executes suspicious web content in a secure, remote environment, isolating any threats from the local systems. This approach allows users to access necessary information without compromising their security.

Enforcing Security Policies Across the Organization: ConcealBrowse's Security Policy Enforcement enables IT administrators to implement and manage security policies centrally. This ensures that all browsers follow the same security rules, reducing the risk of breaches due to inconsistent security practices.

Blocking Inappropriate or Risky Websites: ConcealBrowse's optional URL Classification and Content Blocking allows administrators to block access to classified URLs, preventing users from visiting potentially harmful or inappropriate sites. This helps maintain a productive and secure work environment.



ConcealBrowse inspects all sites visited by the browser and produces a risk score using proprietary content analysis, which determines one of three paths:

Verified Safe: The page is confirmed as safe, allowing the user to continue without any interruptions.

Verified Malicious: The page is identified as harmful, and access is blocked.

Suspicious: The user can proceed to the site, but only in a remote isolation session in Conceal's cloud. In this protective remote isolation environment, the user's local system is protected from the site to prevent malware downloads and credential theft attempts are blocked.

CONCEAL
(706)-481-2642
conceal.io
info@conceal.io