




ConcealBrowse 2023 Solution Brief

A Complete Guide to :
ConcealBrowse

www.conceal.io




83% of organizations
fell victim to a phishing
attack in 2021.

Executive Summary

In today's hybrid work-world, employees are spending a larger part of their day in their web browser to access cloud apps, check social media, etc. One study points to 80% of employees spending 80% of their day in their web browser. This reality, coupled with threat actors exploiting messaging platforms within websites and apps, social sites with shortened, and obfuscated links, creates a recipe for increased exposure that is not protected by existing security controls.

Employees' daily internet usage creates unavoidable risks to your company's cybersecurity posture. Simply visiting a malicious website reveals information about your company and its attack surface. Opening a downloaded file can create a pathway to your company's network for ransomware groups. In some cases, cybercriminals can use unpatched vulnerabilities to compromise a network when you simply visit a website. But your employees can't stop using the internet and must feel comfortable accessing it. They need a way to work securely in an environment where they are protected from malicious and unknown URLs, and they need to be able to do their work regardless of their technical abilities or cybersecurity awareness. ConcealBrowse provides organizations with a lightweight extension to detect, defend and isolate malicious activity at the edge.





Introduction

Web browsers are the primary gateway to the internet. For this reason, web browsers are constantly targeted by malicious threat actors to exploit vulnerabilities and gain access to sensitive data in an organization's environment. Through the web browser, a bad actor can breach an organization's security through unauthorized access to user credentials, personal information, financial data and other sensitive information.

Web browser protection is an essential component to an organization's security program. When properly secured, web browsers can serve as a critical first line of defense in protecting against cyber threats and ensuring the security of sensitive data. Web browser security can help protect against malware infections, defend against phishing attacks, prevent data breaches, and help organizations comply with regulatory requirements.



Key Challenge

One of the most targeted attack surfaces an organization must secure against is the web browser. Web browsers are complex software applications that contain vulnerabilities that attackers can exploit. Organizations need to ensure that they have up-to-date web browsers that receive regular security updates and patches.

Web-based attacks are one of the biggest security challenges facing organizations. Attackers use web browsers to deliver malware, steal sensitive information, and launch phishing attacks. Organizations need to implement security measures that protect against these types of attacks.

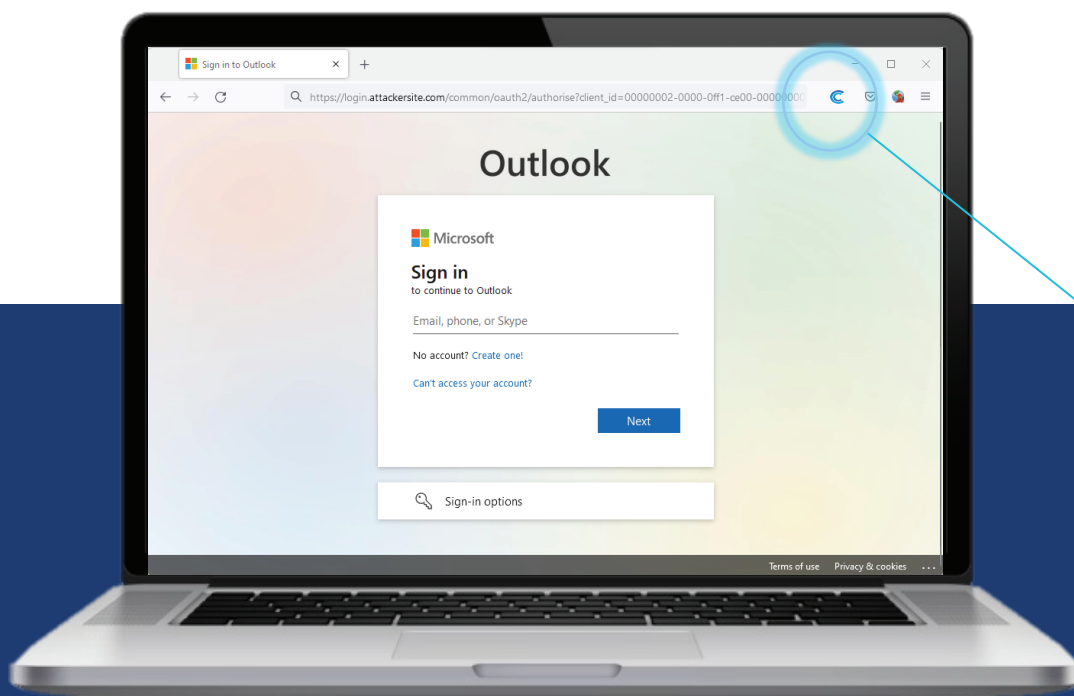
Traditional ransomware and credential theft attacks have evolved beyond email phishing. The days of an attacker sending an employee a phishing email and falling victim through clicking the link is no longer deemed sophisticated. Rather, organizations are dealing with phishing, smishing, slinking and malvertising attacks that target their employees on work applications, such as Google Drive, DropBox, Outlook and Slack, personal/social applications, such as LinkedIn, Facebook and Twitter, and through their mobile devices. This reality poses the risk of employees making crucial decisions on an ever increasing volume of requests. Which are legitimate? Which are fraudulent? Email is no longer the most significant attack vector - it is now the web browser.

Introducing ConcealBrowse, the Ultimate Solution for Browser Security

ConcealBrowse is a lightweight browser extension that converts any browser into a ZeroTrust, secure browser stopping ransomware and credential theft that bypass other security controls. Deployed in minutes and seamless to the user, Conceal protects your employees where it matters most, at the browser. With the lightweight web extension, enterprises are able to disguise and protect their online presence, and stop attacks before they gain a foothold on the endpoint.

ConcealBrowse leverages an intelligence engine that works at machine speed with near zero latency to dynamically and transparently pre-process and analyze code and move suspicious, unknown and risky code to a cloud-based isolation environment.

ConcealBrowse is a simple, drop-in solution that can easily be added to existing security packages. It requires minimal configuration and provides advanced telemetry data that can be integrated with SIEMs and common analytical tools via integrations with Splunk and Elasticsearch. Telemetry can also be consumed in a multitude of applications via a Syslog plugin.



 CONCEAL

Features

ConcealBrowse prevents users from triggering ransomware and credential theft attacks that bypass other security controls by the innovation of the following features into the lightweight and seamless extension:

Dynamic Browser Isolation -

ConcealBrowse protects every endpoint and every user from malicious, unknown URLs and sends them to isolation, while allowing known 'good' URLs to continue down their normal path. It makes proactive decisions about the security risk associated with internet use and isolates it before the activity has the opportunity to cause havoc within the user's environment.

Policy Enforcement - We integrate with existing policy controls for simple provisioning and administration of policy enforcement on the web. This administrative access enables enforcement of company policies, users, and organizations.

Address Unknown Risks - Beyond addressing known threats through policy based filtering and signature based detection, ConcealBrowse addresses unknown risks by isolating unknown activity in remote browser isolation.

Informed Decision Making -

Pre-processing intelligence and policies are fed into the ConcealBrowse decision engine to inform the extension on when to isolate unknown activity before it is too late.

Security Policy Management - In the ConcealBrowse dashboard, admins can control copy/paste capability between the isolation environment and the device. This allows admins to restrict the flow of information between safe and risky web sites and operate within their preferred risk tolerance. Additionally, users can bulk upload allow/block lists instead of having to manually enter them one-by-one, simplifying setup.

Remove Context - Automatically route risky internet traffic through Conceal's dynamic, software-defined network and isolation engine to remove context and provide extra privacy and security to users and organizations.

Risk Mitigation - By isolating potentially malicious activity before it can affect an organization's network, ConcealBrowse mitigates risks before they become a threat to your company's environment.

Multi-Tenant Management - A single instance of ConcealBrowse can be used to serve multiple customers. This feature is specifically beneficial to channel partners, easing the addition of new ConcealBrowse tenants for their customers and directly managing them from their MSP account.

Dashboards - The admin dashboard gives immediate insight to key metrics for ConcealBrowse admins. The most important metrics are highlighted at the top of the screen so that admins can quickly get an overview of how ConcealBrowse is protecting their organization. Multiple viewing options for the graphs makes it easier for admins to conduct a quick visual analysis of the data they are most interested in.

Plugins - ConcealBrowse integrates with a wide variety of other applications that exist within an organization's tech stack.

User Privacy - Individual users' browsing history and URL scan logs do not exist in the admin panel, except for URLs that were considered risky enough to block or isolate. This ensures that administrators have only the information necessary to identify and mitigate threats while maximizing the privacy of individual users.

User Friendly Interface - ConcealBrowse is easy to use and does not require any technical knowledge to set up or use. Once installed, the browser plugin causes minimal interaction with the user, minimizing interference with their web surfing.

Multi-Platform Support - ConcealBrowse is available for Windows, macOS, and Linux, and supports multiple web browsers, including Chrome.

Silent Deployment - With a silent installation process, end-users have a seamless experience when entering the web browser, not having to perform any actions to add ConcealBrowse to their browsing experience. ConcealBrowse also supports various deployment methods including the use of RMM Platforms, SCCM, Intune, and the Google Admin Console.

Benefits:

- Fast and seamless to the end-user. No training required
- Identify and isolate risky internet activity to automatically protect endpoints
- Protection for links from any application on the desktop
- Protect against ransomware and credential theft
- Reduce IT spend on detection, prevention and response solutions
- Lightweight, secure browser extension



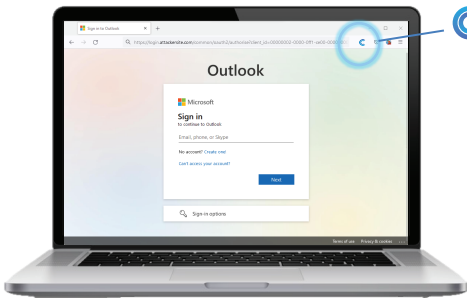
HOW IT WORKS

ConcealBrowse is a cutting-edge security solution that offers an enhanced layer of protection for users while browsing the internet. Its advanced functionality is built upon four primary steps: browser access establishment, user HTTP request, activity risk determination, and the ultimate request decision. Initially, the user establishing a connection with their web-browser while ConcealBrowse establishes a secure connection in the background. The user then will send an HTTP request via the browser or an internet facing application. In this moment, ConcealBrowse will employ to determine the risk of the request and the activity the user is trying to initiate. Once the risk level is determined ConcealBrowse determines if the request is safe and allowed to continue, unisolated, or if it is determined malicious or out of policy by which it will then be blocked. If the risk is unknown, ConcealBrowse will isolate the activity, allowing the user to continue in a safe environment, outside of the organization's network to avoid potential credential theft and/or Ransomware.

Step One

ACCESS BROWSER

User accesses their browser to begin surfing the web. Simultaneously, ConcealBrowse activates in the browser to provide an extra layer of protection at the edge.



Step Two

SUBMIT HTTP REQUEST

User sends an HTTP request via the browser or an internet facing application.



Work



Personal/Social



Mobile Device

BENEFITS:

- ✓ Credential Theft Protection
- ✓ Ransomware Protection
- ✓ Signature Based Protection
- ✓ Policy Based Protection
- ✓ Known Threat Protection



Step Three

DETERMINE ACTIVITY RISK

Identify if the activity request is risky



Step Four

ISOLATE

Isolate the unknown request through ConcealBrowse's remote browser isolation technology.



Remote Browser Isolation



Low Risk



Known



Compromised or Out of Policy

Step Four

BLOCK

Block the request if previously determined as malicious or out of policy.

Step Four

ALLOW

Allow the request to be sent to the internet, un-isolated.

Customer Example: Higher Education POV

A mid-size community college, with approximately 3,000 faculty and staff members and around 70,000 students, wanted to enable users to be cyber smart when surfing the web. Despite years of security awareness training, they continued to see a high susceptibility to phishing attacks among their diverse population, with 20-30% susceptibility rates. Both faculty and students fell prey to scams designed to execute malware and harvest credentials. Furthermore, these cyber-attacks came through various channels, including work and personal email inboxes, social media sites, and messaging applications. As a result, the college needed to find a solution that would be effective and affordable while operating on a limited budget.

The community college turned to a comprehensive web protection solution that met their criteria. The solution provided protection across all delivery methods, required no additional user training, was easy to deploy, and seamlessly integrated with their existing security controls. Since implementing the solution, the college has experienced a 25% reduction in endpoint alerts, with no user complaints, demonstrating its effectiveness. Additionally, they now have increased visibility into credential harvesting sites targeting their users, allowing them to better protect their community from cyber threats. Although the deployment is still in its early stages, the results so far are promising, and the college is confident in its ability to safeguard its faculty, staff, and students from future phishing attacks.

Managed Service Providers

MSPs and MSSPs need solutions that are easily deployed, simple to manage and integrate with other security tools so they can maximize returns.

ConcealBrowse provides enterprise-grade security protection to small and medium businesses with simple, efficient deployment (in minutes) and a low-cost subscription model. With silent deployment, MSPs start benefiting from the value of ConcealBrowse in seconds. MSPs can use Conceal's integration engine to feed into SIEMs, TIPs, automation platforms, and other security operations solutions further extending the value of their investments. These two new features enable service partners to minimize the complexity of managing users in the platform.

For the MSP community, ConcealBrowse offers a tremendous opportunity to provide innovative solutions that address the top two cyber threats affecting small and midsize companies: ransomware and credential theft. A simple, drop-in solution, ConcealBrowse can be easily added to existing security packages or be a stand-alone solution for companies that lack protection, allowing them to instantly add a security control that may have seemed out of reach with their existing security budget.



About Conceal

Conceal is a fast-growing cybersecurity company that offers innovative technology solutions to our customers, globally. Each team member reflects our company's main goal: to protect the world from ever-growing cybercrimes.

Conceal enables organizations to protect users from malware and ransomware at the edge. The Conceal Platform uses Zero Trust isolation technology to defend against sophisticated cyber threats. Conceal is used by organizations of all sizes globally to ensure their users and IT operations remain secure, anonymous and isolated from attacks.

Disguise and protect your enterprise's online presence.

706-481-2642 | conceal.io | info@conceal.io

