

# Conceal & CrowdStrike: Closing the Browser Gap in Endpoint Security

It's a little-known fact that endpoint security solutions such as EDR and EPP lack visibility into browser activity necessary to detect phishing and credential theft. This is because browsers act as a sandbox in an attempt to reduce the risk of browser based threats escaping and reaching the OS. However this means that endpoint security tools such as EDR, lack visibility into browser activity and have to rely on network layer traffic inspection, such as DNS or HTTP to identify web threats.

In a landscape where cyber threats are increasingly sophisticated, ConcealBrowse takes a novel approach, deployed as an extension in the browser continuously assessing sites in real time to protect the user from advanced web-based attacks. Conceal's integration with CrowdStrike enables joint customers to close their browser gap, extending endpoint detection and response into the browser. This new integration automatically ingests malicious or suspicious domains detected by ConcealBrowse as indicators of compromise (IOCs) within the CrowdStrike Falcon® platform, unifying threat visibility in a single console.

## Why Customers Should Care

Adversaries use phishing as a technique to gain initial access to victim systems through credential theft or malicious code execution (see MITRE T-1566). According to a recent Deloitte study, 91% of cyberattacks initiate with phishing. These attacks are conducted via electronically delivered social engineering such as email and, more recently, messaging applications and social media. Regardless of the vector, a victim will click on a malicious link in an email or embedded in a file, which invokes a web browser to present a phishing page intended to steal credentials or execute malicious code. Phishing is also a common technique used for further attack execution and lateral movement (see MITRE T-1204 & T-1534) in the attack chain.



**Advanced Threat Protection:** Integrating ConcealBrowse with CrowdStrike Falcon EDR adds an unparalleled layer of web security, directly targeting threats at their most common entry point—the browser. By integrating ConcealBrowse with the Falcon platform, joint customers can unify web threat domains and custom IOCs in CrowdStrike's threat-centric command console for comprehensive threat context and visibility to accelerate detection, investigation and response to web-based threats such as phishing.



**Prevent Phishing Attacks:** ConcealBrowse offers unique visibility into browser activity, facilitating early detection of threats. Easily create detection events and enhance threat hunting with high confidence phishing IOCs from ConcealBrowse in Falcon, empowering your team to intervene in the kill chain before damage is done.



**Comprehensive Cybersecurity Solution:** The seamless integration of ConcealBrowse allows the ingestion of browser event data into CrowdStrike's platforms, enhancing the ability of Security Operations Centers (SOCs) to detect, respond to, and hunt web-based threats with enriched telemetry.

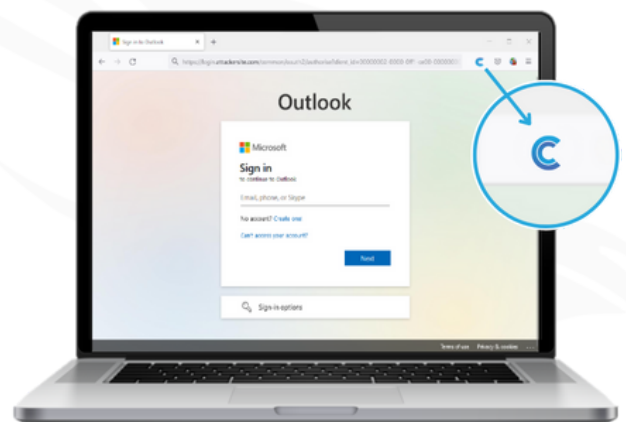
## Additional Value for CrowdStrike Users



**Streamlined Security Operations:** This integration offers a streamlined, lightweight solution that enriches CrowdStrike's security landscape without adding complexity, improving effectiveness and reducing time to value.

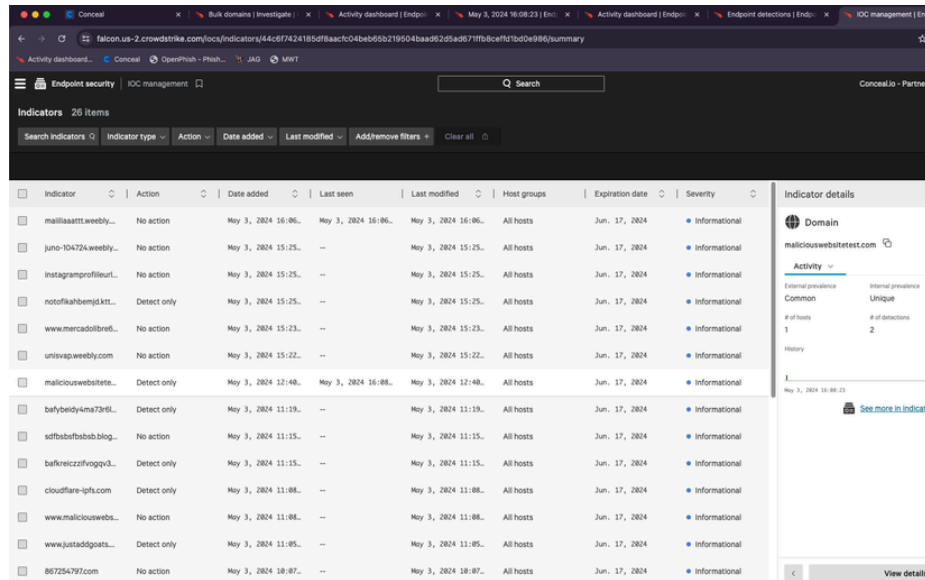


**Vendor-Maintained Integration:** Ease of maintenance through the partnership allows cybersecurity teams to concentrate more on strategic defense initiatives rather than managing the operational overhead of integration upkeep.



## How It Works

ConcealBrowse intervention event domains can be uploaded to Falcon as “Custom IOCs” for detection events or further investigation. When a host detects a Custom IOC (based on network activity), the Falcon console displays a detection in activity. Administrators can set thresholds for Falcon actions, such as detecting or not taking action, as well as a severity based on ConcealBrowse risk score or frequency of the intervention event. This enables real-time response and investigation of ConcealBrowse event indicators of compromise from within the Falcon platform during the critical window when the phishing campaign is still active.



Indicator	Action	Date added	Last seen	Last modified	Host groups	Expiration date	Severity
mailiaaattt.weebly...	No action	May 3, 2024 16:06...	May 3, 2024 16:06...	May 3, 2024 16:06...	All hosts	Jun. 17, 2024	Informational
juno-10472k.weebly...	No action	May 3, 2024 15:25...	--	May 3, 2024 15:25...	All hosts	Jun. 17, 2024	Informational
instagramprofileur...	No action	May 3, 2024 15:25...	--	May 3, 2024 15:25...	All hosts	Jun. 17, 2024	Informational
notofkahbemdjkt...	Detect only	May 3, 2024 15:25...	--	May 3, 2024 15:25...	All hosts	Jun. 17, 2024	Informational
www.mercadolibre6...	No action	May 3, 2024 15:23...	--	May 3, 2024 15:23...	All hosts	Jun. 17, 2024	Informational
unitvap.weebly.com	No action	May 3, 2024 15:22...	--	May 3, 2024 15:22...	All hosts	Jun. 17, 2024	Informational
maliciouswebtete...	Detect only	May 3, 2024 12:48...	May 3, 2024 16:08...	May 3, 2024 12:48...	All hosts	Jun. 17, 2024	Informational
bafybeidy4m473rd...	Detect only	May 3, 2024 11:19...	--	May 3, 2024 11:19...	All hosts	Jun. 17, 2024	Informational
sdfbafbfbbab.blog...	No action	May 3, 2024 11:15...	--	May 3, 2024 11:15...	All hosts	Jun. 17, 2024	Informational
bafkreiczifvogqv3...	Detect only	May 3, 2024 11:15...	--	May 3, 2024 11:15...	All hosts	Jun. 17, 2024	Informational
cloudflare-iplf.com	Detect only	May 3, 2024 11:08...	--	May 3, 2024 11:08...	All hosts	Jun. 17, 2024	Informational
www.maliciouswebs...	No action	May 3, 2024 11:08...	--	May 3, 2024 11:08...	All hosts	Jun. 17, 2024	Informational
www.justaddgoats...	Detect only	May 3, 2024 11:05...	--	May 3, 2024 11:05...	All hosts	Jun. 17, 2024	Informational
867254797.com	No action	May 3, 2024 10:07...	--	May 3, 2024 10:07...	All hosts	Jun. 17, 2024	Informational

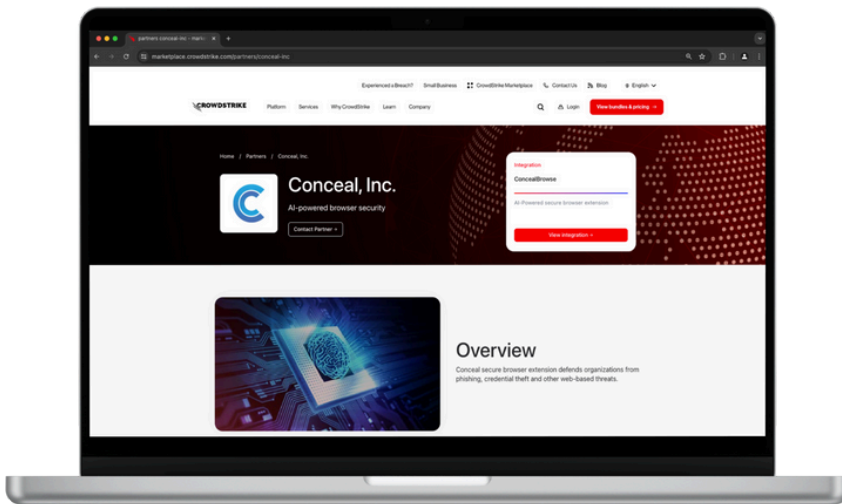
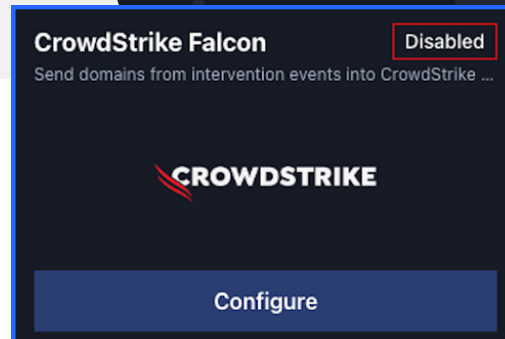
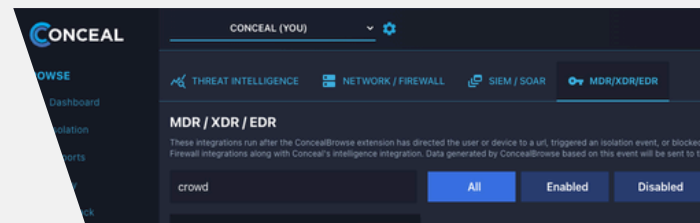
## Seamless Integration Process

The integration process is straightforward, ensuring your CrowdStrike Falcon platform can quickly and efficiently incorporate ConcealBrowse’s capabilities. Available as a plugin within the ConcealBrowse console, administrators can easily activate the integration with a CrowdStrike API token and straight forward configuration options.

## Try It Now

CrowdStrike customers can now try and buy ConcealBrowse in the [CrowdStrike Marketplace](#) to easily add integrated browser security.

The ConcealBrowse integration with the CrowdStrike Falcon platform is immediately available and can be enabled in the Conceal management console.



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

Copyright 2024 Conceal, Inc. All rights reserved.