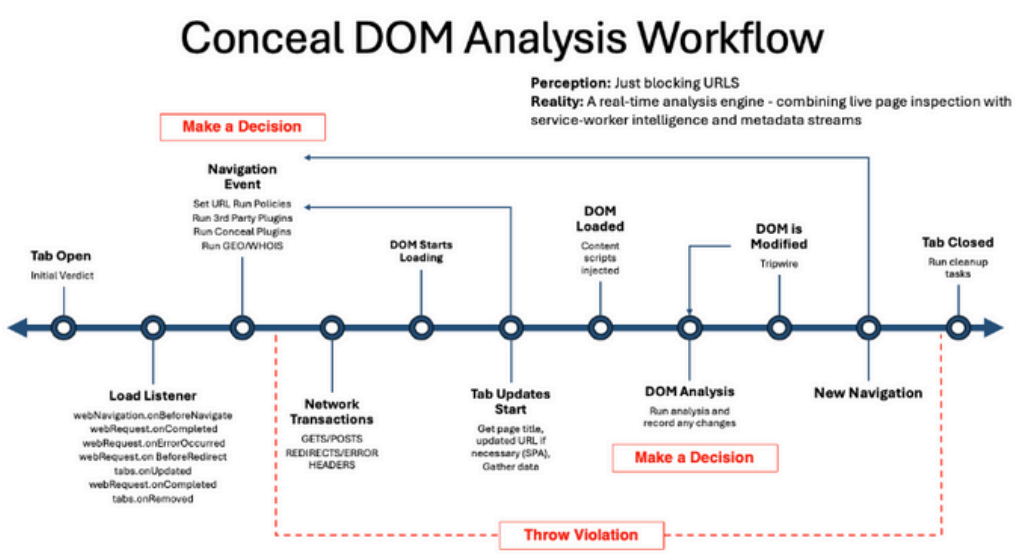
CONCEAL DATA SHEET

Capability Spotlight:
Conceal Document Object Model (DOM) Analysis

OVERVIEW

Traditional browsers are limited to blocking known URLs. Conceal goes further by delivering a live, context-aware analysis engine that uses DOM inspection, network metadata, and service worker intelligence to stop threats before they ever reach the endpoint.

The Conceal DOM Analysis Workflow reveals how Conceal delivers real-time, in-browser protection beyond simple URL blocking. While most solutions rely on static lists or proxies, Conceal actively inspects what's happening inside the browser, detecting and responding to threats as they unfold.



HOW IT WORKS

Tab Open/Initial Verdict:
When a new tab is opened, Conceal assesses the initial state and assigns a preliminary risk score.

Navigation Event Monitoring:
Conceal monitors all navigation events within the tab, tracking URL changes and redirects.

Network Transactions:
All network requests and responses are inspected for malicious content and anomalies.

DOM Loading and Updates:
As the DOM loads and updates, Conceal captures and analyzes changes to the page structure.

Real-Time Decision Engine:
The decision engine evaluates the risk score and determines the appropriate action, such as blocking the malicious script or terminating the tab.

Cleanup and Closeout:
When the tab is closed, Conceal performs a cleanup process to remove any residual threats.

THE BENEFITS

- **True Zero Trust in the Browser:** Every tab, every session, continuously verified.
- **Real-Time Threat Prevention:** Detects and stops emerging attacks as they occur.
- **Visibility & Control:** Full insight into browser activity for compliance and investigation.
- **No Added Complexity:** Works natively in the browser without proxies, VPNs, or traffic backhauling.

To learn more about how Conceal can change the way you deliver zero trust access and secure your browsers, visit www.conceal.io and schedule a demo today.