# Fortify Web Security For Better Detection and Response

SentinelOne & Conceal Joint Solution Brief

## Market Challenges

Web based threats are rapidly evolving with remote work continuing and a lack of network visibility. 91% of cyberattacks begin with phishing. [Resource: Deloitte]

The primary access point for an organization's SaaS applications is the web browser, with up to 75% of employee time spent in this environment. This high usage makes browsers a common target for phishing attacks, leading to credential theft and malware incidents. According to MITRE, phishing is a prevalent initial access vector (T1566), with 83% of businesses experiencing phishing attacks in 2021. [Resource: MITRE]

These attacks are becoming more sophisticated, with 9 new phishing domains registered every second and the use of generative AI to create convincing campaigns. Despite user awareness programs, click-through rates on phishing simulations remain at 2%-5%, emphasizing the need for additional security measures.

Organizations must leverage secure browsers to get real-time assessment of browsing activity to detect malicious or suspicious sites, even when traffic is encrypted, adding a crucial layer of security.

## Joint Solution

ConcealBrowse AI-powered secure browser provides a unique vantage point into browser activity critical to detect phishing, credential theft and other web based threats.

This integration enables SentinelOne Singularity Data Lake to ingest ConcealBrowse secure browser telemetry in real-time for enrichment and analytics. This provides improved detection, streamlined incident response and improved threat hunting through correlation of user browser security events with other security data sources within the organization.

Customers can now proactively monitor risky web activity and intervene earlier in the kill chain to disrupt cyber attacks.

## Solution Use Case

### Ingest telemetry data from ConcealBrowse into Singularity Data Lake

With the ConcealBrowse native post-processing data pipelines, you can configure seamless delivery of real-time browser security telemetry data into SentinelOne Singularity Data Lake. Singularity Data Lake will then automatically parse the JSON payload and make it available for searching, alerting and correlation.

## Joint Solution Highlights

**Visibility**

Seamlessly ingest ConcealBrowse telemetry into SentinelOne Singularity Data Lake

**Threat Detection**

Improve threat detection through enrichment and analytics in combination with other security data sources within Singularity Data Lake

**Accelerate Response**

Track back incidents to specific users and devices for faster remediation and improved mitigation actions

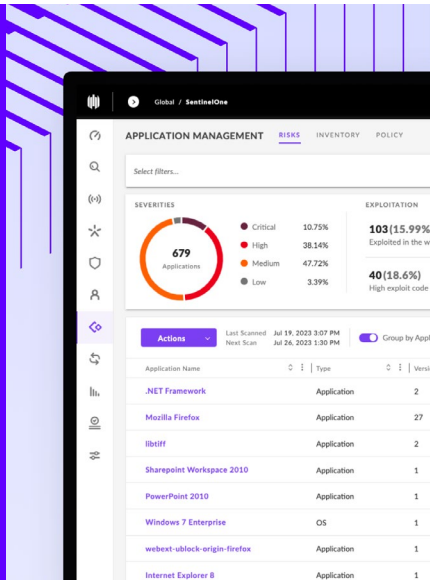
# How It Works

The following fields from ConcealBrowse is available through the integration:

- Event: Scanned URL
- Fields:
  - company_id [ConcealBrowse tenant identifier]
  - company_name [Tenant name]
  - count [number of times URL has been seen in company]
  - decision [detailed decision information used to calculate final_decision]
  - device_id [for device based deployments]
  - final_decision [allow|block|redirect|isolate]
  - url [URL scanned]
  - user_email [user based deployment only]
  - user_id [user based deployment only]

> “
>
> The integration of ConcealBrowse with SentinelOne marks a significant step in our mission to defend organizations against web-based threats. By securing the human element—the most vulnerable part of any organization—we aim to reduce the risk of destructive and costly cyber-attacks dramatically. Together with SentinelOne, we empower organizations to stay ahead of ever-evolving web threats.
>
> **Gordon Lawson**
> CEO OF CONCEAL






## Integration Benefits

+ Reduce risk of successful phishing or other web-based attacks which are typically initial access stage of most sophisticated cyber attacks
+ Improve security time-to-value with ConcealBrowse’s easy to deploy browser extension in combination with a validated and seamless integration to SentinelOne Singularity Data Lake
+ Improved ability for SOC to detect, respond, and hunt web-based threats by enriching Singularity Data Lake with ConcealBrowse secure browser extension telemetry and event data

## Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights™

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

About Conceal

Conceal’s mission is to defend organizations against web-based threats. ConcealBrowse is a lightweight and easily deployed AI-powered browser extension that protects users from ever-evolving phishing and other web threats. By securing the most vulnerable part of any organization, the human using a web-browser, ConcealBrowse dramatically reduces the risk of destructive and costly cyber-attacks.


sentinelone.com

sales@sentinelone.com
+1 855 868 3733