Conceal + EDR:

Enhancing EDR Capabilities with ConcealBrowse

ConcealBrowse exemplifies a user-centric approach to browser security, leveraging advanced, AI-powered features to ensure comprehensive protection against evolving cyber threats.

Benefits of EDR

Endpoint Detection and Response (EDR) solutions offer several key benefits:

- **Comprehensive Threat Visibility:** EDR provides deep visibility into endpoint activities, allowing organizations to detect and respond to threats in real-time.
- **Advanced Threat Detection:** Using behavioral analysis and machine learning, EDR identifies sophisticated threats that traditional antivirus software may miss.
- **Incident Response Capabilities:** EDR enables rapid response to security incidents, helping to contain and mitigate threats before they cause significant damage.
- **Compliance and Policy Enforcement:** EDR ensures endpoints comply with security policies and regulatory requirements, reducing compliance risks.
- **Integration with Security Ecosystem:** EDR integrates with SIEM and SOAR platforms, centralizing security management and enabling automated response to threats.

Benefits of ConcealBrowse

ConcealBrowse enhances an organization's cybersecurity posture and bolsters cyber tools like EDR Solutions with these features:

- **Enhanced Protection:** Analyzes site structure for attack patterns to detect phishing and mitigate social engineering attacks, surpassing traditional blocklist systems with AI-driven adaptability.
- **Sophisticated Phishing Detection:** Utilizes advanced AI to swiftly identify and counter new phishing tactics.
- **Privacy-Conscious:** Respects user privacy by avoiding unnecessary data retention, focusing solely on enhancing security.
- **Seamless Integration:** Integrates selective isolation to prevent workflow disruptions while educating users about web navigation risks.

Gaps of EDR

Despite its strengths, EDR solutions often have gaps that ConcealBrowse addresses:

Limited Browser Visibility: EDR focuses on endpoint activities but lacks detailed visibility into browser-specific threats like credential theft and malicious web scripts.

Browser-Based Attacks: EDR may not effectively detect and mitigate threats originating from browsers, such as phishing attacks and browser-based malware due to its limited visibility into the browser.

Credential Theft: EDR solutions often do not specialize in monitoring and detecting credential theft specifically from browser sessions, which can lead to undetected compromises.

User Awareness and Education: EDR solutions do not focus on educating users about cybersecurity best practices and the risks associated with cyber threats.

Integration Challenges: Integrating browser-specific threat data into existing EDR workflows can be challenging without dedicated browser security solutions like ConcealBrowse.

Browser Security with ConcealBrowse

ConcealBrowse elevates an organization's overall cybersecurity with browser based threat detection and mitigation and feeding the data to the rest of an organization’s tech stack, such as their EDR. It seamlessly complements EDRs like CrowdStrike and SentinelOne by addressing traditional EDR shortcomings and enhancing overall cybersecurity posture.

VALUE PROPOSITION

EDR Capabilities	Description	ConcealBrowse Additional Value
Endpoint Visibility	Provides visibility into endpoint activities and behaviors that may indicate threats.	✓ Extends visibility into browser-based threats on endpoints
Threat Detection & Response	Detects and responds to suspicious activities and potential threats on endpoints.	✓ Real-time monitoring of browser security threats for endpoints
Behavioral Analysis	Analyzes endpoint behavior to detect anomalies and potential threats.	✓ Detection and prevention of phishing credential theft attack patterns in the browser
Incident Response	Responds to security incidents with mitigation and remediation actions.	✓ More complete visibility into attack chain of events for swift response to browser-based threats
Malware Detection	Identifies and removes malware infections on endpoints.	✓ Advanced detection of malware sites within the browser
Compliance Monitoring	Ensures endpoints comply with security policies and regulations.	✓ Ensures browser-based activities comply with security policies
Forensic Investigation	Provides detailed analysis of endpoint activities for forensic purposes.	✓ Can provide details of suspicious web activity to the EDR for more thorough analysis
User Awareness and Education	-	✓ Educates users about safe browsing practices
Integration with SIEM/SOAR	Integrates with Security Information and Event Management (SIEM) or Security Orchestration, Automation, and Response (SOAR) systems for centralized management and automated response.	✓ Integrates browser security events with EDR as well as SIEM/SOAR platforms
Policy Enforcement	Enforces security policies across endpoints to maintain compliance and security posture.	✓ Enforces security policies specific to browser activities
Threat Intelligence Integration	Incorporates threat intelligence feeds to enhance threat detection and response capabilities.	✓ Augments EDR threat intelligence with browser-specific threat data

ConcealBrowse significantly enhances EDR capabilities by focusing on browser-specific threats and ensuring comprehensive protection against sophisticated cyber threats.

CONCEAL®

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