PROTEZIONE
AVANZATA DEL BROWSER
DOVE GLI ALTRI NON ARRIVANO

S3CUR3 BROWSER

Datasheet

Le aziende del Gruppo MEET IT

Via di Corticella, 89/2
40128 Bologna BO

+39 051 4070383
www.3cime.com | info@3cime.com

Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it

NAVIGA. PROTEGGI. AZIONA.

La tua attività si basa sul browser. Ma nessun sistema protegge il tuo browser in modo completo. S3cur3 Browser trasforma il tuo browser in un ambiente Enterprise, la prima linea di difesa proattiva contro le minacce web.

IL SERVIZIO

S3cur3 Browser è la soluzione di Browser Security con Architettura Browser-Native progettata per proteggere ciò che gli altri non possono. Il browser è diventato l'anello debole nelle architetture Zero Trust, considerando che oltre il 90% degli attacchi informatici inizia da una pagina web.
S3cur3 Browser è distribuito tramite una estensione per i browser più utilizzati, consentendo un'implementazione completa tipicamente in poche ore e senza la necessità di modifiche all'infrastruttura. L'Intelligence AI Proprietaria garantisce Visibilità Completa senza ricorrere a ispezioni SSL, VPN o Proxy, offrendo una **protezione diretta sul dispositivo dell'utente**.

VANTAGGI

PROTEZIONE PROATTIVA BASATA SU AI
Rileva e blocca le minacce in tempo reale, andando oltre le statiche threat intelligence o le liste di reputazione.

IMPLEMENTAZIONE LEGGERA E VELOCE
Fornito come estensione browser. Non sono necessarie modifiche infrastrutturali (Zero Infrastruttura) e il rollout completo è tipicamente questione di poche ore.

INTEGRAZIONE CON LO STACK DI SICUREZZA ESISTENTE
Invia log di sessione arricchiti e utilizzabili direttamente a piattaforme SIEM, XDR e MDR.

COMPLETA EDR, XDR, MDR SENZA SOVRAPPOSIZIONE
Protegge lo strato del browser, dove gli strumenti esistenti non hanno visibilità.

MASSIMIZZA GLI INVESTIMENTI DI SICUREZZA ESISTENTI
Aggiunge intelligence unica e dettagliata sulla sessione del browser per rafforzare le prestazioni degli strumenti di sicurezza attuali.

SERVIZI INTEGRATI PER UN'ADOZIONE SEMPLICE
Include servizi di Customer Success e servizi esperti all'interno della licenza per aiutare i team a ottenere il massimo da S3cur3 Browser, riducendo il carico di lavoro sul personale di sicurezza interno.

VISITA IL SITO *MEETIT.CLOUD*

LIVELLI DI PROTEZIONE

S3cur3 Browser offre tre strati di protezione attraverso una singola estensione, garantendo la sicurezza al punto più vulnerabile della tua rete: il browser.

AI BASED PROTECTION (PROTEZIONE IN TEMPO REALE)

Fornisce protezione AI at the Edge alla velocità del web. Utilizza un nuovo e all'avanguardia Anti-Phishing Engine proprietario basato su AI.

- **Anti-Phishing in Tempo Reale**: Blocca il phishing zero-day, il cybersquatting e il credential harvesting su domini non approvati utilizzando modelli AI e intelligence proprietaria sulle minacce.
- **Malvertising & Tracking Protection**: Elimina annunci invasivi, web tracker e cryptominer, riducendo al contempo il rumore nei log di sicurezza e il carico di lavoro nei sistemi SIEM e di rete.

CONTEXTUAL DLP (DLP CONTESTUALE)

S3cur3 Browser **DLP Contestuale** sfrutta l'AI e i Modelli Linguistici di Grande Dimensione (LLMs) per comprendere i dati nel loro contesto. Previene le fughe di dati bloccando o mascherando le informazioni sensibili prima che lascino il browser. Gli utenti ricevono una guida in tempo reale per distinguere ciò che può e non può essere condiviso. Ciò garantisce conformità, consapevolezza e protezione senza interrompere la produttività.

SESSION PROTECTION (PROTEZIONE DELLA SESSIONE)

Include le funzionalità di protezione della sessione. È il cruscotto di governance per monitorare, misurare e ridurre il rischio del browser, allineato con NIST 2.0.

- **Web Data Loss Prevention (DLP)**: Previene l'esfiltrazione di dati tramite operazioni di copia, incolla o caricamento, inclusi Dati Personali (PII) e corrispondenze con parole chiave/pattern, con modalità sia di audit che di blocco.
- **Business Credentials Protection (BCP)**: Agisce come l'ultimo miglio di difesa contro il phishing. Impedisce l'uso non autorizzato delle credenziali aziendali su app e domini non approvati.
- **Browser Extensions Protection**: Identifica e analizza le estensioni installate dagli utenti, valutando tratti dannosi, comportamento di esecuzione, permessi, vulnerabilità note nelle dipendenze, reputazione e presenza su store ufficiali.
- **Advanced Web Filtering**: Fornisce un filtraggio URL granulare senza ricorrere a VPN o ispezioni SSL, garantendo prestazioni e privacy dell'utente.
- **Browsing Risk Assessment**: Classifica il rischio di navigazione in tempo reale, con integrazione nativa SIEM/SOAR, e consente di controllare i rischi causati dal fattore umano.