

ENTERPRISE WEB SECURITY PRODUCT SUITE

AccessScope Deception Guard Honeypot Sentinel

可視化・欺瞞防御・攻撃者観測を、
独立した3製品で段階的に実装する。

AccessScope v2.2.4

Deception Guard v1.4.3

Honeypot Sentinel v1.1.2

WHAT IS HAPPENING?
IS IT HOSTILE?
WHAT WILL THE ATTACKER DO?

WordPress 向け | 独立運用 | Coexistence Mode 対応

Product Visualization / 実際の画面・表示項目は導入設定により異なります。



3 製品は「統合」ではなく「役割分担」で守る

同じデザイン体系を共有しながら、DB・設定・責務は独立維持。

Web アクセスを 見る → 判断する → 観測する

AccessScope

Access Intelligence & IP Control

WHAT IS HAPPENING?

- Traffic / IP / Geo / Security を可視化
- 同一 IP の反復アクセスを把握
- 手動 Block / Unblock、自動遮断設定

独立運用 / 共存可能

Deception Guard

Deception Detection & Response

IS IT HOSTILE?

- Sensitive 404 / Recon を検知
- Risk × Confidence × Campaign 分析
- Adaptive Decoy / Evidence / Response

独立運用 / 共存可能

Honeypot Sentinel

Pure Honeypot Observation

WHAT WILL THE ATTACKER DO?

- Fake Backup / Admin / DB / API
- Honey Token / Session / Timeline
- 観測主体。罠の中では即 Block しない

独立運用 / 共存可能

Coexistence Mode : Deception Guard と Honeypot Sentinel は Namespace / Signal だけで疎結合。AccessScope は独立した観測・制御基盤として並列運用。

AccessScope

See. Understand. Control. — アクセスの実態を見える化し、IP 単位で制御する。

「誰が・どれだけ・どこから」 アクセスしているかを把握。

- アクセス履歴・Traffic・Engagement・Network・Securityを一画面で確認
- 管理者権限で完全 IP を表示し、同一 IP の反復アクセスを集計
- Block / Unblock、一定回数超過の自動遮断を設定可能
- Geo Access、地域・流入・Journey データも既存機能として維持



VISIBILITY

IP History

Hits / 404 / First / Last

CONTROL

Block / Unblock

手動+閾値ベース

ANALYTICS

Traffic / Geo

24h / 7d / 30d

SECURITY

Telemetry

Repeat / 404 / Suspicious

企業利用ポイント：まず観測 → 反復 IP の傾向確認 → 手動遮断 → 必要に応じて自動遮断へ段階移行。

Deception Guard

攻撃者の探索意図を早期に見抜き、偽経路・Risk・Evidence へつなぐ。

罠を踏む「前」から、 Recon をセキュリティシグナル化。

- Sensitive 404 Intelligence： /db.sql / .env / wp-config backup 等の探索を分類
- Risk Score と Confidence を分離し、誤検知を抑えながら判断
- Adaptive Decoy、Campaign Analysis、Attack Stage で行動を相関
- Evidence Vault、Incident Bundle、任意の Cloudflare 連携に対応



DETECTION

Recon / 404

Bot / Login / Decoy

RISK & CONFIDENCE

Risk ≠ Confidence

危険度と確信度を分離

RESPONSE

Campaign / Evidence

Block / Cloudflare / ZIP

COEXISTENCE

Observation Zone

Honeypot 内は観測優先

本番 WordPress は守り、攻撃者には「別の世界」を見せる。攻撃者への反撃や第三者への能動アクセスは行わない。

Honeyplot Sentinel

Observe. Don't Block. — 偽環境へ入った攻撃者の行動を安全に観測する。

「触れてはいけない偽環境」を用意し、
接触そのものを観測シグナルに。

- Fake Backup / Fake Admin / Fake Database / Fake Internal API を仮想構築
- Honey Token と 30 分 Honeyplot Session で行動を追跡
- File Download / Authentication / DB Export 等を Severity 別に記録
- パスワード平文を保存せず、IP も原則 HMAC 匿名化して観測



FAKE BACKUP

Files / SQL / ZIP

download

FAKE ADMIN

Login Trap

authentication

FAKE DATABASE

Browse / Export

database

FAKE API

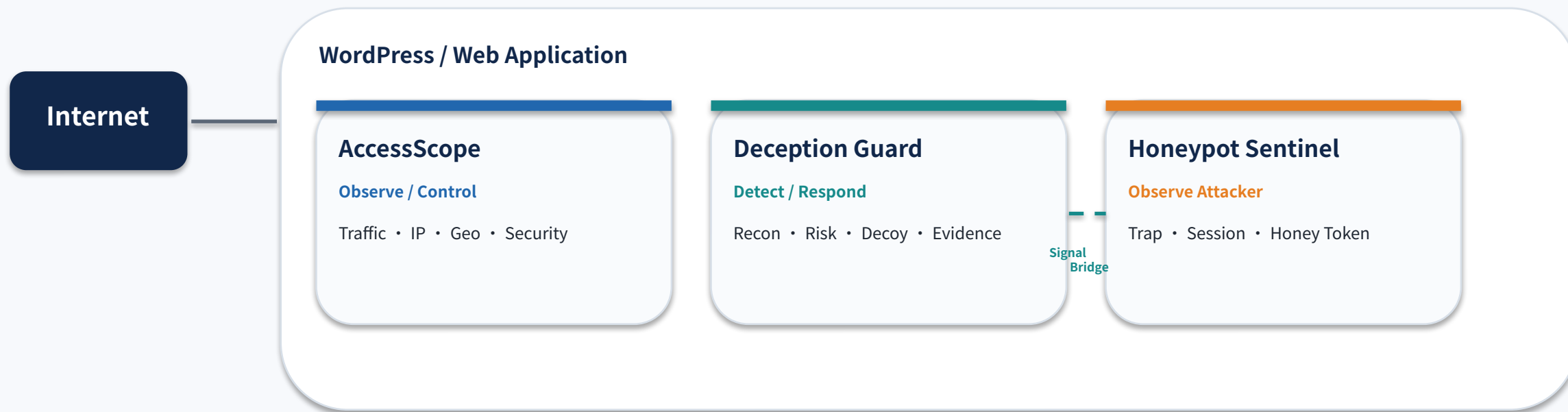
Internal API

api_access

観測が主目的。Honeyplot 内で即遮断せず、Session Timeline と Signal Bridge で「その後の行動」を理解する。

Coexistence Mode — 独立性を維持したまま連携

直接依存ではなく、役割ごとの並列運用と必要最小限の Signal 連携。



独立性契約

DB 共有なし

各製品のイベント・設定を分離

直接 include なし

片方停止でも他方は動作

Clinical Event 混入なし

攻撃ログを業務データへ混ぜない

Cloudflare 主体を整理

遠隔遮断は競合しない構成へ

Honeypot Observation Zone では観測を優先。本番領域へ戻った攻撃行動には Deception Guard の通常防御を適用。

3 製品を、いきなり「全自動防御」にしない。

観測 → 評価 → 手動制御 → 段階的自動化の順で導入します。

- 01 OBSERVE** AccessScope で Traffic ・ IP ・ 404 ・ 反復アクセスを可視化
- 02 DETECT** Deception Guard で Recon ・ Risk ・ Confidence を評価
- 03 LEARN** Honeypot Sentinel で攻撃者の行動を観測
- 04 CONTROL** 手動 Block / Unblock で運用ルールを確立
- 05 AUTOMATE** 実測に基づき閾値 ・ Cloudflare ・ 自動遮断を段階適用

Independent by design. Connected when needed.