RILEVAMENTO E RISPOSTA
AVANZATA PER APPLICAZIONI WEB E API

WAF DeepSight

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

VISIBILITÀ, RILEVAMENTO,RISPOSTA INTELLIGENTE.

Massima Visibilità a Runtime, Rilevamento Avanzato e Risposta Intelligente. La sicurezza delle tue Applicazioni Web e API potenziata oltre il WAF.

IL SERVIZIO

WAF DeepSight è la prima soluzione europea **ADR** (Application Detection & Response) progettata per proteggere Web Application e API con un controllo profondo e continuo, superando i limiti dei tradizionali WAF.
La tecnologia analizza il traffico applicativo in runtime, rileva comportamenti anomali, individua sequenze sospette e attiva risposte automatiche a livello L3 e L7 senza impatti sui servizi monitorati. Completamente containerizzato, scalabile e ottimizzato per **SOC** e **MSSP**, fornisce una protezione evoluta, automatizzata e adatta agli ambienti moderni ad alto dinamismo.

COSA FA?

AppVision introduce la Detection & Response direttamente a livello applicativo, offrendo:

- Monitoraggio profondo e continuo del traffico HTTP/HTTPS
- Rilevamento comportamentale tramite analisi di sequenze e anomalie
- Identificazione di attacchi anche in assenza di vulnerabilità note
- Protezione avanzata contro scraping, bot, exploit, attacchi automatizzati
- Visibilità totale sui flussi applicativi, anche in caso di bypass del WAF
- Automazione delle risposte tramite tecniche intelligenti e policy personalizzabili
- Integrazione immediata con firewall, WAF, ADC e SIEM

Rispetto a un WAF tradizionale, non si limita a bloccare richieste sospette: **comprende il comportamento del client** nel tempo e **reagisce** in modo contestuale, dinamico e affidabile.

VISITA IL SITO *MEETIT.CLOUD*

COME AGISCE?

WAF DeepSight utilizza un approccio multi-livello:

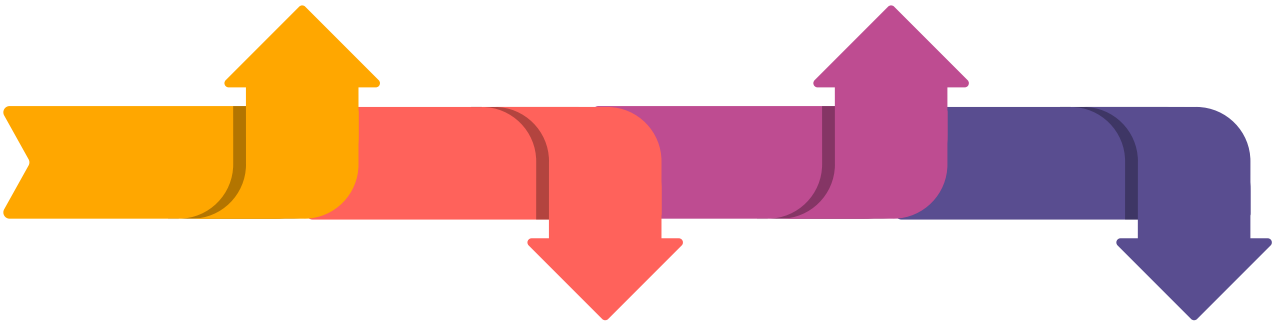
1. ANALISI IN PROFONDITÀ (RUNTIME)
Raccoglie dati da web server, reverse proxy e ADC, osservando realmente ciò che l'applicazione riceve.

2. RILEVAMENTO INTELLIGENTE
Combina:

- analisi comportamentale
- correlazione temporale
- detection delle sequenze
- motori dedicati per bot management e attacchi applicativi
- threat intelligence aggiornata

3. RISPOSTA AUTOMATICA
Applica contromisure tramite tecnologie esistenti:

- Block L3 (IP/Net)
- Block L7 (request / domain)
- Enforcement selettivo per tipo di attacco



4. REPORTING AVANZATO
Dashboard in tempo reale, report automatici, esportazioni personalizzate e integrazione SIEM.

INSTALLAZIONE

Completamente containerizzato
Deploy da Dockerhub o Quay.io, senza downtime.

Modalità offline o integrata
Perfetto anche in contesti complessi con riscrittura del traffico.
Sentinel + Engine

- *Sentinel*: leggero, analizza log e traffico in edge
- *Engine*: esegue correlazioni, interfaccia GUI e orchestrazione

VISITA IL SITO *MEETIT.CLOUD*

CARATTERISTICHE

Caratteristica	WAF Tradizionale	WAF DeepSight
Visibilità applicativa	Limitata	Totale (runtime)
Detection	Regole statiche	Comportamentale + sequenze
Deployment	Invasivo	Non invasivo
Scalabilità	Complessa	Nativa, containerizzata
Risposta	Limitata	Automatica, L3 & L7
Bypass	Vulnerabile	Visibilità anche in caso di bypass
Utilizzo per SOC/MSSP	Limitato	Ottimizzato

VANTAGGI DISTINTIVI

VISIBILITÀ A RUNTIME NON-PERIMETRALE
Opera tramite log server e reverse proxy, garantendo una prospettiva applicativa profonda (DeepSight) impossibile da ottenere con un WAF inline o SaaS.

AI COMPORTAMENTALE E ANALISI DI SESSIONE
Sfrutta Modelli Comportamentali e AI per analizzare sequenze di richieste e pattern complessi, superando le logiche a regole fisse.

INTEGRAZIONE AGENTLESS E NON INVASIVA
Nessuna modifica infrastrutturale: sfrutta componenti già presenti (NGINX, Apache, WAF, SIEM, ecc.) per una messa in opera immediata.

DOPPIO RUOLO: VISIBILITÀ E DIFESA
Può essere utilizzato come prima linea di visibilità e intelligence o come ultima linea di difesa, bloccando attacchi in autonomia.

PERFETTO PER SOC E MSSP (ARCHITETTURA DISTRIBUITA)
Architettura containerizzata (Elixir/Rust) resiliente, modulare e scalabile per ambienti Enterprise, MSSP e grandi SOC.

RISPOSTA AUTOMATIZZATA E COORDINATA
Blocca gli attacchi in autonomia (enforcement) e supporta automazioni e report completamente personalizzabili (integrazione SOAR/SIEM).

PRIMA SOLUZIONE ADR EUROPEA WEB & API
Soluzione sviluppata interamente in Europa, con compatibilità certificata per i principali componenti come NGINX+.

CONCLUSIONI

WAF DeepSight è la **risposta** moderna **ai limiti dei WAF**: una soluzione che vede, comprende e risponde realmente agli attacchi contro Web Application e API, integrandosi nei SOC e potenziando le operazioni di difesa senza impattare sui servizi.

VISITA IL SITO *MEETIT.CLOUD*