



THREAT INTELLIGENCE GEOSPAZIALE · LOCAL-FIRST

Vedere chi attacca la tua infrastruttura.

Una mappa sola per la rete, le minacce e le fonti aperte.
I dati sensibili non lasciano la tua rete.

Lowegate Studio

Documento di presentazione · settembre 2026

facelive.net/orioneye

IN UNA FRASE

Tutto quello che succede alla tua rete, su una mappa sola.

OrionEye raccoglie su un'unica mappa interattiva ciò che oggi è sparso fra registri, portali e fogli di calcolo: chi bussa ai tuoi server, da quale rete arriva, che reputazione ha, e cosa sta succedendo intorno a quel punto del mondo. Poi ti lascia agire, senza cambiare schermata.

La differenza che conta

La maggior parte degli strumenti di sicurezza chiede di mandare i propri dati nel cloud di qualcun altro. OrionEye è costruito al contrario: con i piani professionali l'analisi resta sulla macchina di chi la fa, e nelle installazioni aziendali non esce nemmeno dalla rete interna. È una scelta di architettura, non un'opzione da attivare.



La vista operativa. A sinistra l'analisi dell'area selezionata, a destra il racconto dell'incidente in corso, sotto la sintesi. Immagine ripresa dalla demo pubblica, con dati dimostrativi.

IL PROBLEMA

Cinque schede aperte e un foglio di calcolo

Chi indaga su un indirizzo sospetto apre oggi cinque portali diversi: uno per le porte esposte, uno per i certificati, uno per la reputazione, uno per capire di chi è la rete. Poi ricopia a mano quello che ha trovato.

Il lavoro vero non è la ricerca: è la ricucitura. Ed è proprio la ricucitura che si perde, perché non finisce da nessuna parte. Il giorno dopo, con lo stesso indirizzo davanti, si ricomincia.

Nel frattempo i tentativi di intrusione restano dove sono sempre stati: in un file di registro che cresce, che nessuno legge, e che si guarda solo quando è tardi.

La risposta di OrionEye

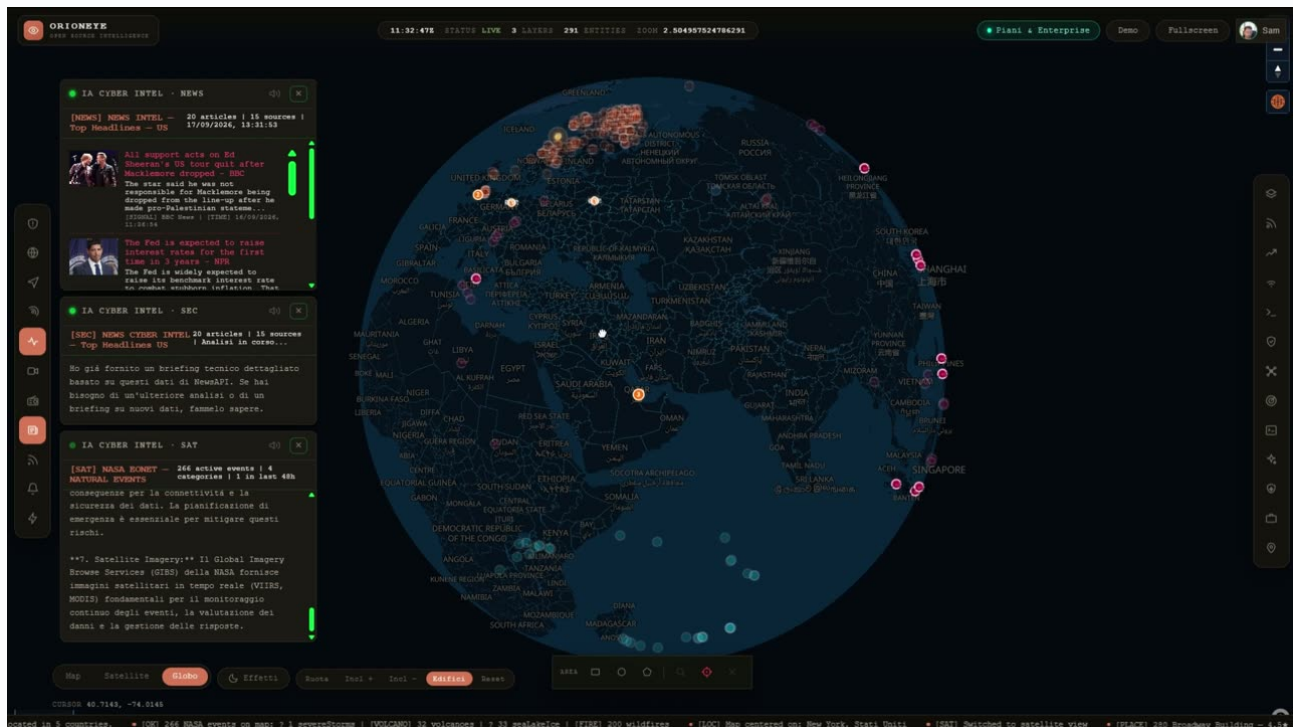
01	Rileva	I tentativi di accesso falliti arrivano sui tuoi server. OrionEye li mette sulla mappa nel momento in cui compaiono, invece di lasciarli in un registro che nessuno legge.
02	Indaga	Un indirizzo ostile, aperto: da dove viene, di chi è la rete, che reputazione ha, cosa tiene esposto. Tutto affiancato sulla stessa mappa.
03	Correla	Gli indirizzi sparsi smettono di essere sparsi: diventano una campagna coordinata, con un punteggio di affidabilità. Si risponde a una campagna, non a duecento righe separate.
04	Rispondi	Blocchi l'intera campagna sui tuoi server, la segnali agli archivi pubblici, condividi la scoperta con gli altri analisti.

LA MAPPA

La stessa scena, da ogni angolazione

Mappa piatta, immagini satellitari, rilievo del terreno o globo tridimensionale: sono modi di guardare, non strumenti diversi. Tutto ciò che hai acceso resta acceso quando cambi vista, e ogni elemento resta cliccabile.

È una differenza pratica: significa che non devi scegliere fra vedere il contesto geografico e vedere i tuoi dati. Li vedi insieme.



Il globo tridimensionale, con i riquadri di analisi aperti sulla sinistra. Gli stessi elementi della mappa piatta, nella stessa sessione.

LE FONTI

Oltre venti sorgenti, accese e spente come interruttori

Infrastrutture malevole note, sonde di rete internazionali, telecamere pubbliche, eventi naturali, lanci spaziali, voli, stazioni radio, notizie. Ogni sorgente è un interruttore: si accende quando serve e si spegne quando è rumore.

Non è accumulo: è contesto. Un indirizzo che bussa da una città rimasta al buio da sei ore è una storia diversa da uno che bussa da un centro dati tranquillo.



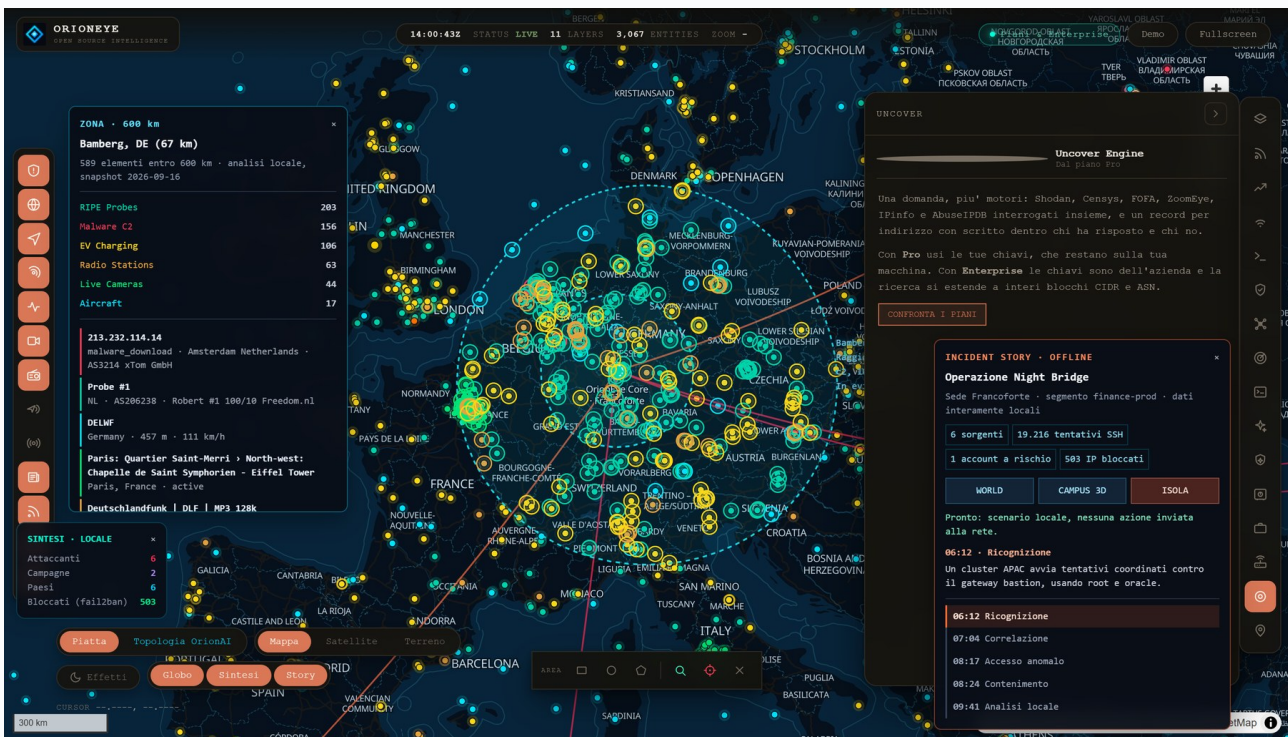
Il pannello delle sorgenti: ciascuna con la sua origine dichiarata e il suo interruttore.

RICERCA MULTI-MOTORE

Uncover Engine: una domanda, sei motori

Invece di rifare la stessa ricerca su cinque piattaforme e ricucire le risposte a mano, la domanda si fa una volta sola. OrionEye la manda insieme ai principali motori di ricognizione pubblici e restituisce **una scheda per indirizzo**: porte esposte, software e versione, nomi di dominio, rete di appartenenza, reputazione.

La scheda porta con sé **da dove viene ogni informazione**. Si vede quali motori hanno confermato un dato e quali non hanno risposto affatto — perché tre motori che concordano non sono lo stesso fatto di uno che tira a indovinare. Nessun dato viene dedotto: una vulnerabilità compare solo dove un motore la dichiara.



Il modulo Uncover nella console. Con il piano Pro le chiavi dei motori restano sulla macchina dell'operatore; con Enterprise sono gestite dall'azienda.

IL CO-PILOTA

Orion IA: sorveglianza, e spiega

Orion IA guarda chi entra nel tuo account e da dove: un dispositivo mai visto, un paese nuovo, due accessi troppo lontani per essere la stessa persona, una raffica di tentativi. Quando trova qualcosa, te lo racconta in italiano, non con un codice di errore.

Perché l'intelligenza artificiale qui non decide

Il rilevamento è fatto da regole precise, sempre uguali; l'intelligenza artificiale scrive soltanto la spiegazione. È una scelta: un allarme di sicurezza che non si riesce a riprodurre non si riesce nemmeno a smentire. E se nessun modello è raggiungibile, l'agente continua a funzionare — i rilevamenti ci sono tutti.

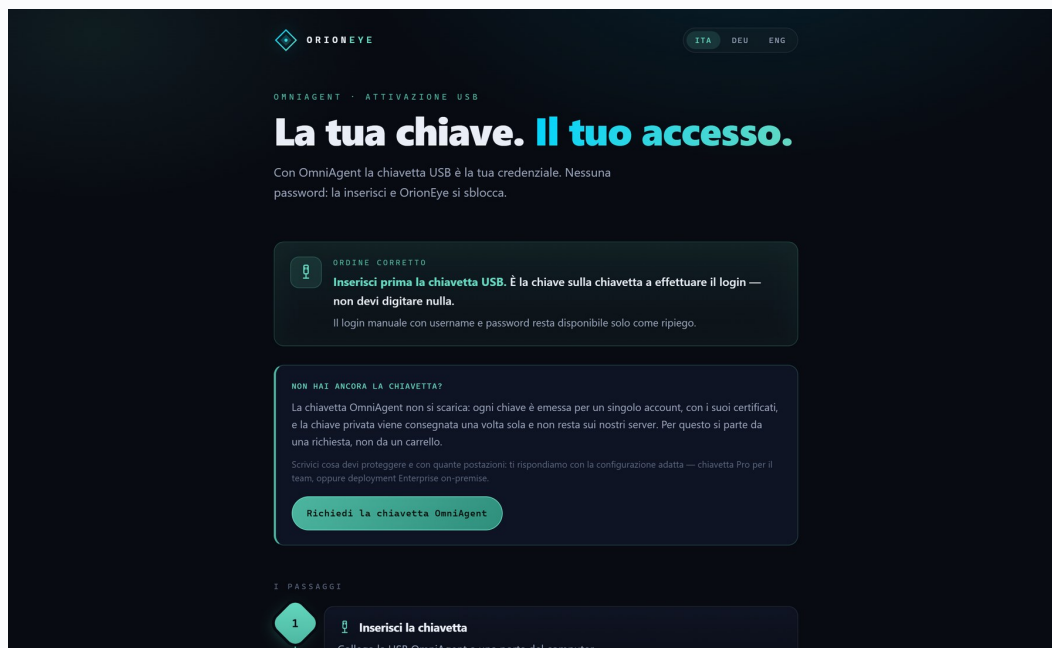
Alla console si parla in linguaggio naturale. Si chiede di mostrare una rete, di confrontare due ipotesi, di preparare un rapporto: gli strumenti li sceglie lei, e nelle installazioni aziendali il modello può girare dentro l'azienda, senza che una sola riga esca.

ACCESSO

La chiavetta al posto della password

Con il piano Pro la credenziale è una chiavetta USB. La si inserisce e OrionEye si apre: niente password da ricordare, niente password da rubare. Dentro c'è anche una cassaforte cifrata che vive sulla macchina dell'operatore, non sui nostri server.

Ogni chiavetta è emessa per un singolo account, con certificati suoi. La chiave privata viene consegnata una volta sola e non resta da noi: se la perdessimo non potremmo restituirla, ed è esattamente il punto.



La guida di attivazione, disponibile in italiano, inglese e tedesco.

I PIANI

Tre livelli, e ognuno è un verbo

Non tre listini: tre posture. Si **esplora** ciò che è pubblico, si **indaga** ciò che è proprio, si **difende** ciò che è in produzione.

	Free · Explore	Pro · Investigate	Enterprise · Defend
A chi serve	Chi vuole guardare	Analisti e PMI	Infrastrutture critiche
Come si accede	Email e password	Chiavetta USB, senza password	Licenza firmata
Dove vivono i dati	Cloud	Cassaforte cifrata in locale	Infrastruttura del cliente
Mappa e fonti aperte	Sì	Sì, avanzata	Sì, avanzata
Ricerca multi-motore	—	Fino a 5 motori, con le tue chiavi	Senza limite, chiavi aziendali
Ricognizione su intere reti	—	—	Blocchi e reti per intero
Topologia e cassaforte USB	—	Sì	Sì
Orion IA, il co-pilota	—	Sì, con modelli in cloud	Sì, con modelli in locale
Telemetria della rete interna	—	—	Sì (SentraLink)
Funziona senza Internet	—	In parte	Sì, air-gapped

La chiavetta porta il piano Pro sulla postazione in cui è inserita, anche partendo da un account gratuito: vale finché resta inserita.

RISERVATEZZA

Dove vivono i dati

È la domanda che un responsabile della sicurezza fa per prima, e merita una risposta precisa invece di una rassicurazione.

Con il piano gratuito si guardano fonti pubbliche, e i dati stanno sul nostro server come in qualunque servizio online.

Con il piano Pro la parte che riguarda la tua infrastruttura vive sulla tua macchina: la cassaforte sulla chiavetta, il programma che legge i tuoi server, le chiavi dei motori di ricerca. Noi non le conserviamo.

Con il piano Enterprise nulla lascia l'azienda: la telemetria della rete interna si legge da dentro il perimetro, i modelli di intelligenza artificiale girano su hardware vostro, e l'installazione funziona anche su reti isolate da Internet.

In pratica

Più il dato è sensibile, meno si muove. È il contrario di come funziona quasi tutto il resto del mercato, ed è la ragione per cui questo prodotto esiste.

COME SI COMINCIA

Tre passi, e il primo non costa nulla

Uno. Apri la demo pubblica e guarda la piattaforma in funzione, con dati dimostrativi, senza registrarti: facelive.net/orioneye

Due. Raccontaci cosa devi proteggere e su quante postazioni. Ti rispondiamo con la configurazione adatta — chiavetta Pro per il gruppo di lavoro, oppure installazione Enterprise dentro la vostra infrastruttura.

Tre. Una sessione tecnica insieme, sui vostri dati veri, prima di qualunque decisione.

Per parlarne

facelive.net/orioneye/landing/piani.html — sezione Contatti.

Indica «Pro (OmniAgent USB)» oppure «Enterprise» nel modulo, così la risposta arriva già mirata sul vostro scenario.

Le schermate di questo documento sono riprese dalla demo pubblica di OrionEye con dati dimostrativi, senza ritocchi.