

# La prospettiva degli hacker

L'hacking agentico identifica, convalida e assegna priorità alle esposizioni prima che gli avversari colpiscano. Con Hadrian, l'IA agentica è in grado di individuare e mitigare in modo proattivo i problemi OWASP Top Ten, le vulnerabilità zero-day e note e le configurazioni errate su tutta la superficie di attacco esterna.

Anticipa gli avversari e previeni le violazioni prima che possano sferrare un attacco. Hadrian ti aiuta a passare da un approccio alla sicurezza informatica reattivo a uno proattivo, automatizzando la gestione della superficie di attacco, la convalida e la gestione dell'esposizione alle minacce.

Hadrian monitora continuamente l'intera infrastruttura digitale, aumentando la scalabilità per individuare le vulnerabilità in ambienti on-premise e cloud, fornendo al contempo approfondimenti sulla sicurezza in tempo reale. L'automazione fa sì che i team di sicurezza possano concentrarsi sui rischi a più alta priorità, prevenendo potenziali violazioni e rafforzando la postura di sicurezza sull'intera superficie di attacco.

## Cosa contraddistingue Hadrian

### ■ Sempre attivo

A differenza dei test tradizionali che avvengono periodicamente, Hadrian funziona 24 ore su 24, 7 giorni su 7, garantendo visibilità in tempo reale e protezione dalle minacce emergenti.

### ■ Precisione elevata

Hadrian elimina i problemi convalidando le esposizioni con test avversariali guidati dall'IA, in modo che i team di sicurezza agiscano solo sui rischi reali e sfruttabili.

### ■ Distribuzione immediata

Hadrian non richiede alcuna configurazione o manutenzione, e fornisce informazioni istantanee sulla superficie di attacco per le minacce più recenti senza aggiungere oneri operativi.

## Principali vantaggi



### Rilevamento degli asset

Ottieni informazioni in tempo reale sugli asset grazie alla reconnaissance e alla contestualizzazione automatizzate. L'inventario degli asset di Hadrian consente ai clienti di risparmiare in media oltre 10 ore alla settimana.



### Rivelazione delle esposizioni

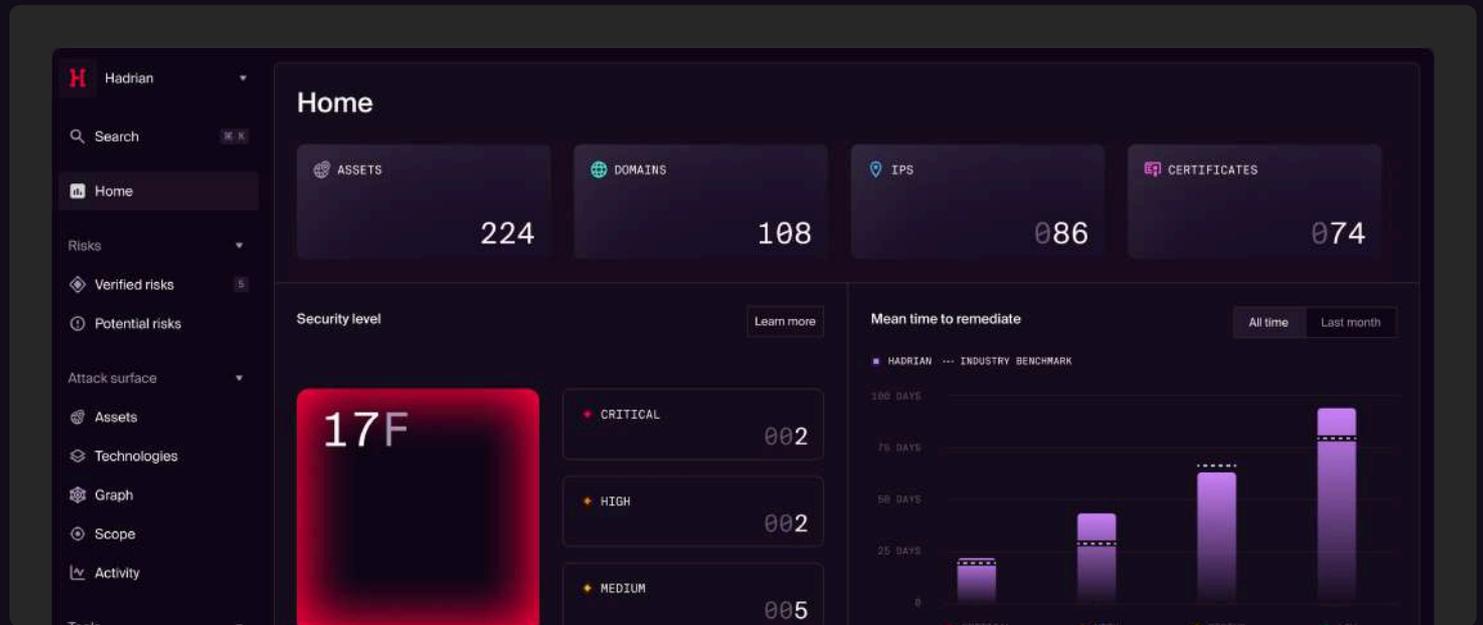
Ottieni una visibilità 10 volte superiore dei rischi critici con valutazioni approfondite. L'architettura modulare di Hadrian per la valutazione delle minacce riproduce le tecniche e i comportamenti degli hacker nel mondo reale.



### Risoluzione dei problemi

Riduci l'MTTR dell'80% con flussi di lavoro semplificati e integrazioni flessibili. Hadrian fornisce istruzioni di riparazione passo per passo e una suite di strumenti di collaborazione per accelerare la risoluzione dei problemi.

# Piattaforma di sicurezza offensiva di Hadrian



## 🌐 Prospettiva esterna

Hadrian esegue una scansione continua della superficie di attacco esterna, identificando le esposizioni proprio come farebbe un aggressore.

## 🔍 Architettura basata sugli eventi

Hadrian risponde ai cambiamenti dell'ambiente in tempo reale, garantendo il rilevamento delle minacce nel momento in cui queste emergono.

## ⚙️ Distribuzione zero-touch

Hadrian non richiede l'installazione o la configurazione di agenti e fornisce una visibilità immediata della superficie di attacco.

## 🌟 Test guidati dall'IA

I test automatizzati basati sull'IA simulano le tecniche di attacco del mondo reale per scoprire le vulnerabilità con precisione.

## 📈 Priorità basate sul contesto

Il punteggio di rischio intelligente aiuta i team a concentrarsi sulle vulnerabilità più critiche in base alla sfruttabilità reale.

## ⚙️ Integrazione perfetta

Si integra facilmente con i flussi di lavoro di sicurezza esistenti, migliorando le difese senza aggiungere complessità.

## Il migliore in assoluto

La sicurezza offensiva di Hadrian rivela il modo in cui gli attacchi del mondo reale potrebbero compromettere applicazioni e infrastrutture. La nostra piattaforma autonoma esegue continuamente test per valutare in modo completo gli asset presenti su Internet. La tecnologia agentless basata sul cloud viene costantemente aggiornata e migliorata dal team di hacker etici di Hadrian.

FROST & SULLIVAN  
**BEST PRACTICES**  
AWARDS

Gartner. 4.9/5 ★  
Peer Insights™

