

ATTACK SURFACE MANAGEMENT • DIGITAL RISK PROTECTION • AGENTIC TESTING

Know which exposures attackers can **actually exploit**.



DarkSense runs a continuous offensive security program across your perimeter and brand — discovering exposures, validating what's truly exploitable with AI agents, and mobilizing the remediation.

THE PROBLEM — ATTACKERS MOVED TO MACHINE SPEED

AI has industrialized offense: Vulnerabilities are weaponized before patches ship and stolen credentials are abused within minutes — while most organizations still rely on annual point-in-time pentests and noisy scanners that can't tell exploitable from theoretical.

\$4.44M

Average cost of a data breach — \$10.22M in the US
IBM • 2025

31%

Of breaches now start with vulnerability exploitation
VERIZON DBIR

69%

Of orgs attacked via unknown or unmanaged internet-facing assets
ESG RESEARCH

–7 days

Mean time-to-exploit — flaws weaponized before the patch exists
MANDIANT M-TRENDS

One platform. The full offensive loop, continuously.

DarkSense **discovers** everything you expose to the internet, **validates** what's genuinely exploitable with evidence-backed AI testing, and **mobilizes** the fixes and takedowns that matter — around the clock, with no agents to install.



PLATFORM CAPABILITIES



Infrastructure Perimeter Testing EXTERNAL SURFACE • EASM

- Continuous discovery of domains, hosts, services and certs
- Port and service fingerprinting with exposure validation
- Change detection alerts when your surface shifts
- Live attack-surface graph of your entire perimeter



Web DAST with AI Login AUTHENTICATED APP TESTING

- AI agent logs in like a human — forms, flows & MFA
- Scans behind login with session keep alive & re-auth
- Multi-role access control testing
- Captured evidence on every finding — proof, not noise



Digital Risk Protection BRAND & IDENTITY THREATS

- Typosquat & lookalike domains — 13 detection algorithms
- Leaked credentials from stealer legs & breach dumps
- Brand & executive impersonation watch across social media
- Built-in takedown workflow with evidence bundles



Fully Agentic & Programmatic Testing THE BYTESIEGE ENGINE

- Coordinated AI specialists — recon, web, intra, OSINT
- Programmatic, hybrid, and fully agentic execution
- Approval gates & enforced scope • you stay in control
- Full audit trail of every agent decision & tool call

AGENTLESS
Nothing to install — connect a domain and go

MINUTES
From sign-up to initial validated results

CONTINUOUS
The full loop runs around the clock

AUDIT-READY
Evidence on every finding, every action logged

Validate your exposures **before attackers do**.

www.arancia.io
REQUEST A DEMO