THE MSSP PLATFORM PLAY

One Platform. Five Products. Zero Tool Sprawl.

Breacher.ai is built for the way MSSPs sell and the way enterprise red teams operate. One multilingual platform: deepfake red team, awareness training, tabletop exercises, identity-verification pen testing, and breach & attack simulation. Run it across every client. Stop paying five vendors to do one job.

Multilingual | Multi-Tenant | White-Label Ready | Set-and-Forget | One Contract | One Dashboard

Book a 30-Minute Briefing

No deck. Straight to a practitioner.

BUILT AROUND HOW YOU DELIVER

Tool Sprawl Is Killing Your Margin

You run a security practice. The budget and the authority sit with you. The time does not.

Your stack is bloated. One vendor for phishing simulation. Another for awareness training. A third for tabletops. A fourth for pen testing. A fifth for breach and attack simulation. Five contracts. Five dashboards. Five renewals. Five integrations your team babysits instead of billing.

Most of those tools were built for a single enterprise to run on itself. They were never built for an MSSP to run across fifty clients in twelve languages from one console. So you absorb the overhead. Sprawl burns margin. It burns analyst hours. It burns the client experience.

And it leaves a gap nobody is covering: synthetic media. Voice clones and video deepfakes walk past every tool on that list.

> **Breacher.ai was built the other way around. Multi-tenant, multilingual, white-label ready. One platform that collapses five buying motions into one delivery motion.**

FIVE PRODUCTS. ONE BUYING MOTION.

Lead With The Differentiator. Cross-Sell The Rest.

1 LEAD DIFFERENTIATOR + 4 CROSS-SELLS = 1 UNIFIED PLATFORM

One platform. Every buying motion.

The deepfake red team opens the door. The other four sell themselves off that first report. Nobody else runs all five from a single console.

01

LEAD / DIFFERENTIATOR

Red Team + Deepfake Simulations

This is the wedge. Nobody else runs it at MSSP scale.

DEEPFAKE RED TEAM uses our OSES™ methodology to attack your client the way a real adversary does in 2026. Cloned voices. Synthetic video. Believable personas at scale. Not a fake login page. A fake CFO on a call. You walk into the renewal with proof nobody else can produce, and that report opens every cross-sell below.

- Voice cloning, deepfake video, synthetic persona campaigns
- OSES™ click, action, and vulnerability scoring per target
- Multilingual payloads for global client footprints
- Practitioner-built reports you can hand straight to the board

02

Awareness Training

Train against the exact attack you just ran.

The red team shows the gap. Training closes it. Same platform, same data, same dashboard. Your client sees the simulation result and the remediation in one place, so next quarter's numbers move.

- Content mapped to the real deepfake scenarios that landed
- Multilingual delivery for every region a client operates in
- Closed-loop reporting from simulation to behavior change

FIVE PRODUCTS. ONE BUYING MOTION. (CONT.)

Deepen The Account. Lock The Renewal.

03 Tabletop Exercise

Put the deepfake incident in front of the executives.

Facilitated scenarios built around synthetic-media attacks. Walk leadership through a cloned-voice wire fraud or a deepfake impersonation of the CEO before it happens for real. This is the engagement that gets you in the room with the buyer above your buyer.

- ✓ Executive and IR-team scenarios grounded in real attack data
- ✓ Deepfake incident response playbook stress-tested live
- ✓ Findings feed back into training and red team scope

04 Identity Verification & KYC Pen Test

Deepfakes break onboarding. Test it before the fraud team finds out.

We attack the KYC and identity-verification flow with synthetic faces, voices, and documents. Liveness checks, video selfie verification, voice biometrics. If a deepfake can pass your client's onboarding, that is a finding worth a contract.

- ✓ Synthetic media against liveness and document verification
- ✓ Voice-biometric and video-KYC bypass testing
- ✓ Clear pass/fail evidence the client's risk team can action

05 Breach & Attack Simulation

Prove the controls fire. On a cadence, not once a year.

Red team proves the people can be fooled. Breach & attack simulation proves whether the controls behind them actually work. We continuously run real adversary techniques mapped to MITRE ATT&CK against your client's stack, then show exactly which detections fired, which blocked, and which did nothing. The control gap, in evidence, every cycle.

- ✓ Continuous simulation of real-world TTPs mapped to MITRE ATT&CK
- ✓ Validate detection and prevention across the client's existing stack
- ✓ Multi-tenant, multilingual rollout built for MSSP scale
- ✓ Pass/fail evidence that ties gaps back to red team and training scope

THE NUMBERS YOUR CLIENT CANNOT IGNORE

Synthetic Media Walks Past The Stack

92%
of organizations vulnerable to deepfake social engineering

63%
of users cannot tell synthetic from real

78%
rated highly vulnerable across our OSES™ runs

Across 15 OSES™ simulations and 1,057 targets. 14.4% median click rate. 11.7% median action rate.

TWO AUDIENCES. ONE PLATFORM.

Purpose-Built For MSSPs And Enterprise Red Team

For the MSSP

Multi-tenant by design. Run every client from one console. White-label the reports. Standardize delivery, lift margin, and lock in renewals with coverage your competitors cannot match. Set the cadence once and let the platform run.

For Enterprise Red Team

Operator-grade deepfake tooling that scales past one-off engagements. Voice cloning, synthetic video, and OSES™ scoring you can point at any business unit, in any language, and walk straight to the board with the results.

WHY IT PAYS OFF

Why MSSPs Standardize On Breacher.ai

Set It And Forget It

Configure cadence and scope once. Campaigns run, reports generate, training assigns itself. Bill hours instead of babysitting tools.

One Platform, Every Region

Multilingual across simulation, training, and tabletop. A client in five countries does not become five vendor problems.

Consolidate The Stack

Five point tools become one contract and one dashboard. Lower cost to serve. Higher margin. A renewal that is hard to unseat.

Lead With What No One Has

Deepfake red team is the door-opener. The other four products sell themselves off that first report.

Practitioner-Built

Reports written by operators, for operators. Hand them to a CISO or a board without a rewrite.

Coverage Nobody Else Has

Synthetic media walks past phishing sims, training quizzes, and legacy pen tests. You close the gap competitors do not test.

Stop Buying Five Tools. Standardize On One.

Bring deepfake red team, training, tabletops, KYC pen testing, and breach & attack simulation under one multilingual platform. Built for practice leaders who have the budget, the authority, and none of the time.

Book Your 30-Minute Briefing

30 minutes. Straight to a practitioner. We show you the platform live.