



# Secure More Than Humanly Possible

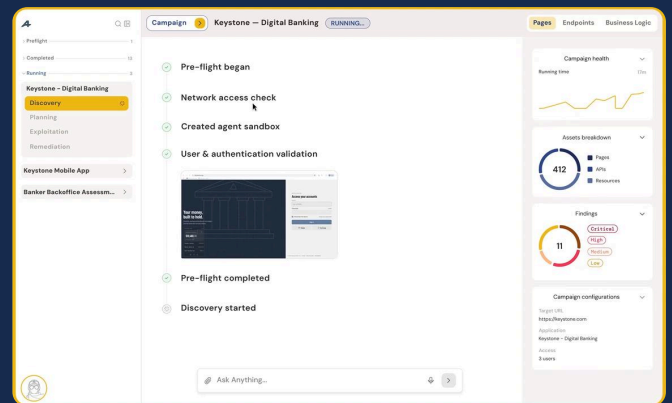
A Security Platform Datasheet

a.security

**A Security** is an autonomous offensive security (AOS) platform. You get an agentic team of cyber attackers on your side, applying the pressure a real adversary would, continuously.

It discovers your estate with business context, maps cross-domain exploit paths, proves what can actually be exploited, fixes it at the source, and re-tests until the path is confirmed closed.

Inside the platform →



## WHY A SECURITY EXISTS

Every security program runs on one assumption: that the controls you bought are holding. Attackers are the only ones actually testing that, and they now run AI at machine speed, around the clock. Frontier-quality offense is now a line item on an API bill, and the exploitation window has gone from months to minutes.

Your own evidence, an annual pentest and a library of prewritten scenarios, was produced at human pace for human-pace adversaries. This is not a coverage gap you can staff your way out of. It is an asymmetry, and only machine-speed offense on your side closes it.

### PROBLEM #01

YOU TEST 5% OF THE SURFACE, 1% OF THE TIME

### ITS IMPACT ON YOU

Annual pentests, BAS scripts, and DAST scans describe a slice of an environment that has already changed by the time the report lands. Then you defend all of it with a report about some of it.

### PROBLEM #02

THE AI-POWERED ATTACKER IS FASTER, CHEAPER, AND EVERYWHERE AT ONCE

### ITS IMPACT ON YOU

AI-run adversaries no longer pick one likely path. They probe every asset and identity in parallel, and the instant a config changes they are already mapping the gap. They test all of you, continuously, while you sample some of you, occasionally.

### PROBLEM #03

FINDINGS SCALE, REMEDIATION CAPACITY DOES NOT

### ITS IMPACT ON YOU

Roughly 900 of every 1,000 flagged issues cannot be executed, and the ~100 that can arrive with no business context. Teams burn the week triaging what no attacker could reach, and lazy AI is making the pile bigger.



# THE SECURITY ADVANTAGE

## Continuous Discovery:

EAP-grade breadth across the enterprise's cyber estate, with business and asset-criticality context. Execution runs outside-in and inside-out from real points of attack, and it re-runs the moment your environment changes, not when the calendar says it is time. Scheduled testing tells you about last quarter. This tells you about right now.

## Proven Exploitation Paths:

We emulate, we do not simulate. Live exploitation chains vulnerabilities into the paths an adversary would actually walk, and hands you a fully logged, audit-ready trail. Pursuits run cross-vector across malware, email, infrastructure, application, and identity abuse. A green checkmark is not proof. A verified path is.

## Break Exploitation Paths:

This is the part no one else promises. Pure validators prove a finding and hand it back to you. Pure exposure platforms prioritize but never prove. We remediate at the source and adjust compensating controls automatically. Gartner expects only 30% of organizations to link validation to automated remediation by 2029. For us that link is the product, not the roadmap.

## Validate, Validate & Validate:

The path is re-tested until it's confirmed closed. We close the loop the attacker does not have to, and every pursuit compounds into a sharper map of how your environment actually fails.

## Attack Path

Verified exploit path end to end



### DISCOVERY

Map the attack surface

01



### PLAN

Prioritize paths to critical assets

02



### EXPLOIT

Execute validated attack chains

03



### REMEDiate

Fix and re-validate

04

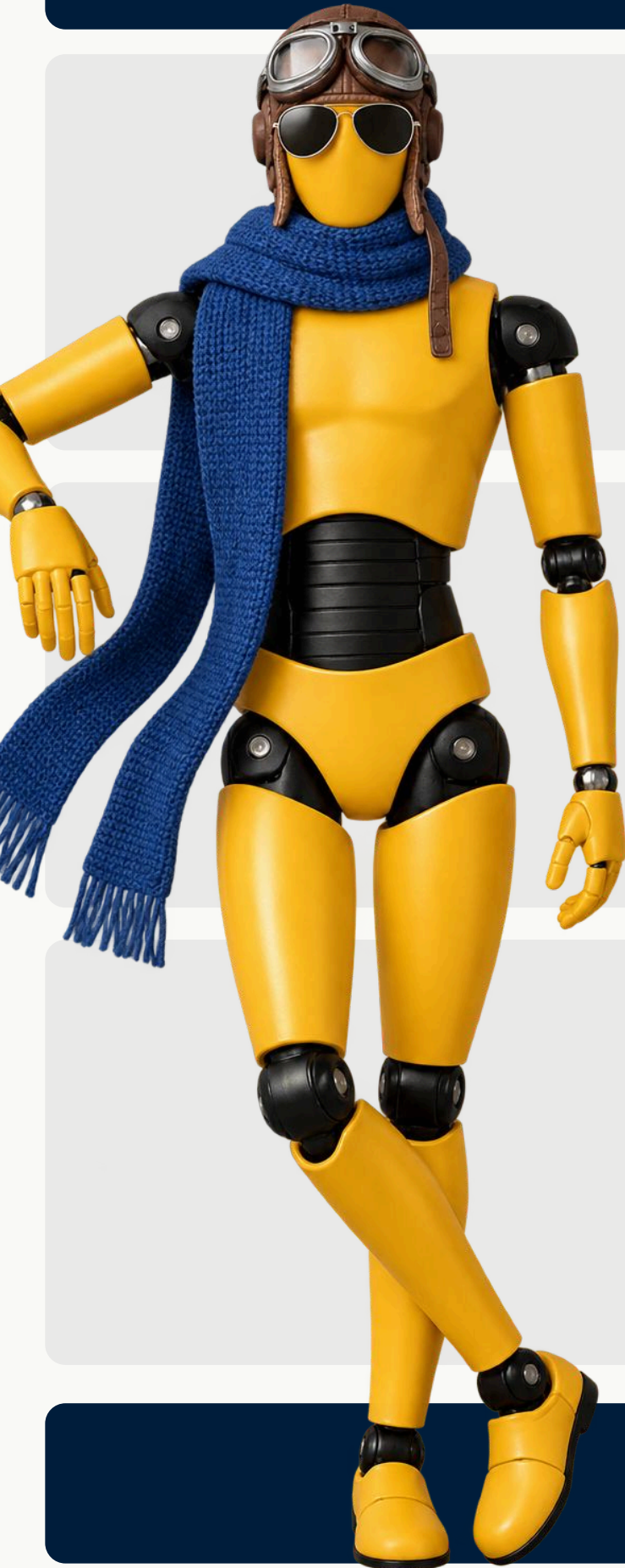


### CONTINUOUS

Repeat as the environment changes

05

# → BUSINESS OUTCOMES



## **Shrink exposure from months to minutes with Autonomous testing.**

So gaps quickly close before adversaries are able to weaponize them against you. Every run tunes your controls, detections, and defensive posture against up-to-date threat scenarios that are continuously enriched. You get empirical proof of security readiness, not theoretical vulnerability data.

## **Compound offensive intelligence and get better.**

Defenses against exploitation paths (and our ability to break them) compound and grow more sophisticated over time as more attack paths are validated, instead of staying static. Every campaign makes you a harder target, without needing to staff an elite (and expensive) human red team to keep pace. This is how you scale offensive testing across the enterprise with little to no specialized skill required.

## **True risk reduction with precision-focus on priority exploit paths**

We present findings in a way that clearly connects A Security outcomes to business risks and objectives. These are the outcome-driven, business-tuned metrics a CTEM program needs to earn board attention. That enables leaders to make informed, risk-based decisions that protect revenue, reputation, and operational continuity, and to show trending proof that security investments are working.

**Explore the use cases →**

# Use cases



1

## Continuous Exposure Validation

### CHALLENGE

Scanners and exposure platforms hand you volume, not proof of what an attacker can actually reach

### HOW <sup>Ⓐ</sup> HELPS YOU

- Runs every exposure from a real point of attack, turning the hits into verified paths with blast radius attached.
- Re-prioritizes, routes, and re-tests until the path is confirmed closed, driving Discover, Prioritize, Validate, and Mobilize continuously.

2

## Next-Gen Pentesting

### CHALLENGE

The annual engagement is stale within weeks, and budget will not stretch to running it more often

### HOW <sup>Ⓐ</sup> HELPS YOU

- Re-maps the estate on every deploy, endpoint, and identity change, so coverage tracks your environment instead of your calendar
- Gives leadership a standing, always-current picture of risk instead of a report that expired on delivery.

3

## Next-Gen BAS

### CHALLENGE

Prewritten playbooks only fire the scenarios someone remembered to configure, and a green pass proves nothing about a real, chained intrusion

### HOW <sup>Ⓐ</sup> HELPS YOU

- Actually exploits and chains paths across threat vectors instead of simulating them, from external and internal points of attack.
- Returns ATT&CK-aligned detect, block, and miss evidence, plus the vendor-specific tuning your SIEM, EDR, and XDR need.

4

## Next-Gen DAST

### CHALLENGE

DAST floods AppSec with unverified severity and misses the chained, business-logic flaws that actually matter

### HOW <sup>Ⓐ</sup> HELPS YOU

- Confirms real exploitability against the running build and re-tests on every deploy, not at the next scan window.
- Chains findings into verified attack paths and attaches blast radius to the systems downstream.

## 5

## Adversarial AI Protection

**CHALLENGE**

Your board asks whether you would hold against a frontier model, and nothing you own today can answer it

**HOW  HELPS YOU**

- Runs frontier-model offense continuously and responsibly inside your perimeter through our agentic harness.
- Finds the machine-speed, cross-domain paths no human tester had the hours to reach, then closes and re-validates them until confirmed shut.

## 6

## De-Risk M&amp;A, Divestitures and Due Diligence

**CHALLENGE**

Posture at the target is self-reported and months old by the time you sign

**HOW  HELPS YOU**

- Delivers full exposure assessment breadth against an estate you do not control yet, inside the diligence window.
- Surfaces the verified paths their own reporting missed, so remediation lands in the deal terms instead of on your roadmap.

## 7

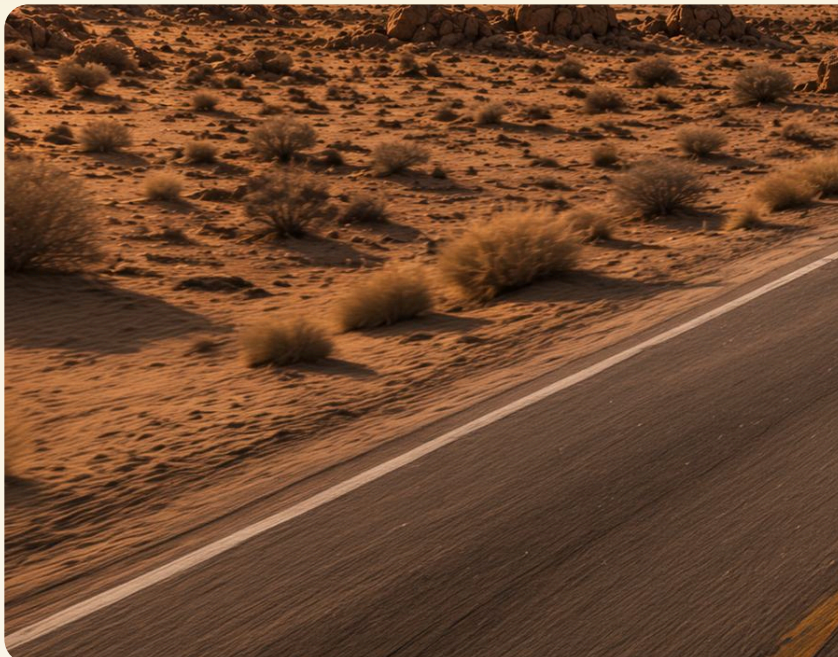
## Accelerate AI Adoption

**CHALLENGE**

Teams ship AI-built tools wired to real data, live in production before AppSec knows they exist

**HOW  HELPS YOU**

- Discovers and tests vibe-coded applications as they ship, before they ever touch sensitive data.
- Closes the lateral chains into systems those apps were never meant to reach, ahead of go-live.





# Secure More Than Humanly Possible

We relentlessly defend humanity against weaponized AI: → Book a demo today by visiting [a.security/get-a-demo](https://a.security/get-a-demo)

