

How to Get Fortune 500 Inbounds in Cybersecurity

Michael Bargury
Co-founder & CTO
Zenity

Vertex Ventures Israel | Founder-led-Growth for Cyber Startups | April 30, 2026



How to ~~Get Fortune 500~~ ~~Inbounds~~ Create Value in Cybersecurity

Michael Bargury
Co-founder & CTO
Zenity

Vertex Ventures Israel | Founder-led-Growth for Cyber Startups | April 30, 2026



CISO: DAY JOB

UNATTAINABLE. SKEPTICAL. DONE WITH THE HYPE.





RSAC, Infosec-themes, and crummy products

March 27, 2026  haroon meer



RSAC was more subdued this year.

Although the floor was plastered in AI, AI protection & Agentic*, everyone knows its a placeholder while we figure things out..

So it's more performative than normal:
Vendors act like they have the solutions & attendees act like they believe it

“He's saying the quiet, obvious part out loud.”

“The problem was that in the process, they were over-rotating these companies to spend massive amounts of money not on building products, not on improving customer experience, not trying to solve a meaningful problem, but on marketing and hype building. So what you got was a lot of very big, very notorious, very xxxxy, hollow companies.”

“At no point of any of that has somebody built a security product or focused on solving a security problem. That’s the feel of walking the RSA floor.”

JAGS, 2026



r/cybersecurity · 3y ago
[deleted]



What vendor looks really good but is actually terrible?

Business Security Questions & Discussion

I've had some great demos that fall apart on first contact with our environment and users. Was wondering what you've seen



exceptionallynormal · 3y ago

Securonix UEBA.

70 Award Share ...

8 more replies



[deleted] · 3y ago

McAfee ePO was hot garbage, dunno if its improved since Trellix, I refuse to use it

267 Award Share ...



VHDamien · 3y ago

At this point I believe ePO survives entirely off of long standing federal government contracts.

140 Award Share ...



CosmicMiru · 3y ago

I use epo due to a long standing government contract, want to die everytime something breaks



darKv8 · 3y ago

Darktrace

170 Award Share ...



tedchambers1 · 3y ago

I was wondering how long I'd have to scroll until I saw this.

I've been at three separate fortune 200 companies that have gotten rid of darktrace - that is remarkable because companies that size never really get rid of anything.

Darktrace's value is having a cool screen for your SOC and literally nothing else and the cost of that screen is astronomical.

54 Award Share ...

64 more replies



130 Award Share ...



NBA-014 · 8mo ago

Service Now - having to create ticket after ticket to get people to do their job. Issue is that the tool never routed the ticket to the right sysadmin or networking group.

Another was Archer. What a piece of crap!



2 Award Share ...



Orangesteel · 8mo ago

Symantec and Oracle. Both gouge customers and should have died long ago.



304 Award Share ...



r/cybersecurity · 8mo ago
Mobile-Astronomer428



The most hated vendor

Other

What is the vendor you guys hate the most?



SwiftOnSecurity
@SwiftOnSecurity

@ucsenoi @jeremiahg
@ThinkstCanary Yeah it's the only thing that's impressed me for people whose job isn't "Run honeypots." I was hugely into honeypots years ago and it's an expensive hobby time-wise.



Vlad Ionescu
ucsenoi

@jeremiahg @ThinkstCanary
Their on-prem canary is one of the only things that caught me right away in post-exploitation without my knowing I was burned. Solid concept and product.



thaddeus e. grugq
@thegrugq

Get [canary.tools](#), it can't protect against shitty security products but at least you'll know they failed



Cesar Cerrudo
cesarcer

How long until we see products to protect against security products?



Corey Quinn
@QuinnyPig

I'm not particularly biased at all; they're not a current sponsor to the best of my knowledge. @ThinkstCanary operationalizes a pattern I fell in love with a decade ago. Heartily endorse.



haroon meer
haroonmeer

Can verify. @BradleyJayanath has a lovely radio-voice.

Also: @ThinkstCanary is pretty useful.

(I'm a little biased here)

How to contribute to the cybersecurity community?





OWASP Top 10 For Agentic Applications 2026

OWASP Gen AI Security Project – Agentic Security Initiative

Version 2026
December 2025

OWASP Agentic Skills Top 10

[Main](#)

owasp

incubator

License

CC BY-SA 4.0

version

1.0-2026

updated

March 2026

Security Risks and Mitigations for AI Agent Skills

Covering OpenClaw (SKILL.md YAML), Claude Code (skill.json), Cursor/Codex (manifest.json), and VS Code (package.json) ecosystems.

Breadcrumb: [OWASP](#) > [Projects](#) > Agentic Skills Top 10



OWASP Non-Human Identities Top 10

 Search

OWASP Non-Human Identities Top 10

[Home](#)

Table of Contents

Introduction

Ranking Criteria

Release Notes

Methodology and Data

OWASP Non-Human Identities Top 10 - 2025

NHI1:2025 Improper Offboarding

NHI2:2025 Secret Leakage

NHI3:2025 Vulnerable Third-Party NHI

NHI4:2025 Insecure Authentication

NHI5:2025 Overprivileged NHI

NHI6:2025 Insecure Cloud Deployment Configurations

Home

Welcome to the **OWASP Non-Human Identity (NHI) Top 10 - 2025!**

This project outlines the **top 10 risks associated with non-human identities (NHIs)** for application developers. With NHIs becoming vital in development pipelines, understanding these risks is critical.

The list was compiled by identifying key risks organizations face with NHIs and ranking them using the [OWASP Risk Rating Methodology](#). Data sources included real-world breaches, surveys, CVE databases, and more. For details on our process, see [Ranking Criteria](#) and [Methodology and Data](#).

Start with the project's [Introduction](#), and explore the [OWASP Non-Human Identity Top 10 - 2025](#) for an overview of the risks.

Contributions are welcome! See our [Contributing Guidelines](#) to get involved and help improve the project.





OWASP Top 10:2025

 Search

 OWASP/Top10
☆ 5.6k 🗨 1.1k

OWASP Top 10:2025

[Home](#)

Introduction

About OWASP

What are Application Security Risks?

Establishing a Modern Application Security Program

OWASP Top 10:2025

Welcome to the OWASP Top 10:2025 Release.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Table of contents

About This Release

Main Project Page

Getting Started

Navigation

Top 10:2025 List

OWASP Top 10 for Large Language Model Applications

[Main](#)[Example](#)

About This Repository

This is the repository for the **OWASP Top 10 for Large Language Model Applications**. However, into the comprehensive **OWASP GenAI Security Project** - a global initiative that encompasses much beyond just the Top 10 list.

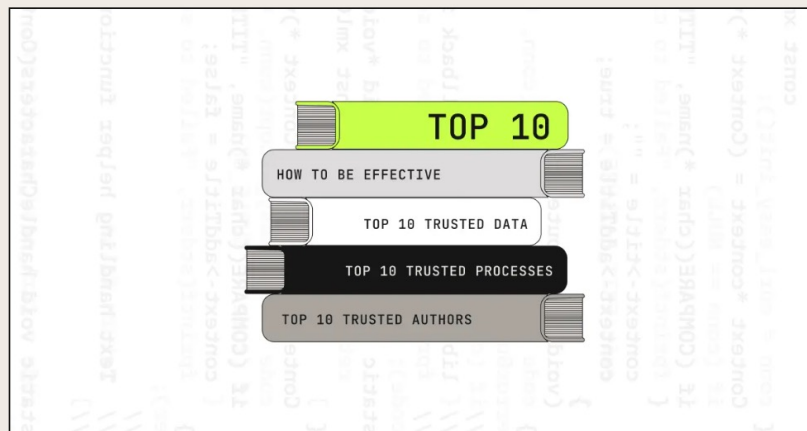
Create unique value and open source it

[Home](#) / [Blog](#) / [Security](#) / Five Questionable Things About Top Ten Sec...

By Mark Curphey

October 3, 2023

Five Questionable Things About Top Ten Security Lists



Everything is not as it seems when you look under the hood

at top ten security lists.

Can you trust the authors?

I know there will be blowback from some people about that question, so I am going to tackle it upfront and head-on. The blowback is going to come from people who don't like the inference of the quote below, the authors of the lists themselves.

"It is difficult to get a man to understand something when his salary depends upon his not understanding it." - Upton Sinclair

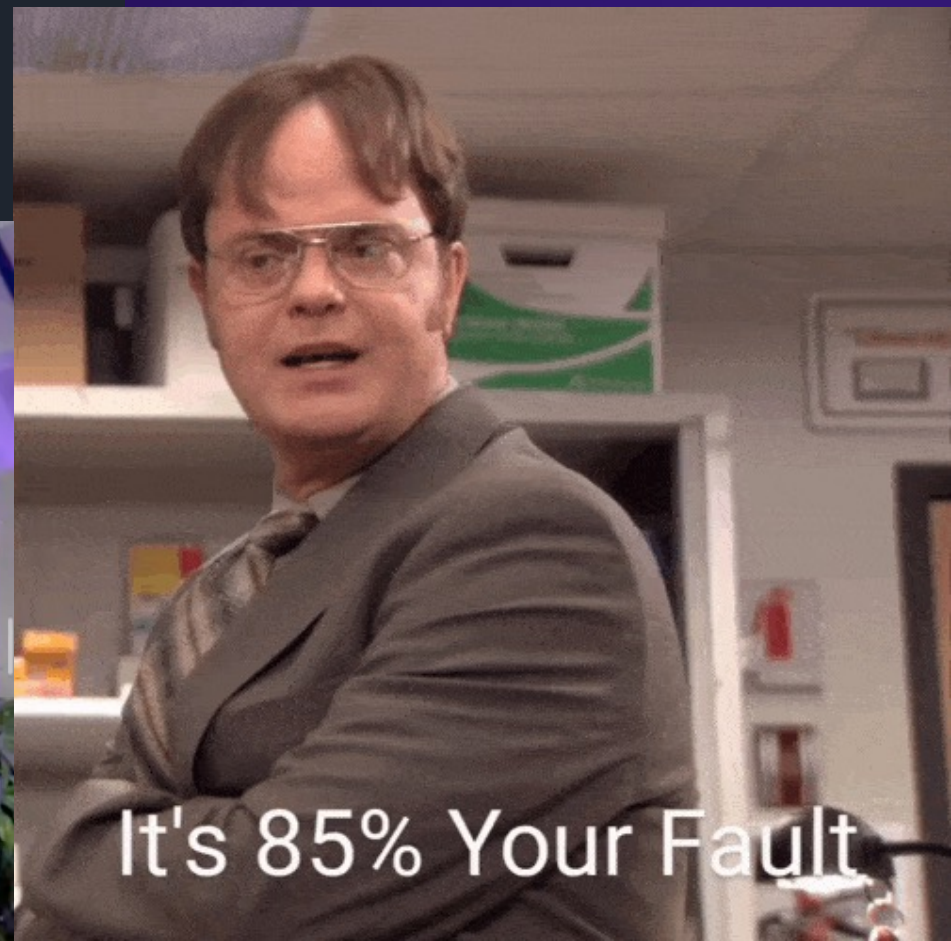
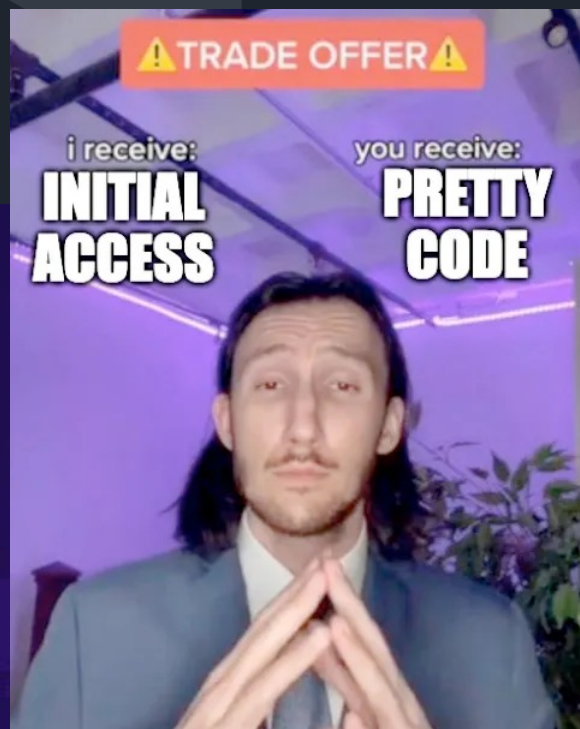
Ill-Advised Adventures

Stop Putting Your Passwords Into Random Websites

(Yes, Seriously, You Are The Problem)

Vulnerability Research

Find unique vulns /
issues and say
things as they are



The sins of security vendor research

1. FUD: *Every vulnerability is a “critical risk”*
2. False novelty: Don't ignore or take credit for other work
3. Correlation, not caution
4. Selling out to marketing



We are all AI security n00bs



ALL OF US



Be honest

@mbrg0
#BHUSA

@mbrg0

We aren't making *real* progress.

AI Agent Security Summit | Presented by **zenity** Labs

THE LEAGUE
ASSEMBLY
SAN FRANCISCO

CYBERSECURITY
MONTH

Hobble your AI agents to prevent them from hurting you too badly

That's the main takeaway from the Zenity AI Agent Security Summit

 [Thomas Claburn](#)

Thu 9 Oct 2025 // 07:27 UTC

11 



Michael Bargury, CTO of AI security company Zenity, welcomed attendees to the company's AI Agent Security Summit on Wednesday with an unexpected admission.

"This is a new space and we – frankly – don't really know what we're doing," he said at San Francisco's Commonwealth Club. "But we're trying ... We need to face things as they are. And the only way to do it is together."

Zenity's marketing graphic for its AI Agent Security Summit inadvertently made that point by mixing Marvel and DC Comics motifs. The conference graphic read, "The League Assembles," applying Marvel's "Avengers, assemble!" catchphrase and font styling to what DC fans might read as a reference to The Justice League.





@DavidSchutt1 3 months ago



This was one of the more honest and useful talks I've seen on agent security in a while.

The distinction between soft boundaries (guardrails, classifiers, “another LLM checking the LLM”) and hard boundaries enforced by architecture is critical, and it’s refreshing to hear it stated plainly. The reframing of “prompt injection” as persuasion rather than a patchable technical flaw also feels exactly right — it explains why benchmarks can look great while real systems remain fragile.

The concrete examples around memory shutdown on untrusted context, connector scoping, tool-chaining breaks, and runtime mutability (especially MCP) were particularly valuable. They highlight how many current failures aren’t novel AI problems so much as violations of lessons we already learned in other domains — just reintroduced at a higher level of abstraction.

Appreciate the focus on discipline and restraint over optimism. This kind of thinking moves the field forward more than another “better guardrail” ever will.

Thanks for putting this together and for sharing real design tradeoffs instead of slogans. 🏆

Show less



Reply





Joshua Woodruff  • 1st
Helping companies deploy AI without compromising their data | Author o...
[View my newsletter](#)
1mo • 

I met **Gadi Evron** yesterday for the first time.

A few hours later I watched him do something I won't forget.

Gadi is CEO of Knostic, an AI security company. Zenity, one of his direct competitors, was supposed to present at [un]prompted in San Francisco. They couldn't make it. Israel's airports shut down.

Gadi picked up their slides and presented for them.

No announcement. No fanfare. Just: these are our colleagues and they can't be here.

I've been in enterprise security for over 30 years. I've watched competitors tear each other apart over market share, positioning, pipeline. I've seen companies quietly celebrate when a rival stumbled.

   You and 720 others 126 comments · 36 reposts

Reactions



Be collaborative.
Community >> company.



Panel Discussion: How Leading AI Platforms Approach Building Trustworthy Agents

In this panel, security leaders from ServiceNow, Microsoft, Google, and OpenAI will share how

[Read more](#) ▾

Speakers



Amanda Grady

VP of AI Platform Security, ServiceNow



Michael Bargury

Co-Founder & CTO, Zenity



Naveed Makhani

Product Lead for AI Security Products, Google



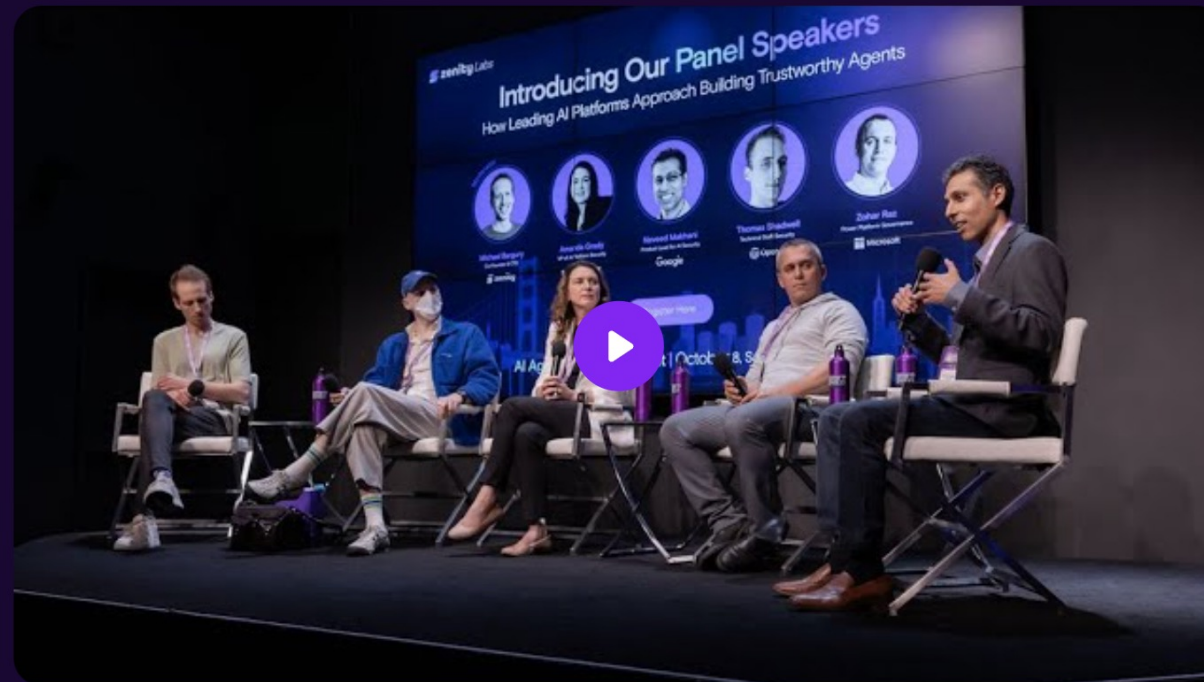
Zohar Raz

Group Product Manager Power Platform Governance, Microsoft



Thomas Shadwell

Member of Technical Staff,
Product & Application Security



CISO: DAY JOB

UNATTAINABLE. SKEPTICAL. DONE WITH THE HYPE.



CISO: DEF CON

OPEN. CURIOUS. ONE OF THE GOONS.

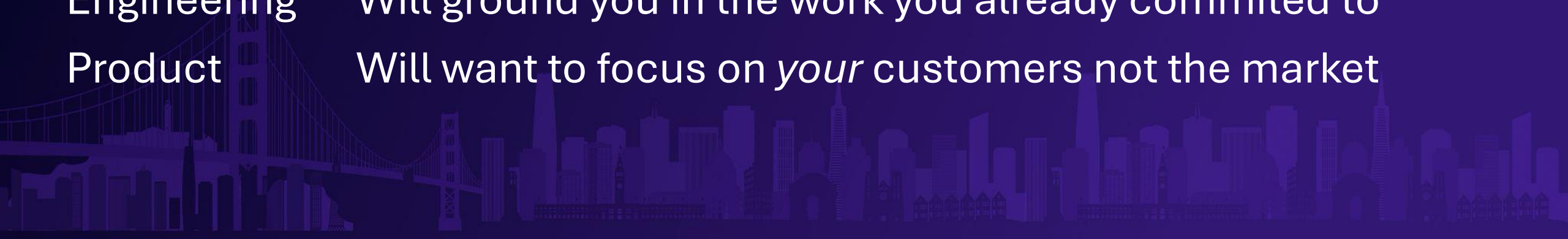


Generate value **for others**



REASONS WHY YOU WON'T FOLLOW THIS ADVICE

Marketing	Will loss a lead-generation opportunities
Legal	Will say NO because sharing research is risky
Sales	Will tell you its not helping them hit quota
Partnerships	Will explain that sharing vendor errors is not good business
Engineering	Will ground you in the work you already committed to
Product	Will want to focus on <i>your</i> customers not the market



They're all right. Lead anyway.

