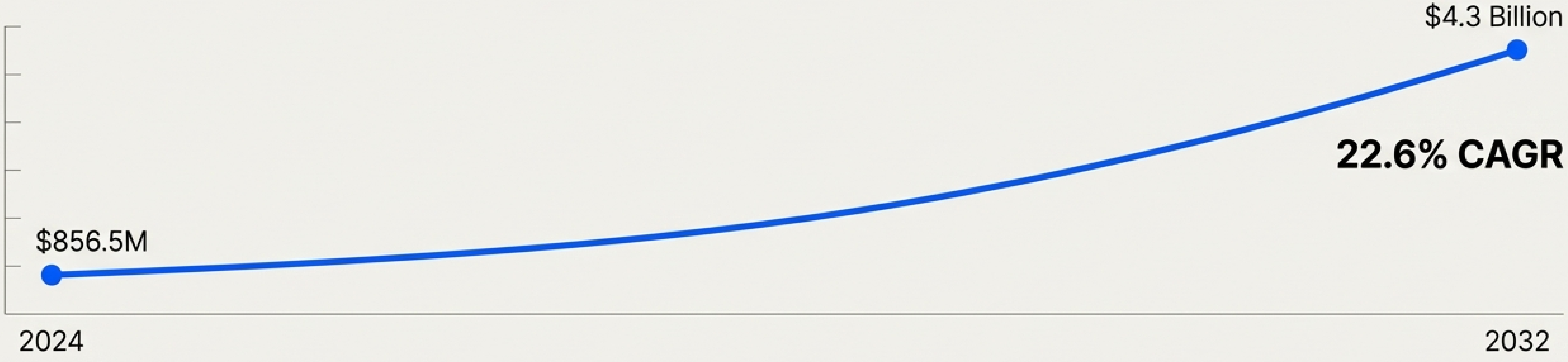
Attack Surface Management Still Makes Security Teams Angry

The Promise, The Peril, and The Path to an ASM That Works

The Market Agrees: ASM is Mission-Critical



Digital Expansion & Shadow Assets

The traditional perimeter has dissolved. Businesses face a sprawling map of web apps, APIs, shadow IT, and third-party services.

Supporting Stat: 92% of enterprises now use multiple clouds, creating immense complexity.

Dynamic Environments

Attack surfaces are not static. Cloud workloads, new APIs, and remote connections change daily. Attackers exploit this drift.

Supporting Stat: Over 70% of businesses now spend more on tools for real-time visibility and continuous monitoring.

Compliance and Trust

New regulations (SEC cyber disclosure, NIS2) mandate continuous asset monitoring. ASM has become a business imperative for demonstrating proactive risk management.

The Technology is Evolving at Breakneck Speed

AI-Powered Discovery

Using AI/ML to automatically discover assets and prioritize real threats from noise.

Example: An AI-driven tool found 1,000+ misconfigured cloud buckets for a bank in hours.

IoT & OT Security

Special emphasis on discovering and hardening connected devices with default passwords or outdated firmware.

Proactive Threat Intelligence

Correlating asset data with CTI feeds to prioritize vulnerabilities being actively targeted in the wild.

ASM
PLATFORM
2025

Zero Trust Integration

Feeding continuous asset insights into ZTA frameworks to ensure every device, user, and service is verified.

Cloud-Native Coverage

Direct integration with AWS, Azure, and GCP to continuously inventory cloud assets.

Third-Party Risk Monitoring

Mapping the attack surfaces of vendors and partners as an extension of your own.

The Market is Soaring. The Tech is Evolving.

So why does this all feel so familiar?

And why are security teams still getting breached by things they thought ASM would solve?

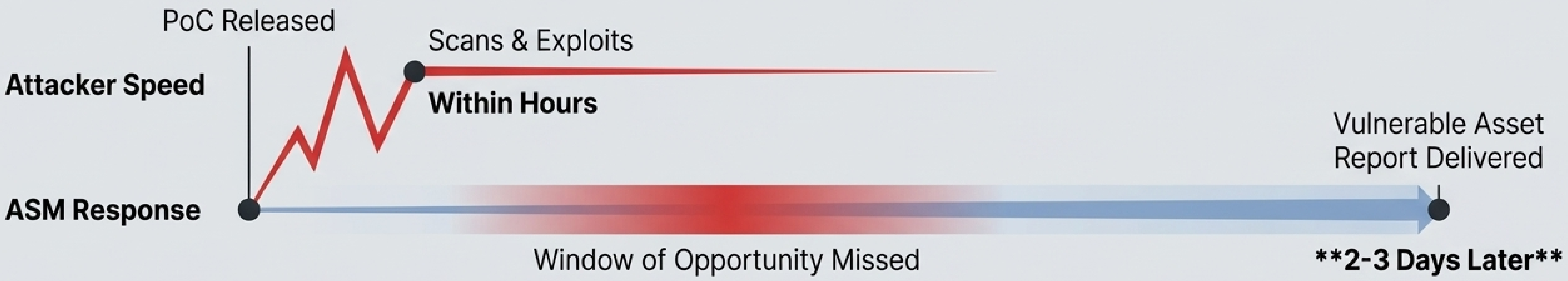
A Practitioner’s View: “ASM is Still Structurally Broken”

> “I’ve spent a decade analyzing zero-day and one-day vulnerabilities. I’ve seen how attacks start, spread, and repeat. ASM was meant to standardize our defense, but in 2025, the experience is the same: It still makes us angry.”

1. The Speed Mismatch: ASM operates in days, attackers operate in minutes.
2. **The One-Dimensional Map:** It lists external assets but misses the true attack surface.
3. **The Human Blind Spot:** It sees vulnerable code but not the flawed human processes that create it.

Problem #1: ASM is Structurally Slow

ASM vendors talk “near real-time,” but the operating model is built for “after the fact.”



Case Study: The `react2shell` Incident

Case study has the `react2shell` Incident infertated increasing the reactive script in a rausing tospecure vee beings materaed, that ASM changed had a been a tize detection, expervs more intections or y time gap remediation.

The Root Cause

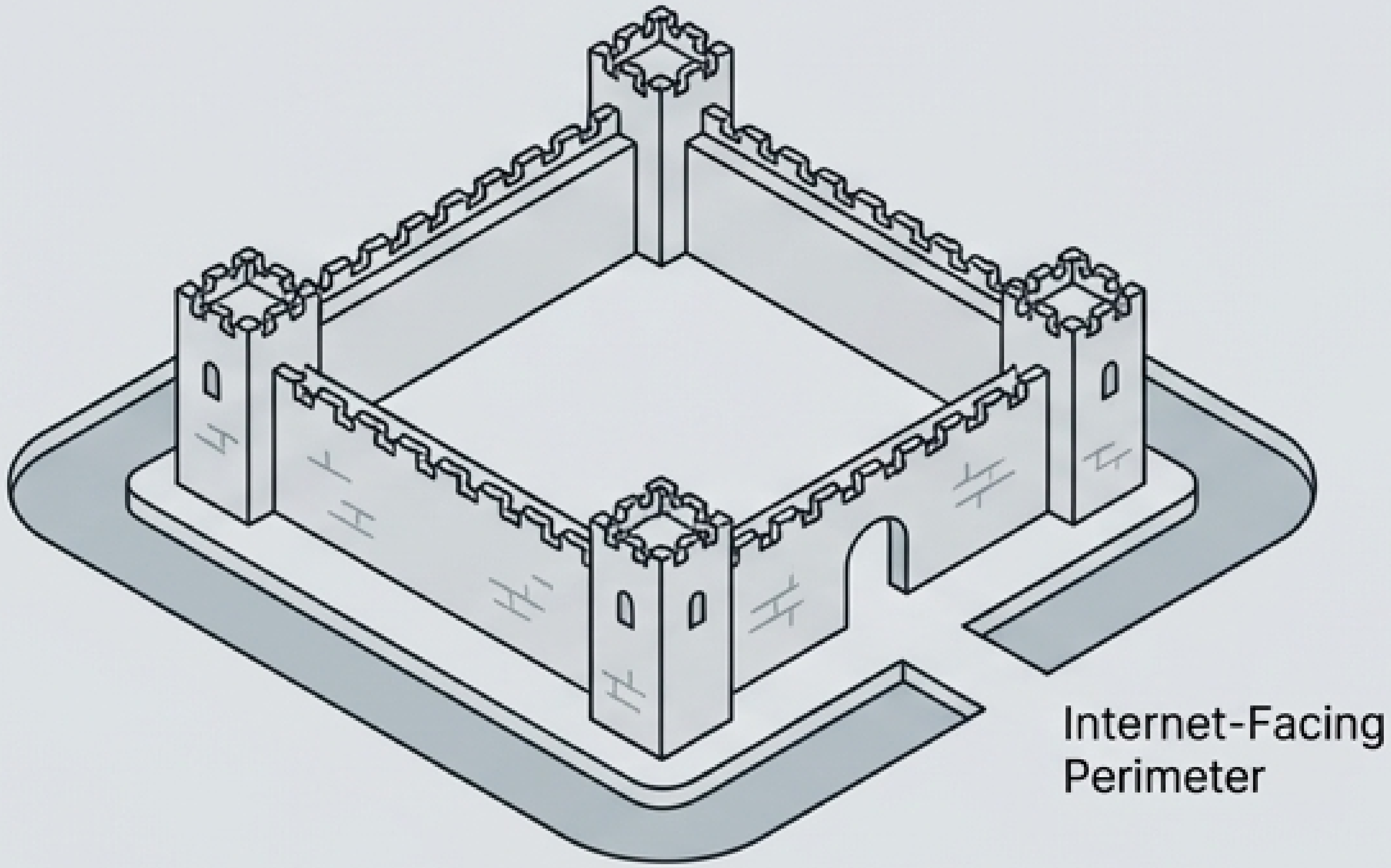
- Slow, periodic scanning cycles designed for massive customer bases.
- Internal processes focused on “Detection → Verification → Approval → Reporting.”
- A model built for notification, not immediate, automated blocking or suppression.

The top frustration in the SANS 2025 survey was the **time gap between detection and actual remediation**.

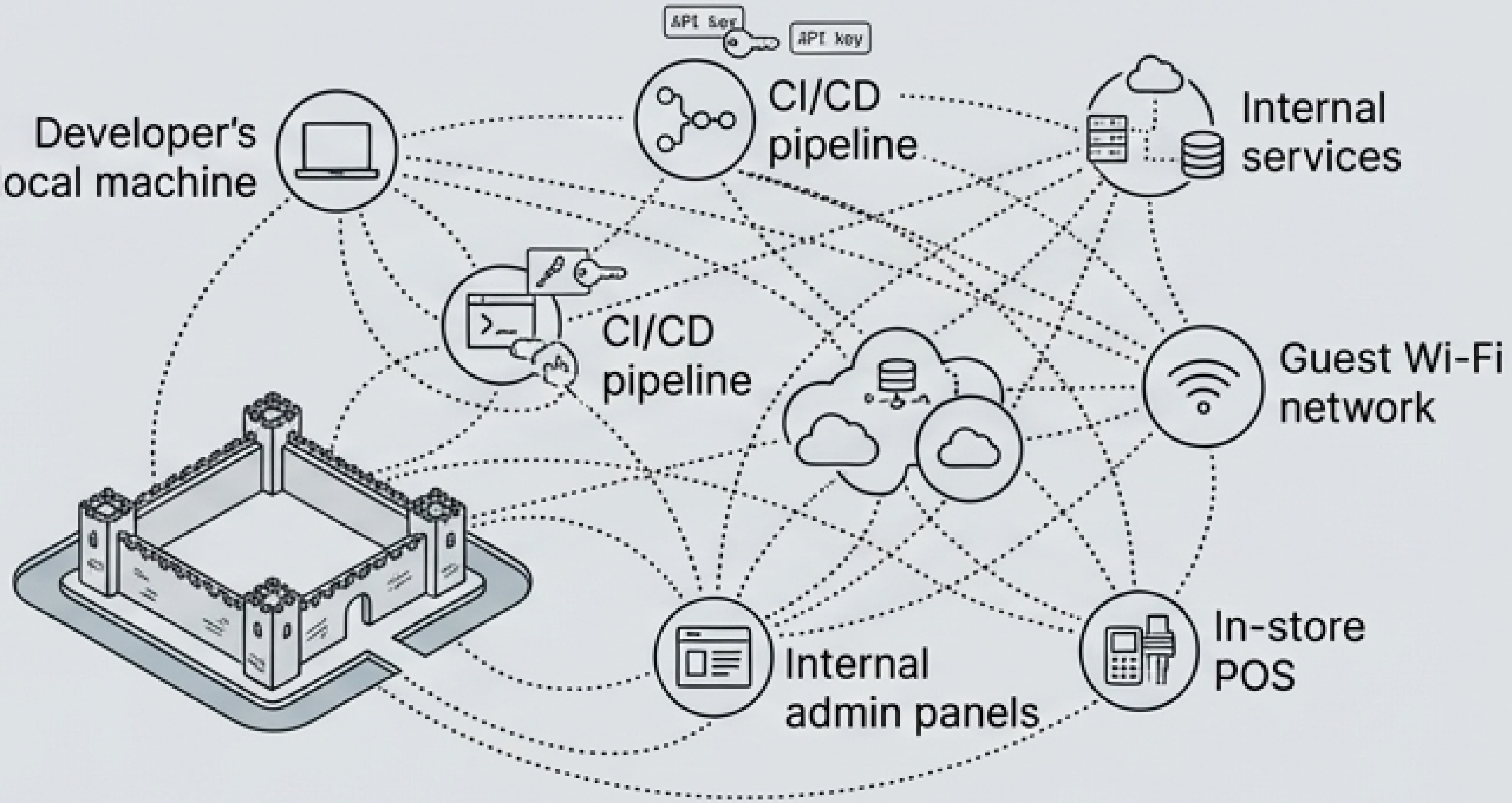
Problem #2: ASM Sees the Attack Surface in 1D

Today's ASM isn't Attack Surface Management. It's **External Asset Listing**.

What ASM Sees



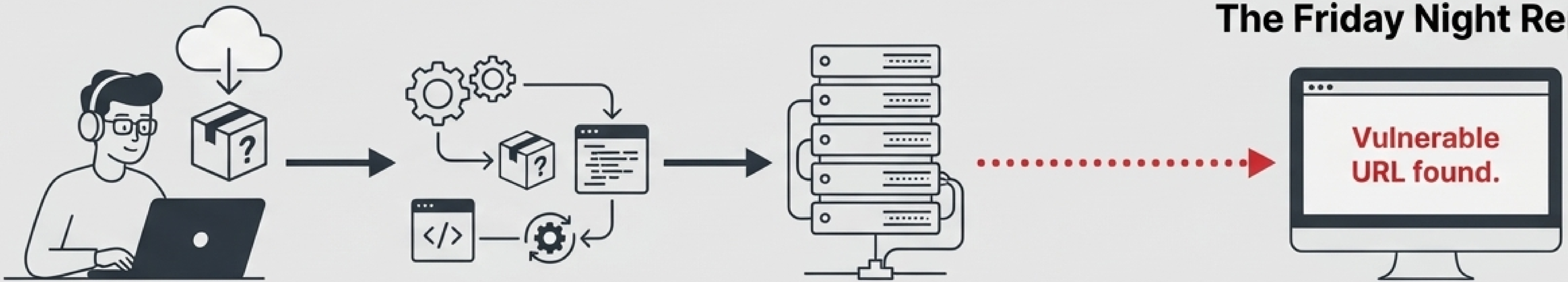
The Real Attack Surface



KuppingerCole calls this a lack of **"ownership-aware discovery."** The problem isn't just a lack of integration; it's a fundamental misunderstanding of the problem."

Problem #3: ASM Focuses on PoCs, Not People

The Friday Night Report



A developer downloads an unvetted package.

It’s included in the build pipeline.

It’s deployed to production.

ASM finds the what, but can’t answer the why.

- Which development practice is dangerous?
- Who or which team repeats this behavior?
- What organizational process allows this to happen?

A SANS survey found that only a “tiny fraction” of organizations had an ASM that could link vulnerabilities back to the root-cause behaviors.

But Hasn’t “AI-Powered ASM” Solved This?

No.

AI

Old ASM Model

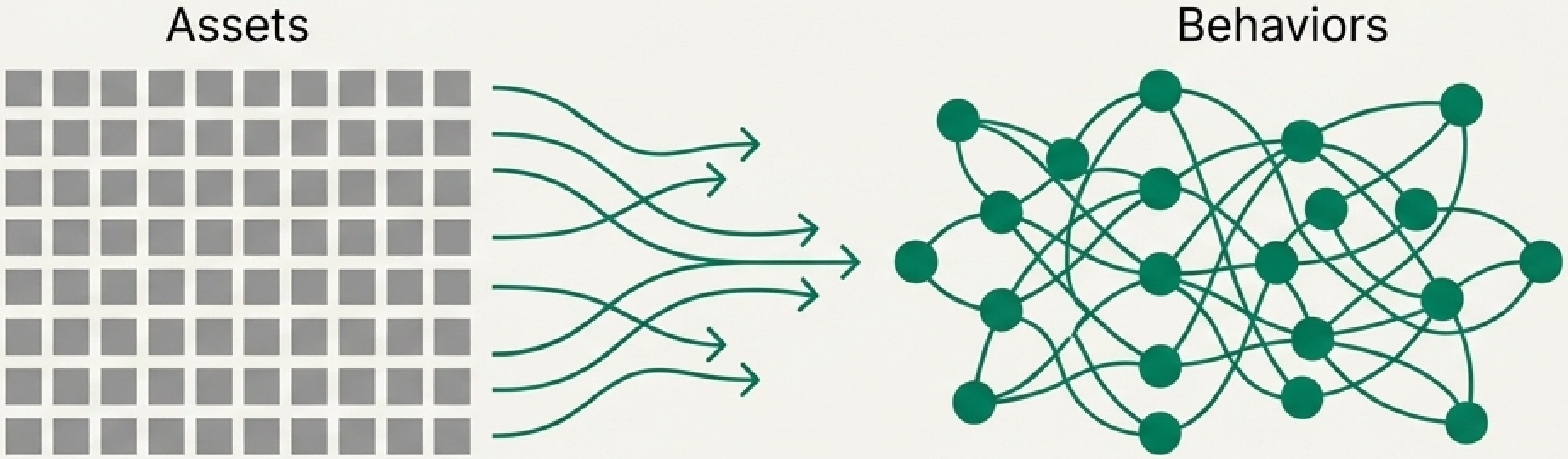
The Same Frustrating Report

AI can make discovery *faster* and asset *identification* more accurate.
However, it doesn't change the flawed operating model.

- The model is still **report-centric**.
- It still struggles with **unclear asset ownership**.
- It is still fundamentally **blind to the human behaviors** and processes that create risk.

> “AI just got better at making the lists.
> It didn’t save the security team’s Friday night.”

The Future of ASM: Manage Behavior, Not Just Assets



The Attack Surface is not a list of assets. It is the collection of **human and system behaviors** that create risk.

This changes everything

- Vulnerability Management is no longer about managing URLs; it’s about managing development habits and pipelines.
- Defense is no longer about external scanning; it’s about building immediate, internal feedback loops.

What Behavior-Based ASM Looks Like

Old Paradigm (Asset Listing)

Focus: Internet-facing assets.

Unit of Work: A vulnerable URL or CVE.

Output: A static report or ticket.

Goal: Achieve a complete asset inventory.

Question Answered: “What is exposed?”

New Paradigm (Behavior Management)

Focus: Risky development & operational patterns.

Unit of Work: A flawed process or repeated bad habit.

Output: An automated feedback loop to a specific team.

Goal: Fix the system that creates vulnerabilities.

Question Answered: “Why does this keep happening?”

The Four Pillars of a Smarter ASM

1. CI/CD & SCM Integration

Detect risky behaviors directly where code is built and stored—like hardcoded secrets, use of vulnerable libraries, or insecure configurations *before* they are deployed.

2. Pattern Recognition

Identify recurring patterns of vulnerability creation. Is a specific team, application, or development process consistently introducing the same type of flaw?

3. Systemic Feedback Loops

Move beyond ticketing individuals. Create feedback that helps managers and architects fix the underlying process, training, or structural issues causing the risk.

4. Attack Path Correlation

Integrate with XDR/ADR data to prioritize not just what is *vulnerable*, but what is on a *proven attack path* that threat actors are actively using.

From an Illusion of Security to a System of Defense

The ASM market is growing, and vendors claim to be evolving. But for practitioners on the front lines, the core experience remains one of frustration—too slow, too narrow, and blind to the real source of risk.

“For ASM to become a true security tool, it must evolve from a tool that lists assets into a system that manages the very structure of how risk is created.”

Until then, it provides little more than the illusion of security.