

The \$0 Perimeter

Why Your SaaS Security is Broken (And Why 16 Tools Aren't Enough)

By TekSol Global | Cybersecurity & AI Practice

"We take security seriously."

Every company says it. Every vendor promises it. Yet breaches keep happening - not just to small businesses, but to well-funded enterprises with entire security teams. Why? Because traditional cybersecurity was built on a mental model that no longer exists: **The Perimeter**.

The Game Has Changed

In the past, we built a strong wall around our network and locked the doors. But today, your data lives in 40 different SaaS apps - Salesforce, Microsoft 365, Slack - and your employees are layering AI tools on top of all of them.

There is no wall anymore.

The barrier to entry for attackers is also dropping fast. Within the next six months, an attacker won't need deep technical skills. They'll simply hand a list of IP addresses to a Large Language Model and say, *"Go - tell me what you find."*

The 16-Tool Paradox

Research from the Cloud Security Alliance (CSA) reveals a startling reality: the average organization runs **13 separate security tools** just for SaaS and AI. In financial services, that number jumps to 16.

And yet, **83% to 97%** of those same firms report above-average breach rates.

You can have sixteen tools, but if you don't have the right people who understand your environment, those tools are just expensive dashboards. A new security engineer might take months just to understand what a "normal" day looks like in your environment - let alone spot a silent intruder.

The "Engine Room": Non-Human Identities

This is the part most leaders miss. When we think about access, we think about people. But today, the vast majority of entities accessing your data are **Non-Human Identities (NHIs)**: bots, service accounts, API keys, and OAuth tokens.

- **The Scale:** There are now **30 non-human identities for every 1 human identity**.
- **The Blind Spot:** 5 out of 6 CISOs admit their tools are inadequate at distinguishing between human and bot behaviour.

If your security is designed to watch people, you are functionally blind to the engine room where the real work - and the real theft - happens.

The "Museum" Analogy & The ShinyHunters Breach

Attackers are exploiting this gap in governance. The massive ShinyHunters attack is a perfect case study. They didn't need to plant complex malware. They simply walked through a "trusted" side door.

Case Study: The Salesforce / Drift Breach

- **The Scale:** Over 1.5 billion records stolen from approximately 760 organizations.
- **The Entry Point:** Attackers found hardcoded OAuth tokens for a Drift chatbot integration hidden in a public GitHub repository.
- **The Lateral Movement:** Because those tokens were "trusted" by customers' Salesforce instances, attackers moved silently between applications - exfiltrating databases from companies including Cloudflare, Google, and Zscaler.

It is like having world-class museum security for after-hours break-ins, while the real theft happens at 2:00 PM on a Tuesday - because the side doors were left wide open.

Here is the gap that makes this so alarming: **90% of CISOs believe they have strong OAuth governance, yet 27% of organizations were breached through those exact keys.**

4 Practical Steps for Leaders

Before you buy your 17th security tool, take these four steps:

- 1. Take Stock** Ask yourself: *"How long would it take to get a full list of every application connected to our company data?"* If the answer isn't "minutes," that is Priority One.
 - 2. Audit the Endpoints** Identify which AI plugins or coding environments (like Cursor or specialized IDEs) your developers are actually using. You cannot govern what you do not know about.
 - 3. Map Non-Human Access** Review your service accounts and API keys. When were they last rotated? Do you know what they have access to? Most organizations cannot answer this question.
 - 4. Speed of Detection** Prevention is the goal, but detection is the reality. You must be able to answer *"What happened?"* in hours, not weeks.
-

Want to Know Where Your Organization Stands?

At TekSol Global, we help organizations bridge the gap between AI adoption and ironclad security - through practitioner-led training grounded in real-world experience.

[Book a free consultation →](#)

Next week: We've discussed the unlocked doors. Next, we meet the intruders - the AI Agents that are already acting on your behalf, sometimes with catastrophic results.