



REDHUNT LABS

DISCOVER. ATTACK. REPEAT.

All Your Shadow SaaS Are Laughing at Your Firewall

Shubham Mittal

11th July 2025



#WHOAMI

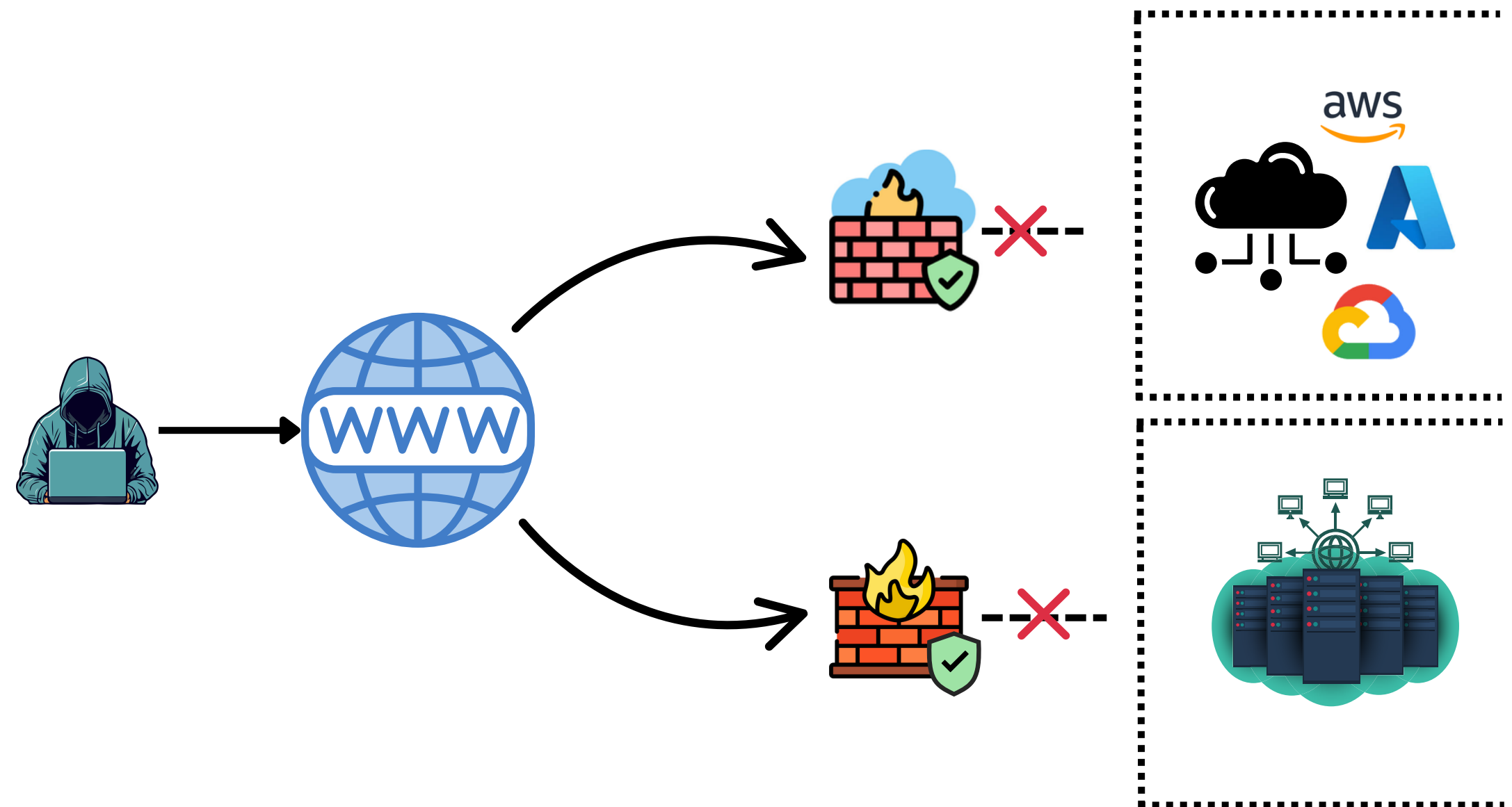
Shubham Mittal

- CEO & Co-Founder, RedHunt Labs
- Co-Founder, Recon Village @ DEF CON
- BlackHat Review Board – US, EU, Asia
- 14+ years in Infosec, OSINT, and Threat Intel
- Runs Project Resonance: tracking real-world exposed assets
- Scans the Internet for fun
- OSINT, Recon, Travel & Cricket

What **CAN** Firewalls do?

Monitor and Prevent Attacks
to **YOUR** Infra.

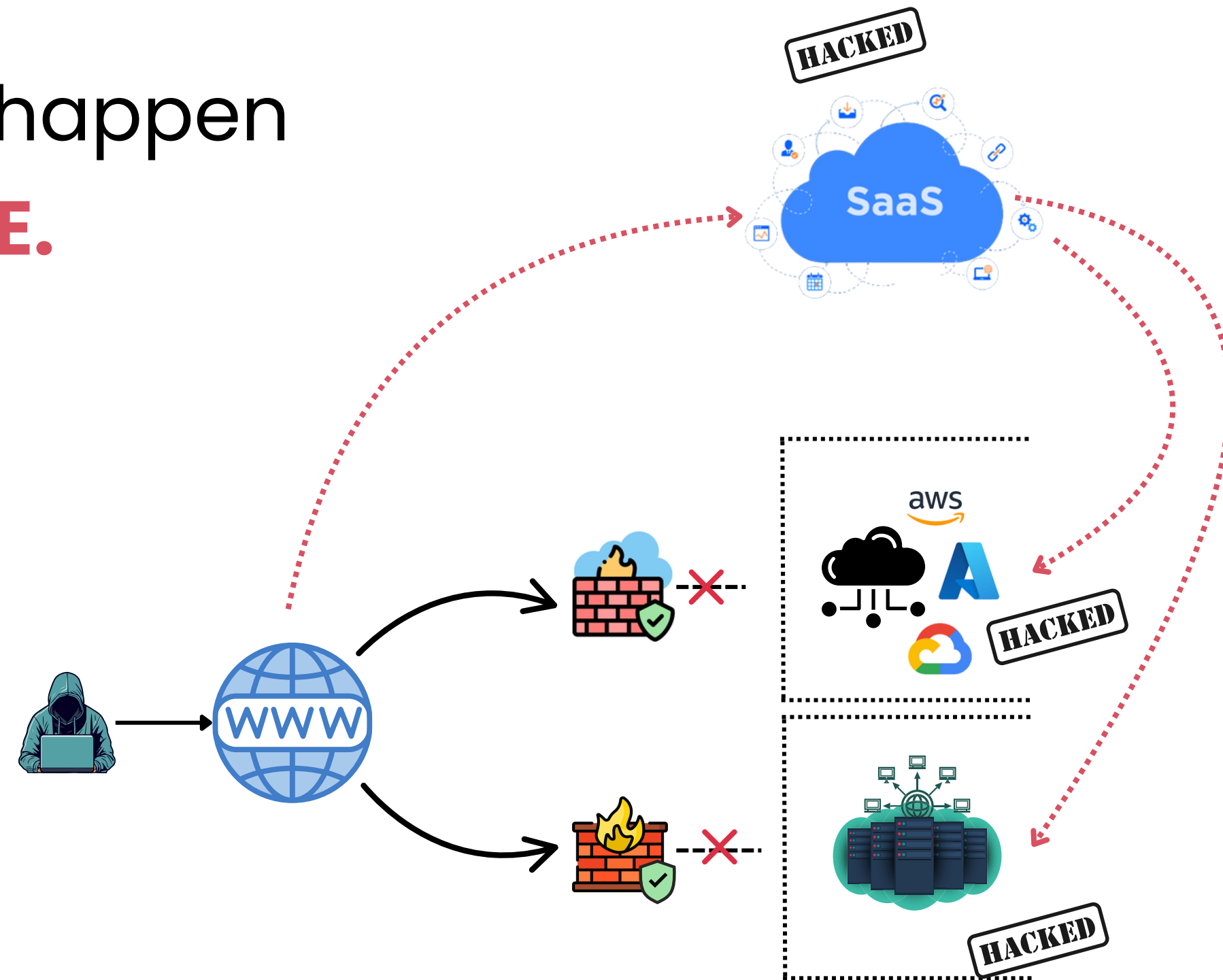
- On-Prem Infra
- Cloud Infra
- Hybrid Environment



Firewalls **CAN'T** do, what?

Monitor or prevent attacks that happen
OUTSIDE YOUR INFRASTRUCTURE.

- SaaS
- Shadow SaaS
- Public Link Sharing
- Public Source Code Repos



SaaS

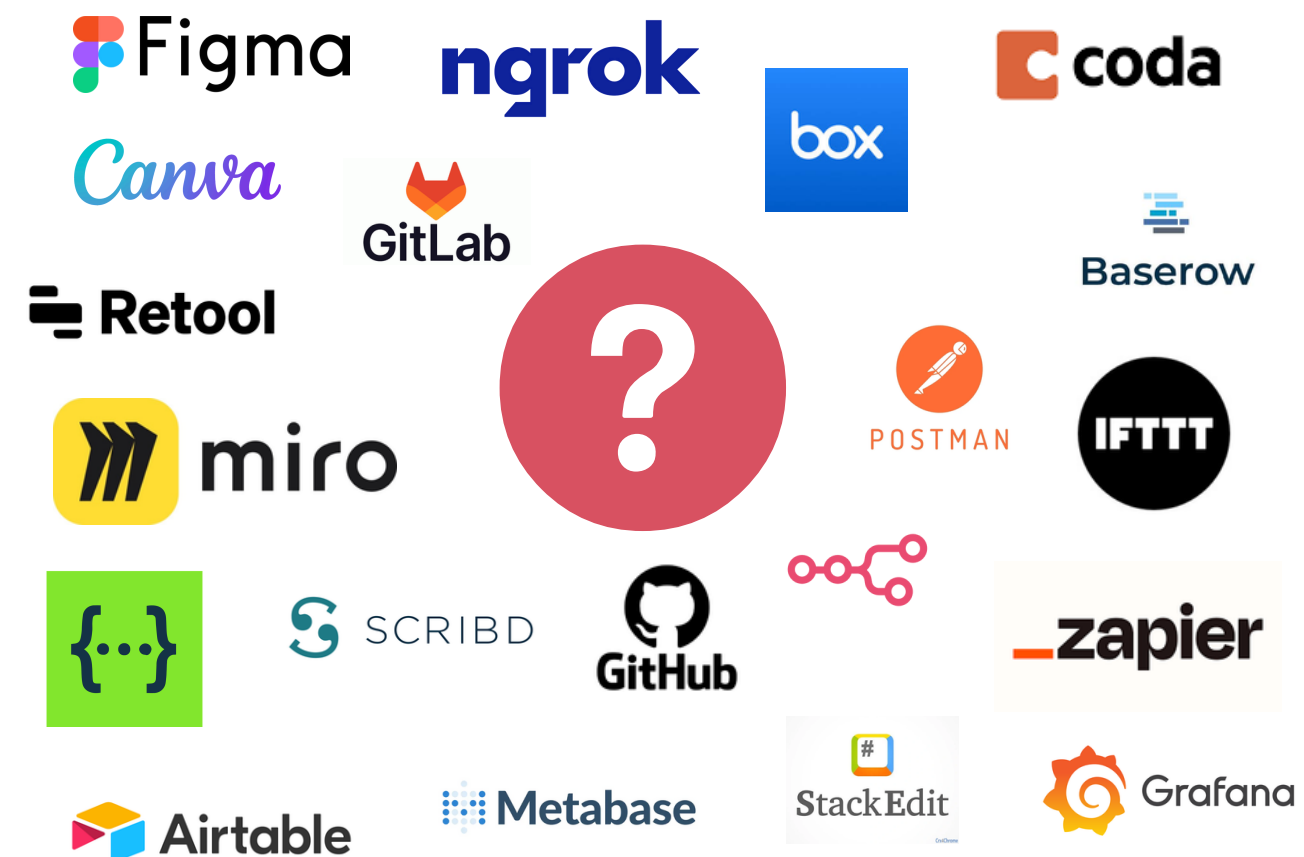
What You Know You Are Using



- **Known to IT & Security**
- Can be Integrated with SSO / IAM
- Org-approved tools: Google Workspace, Salesforce, Slack
- Covered by vendor agreements and controls
- **Moderately Difficult** to Track and Monitor

Shadow SaaS

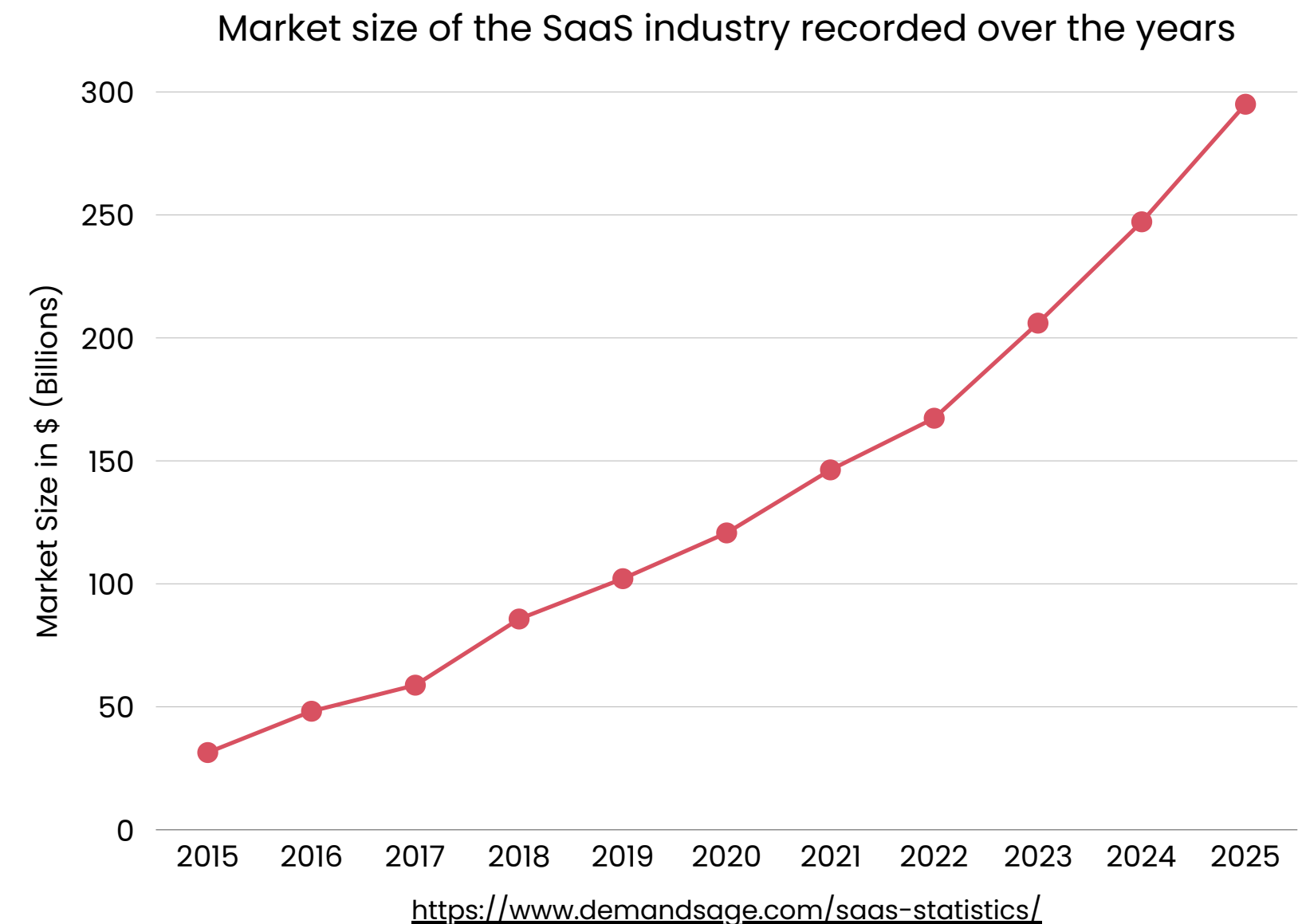
What You Don't Know You Are Using



- **UnKnown to IT & Security**
- No SSO, no approval, no visibility
- Set up by users or teams, outside IT
- Public links, tokens, and credentials are often exposed
- **EXTREMELY Difficult** to Track and Monitor

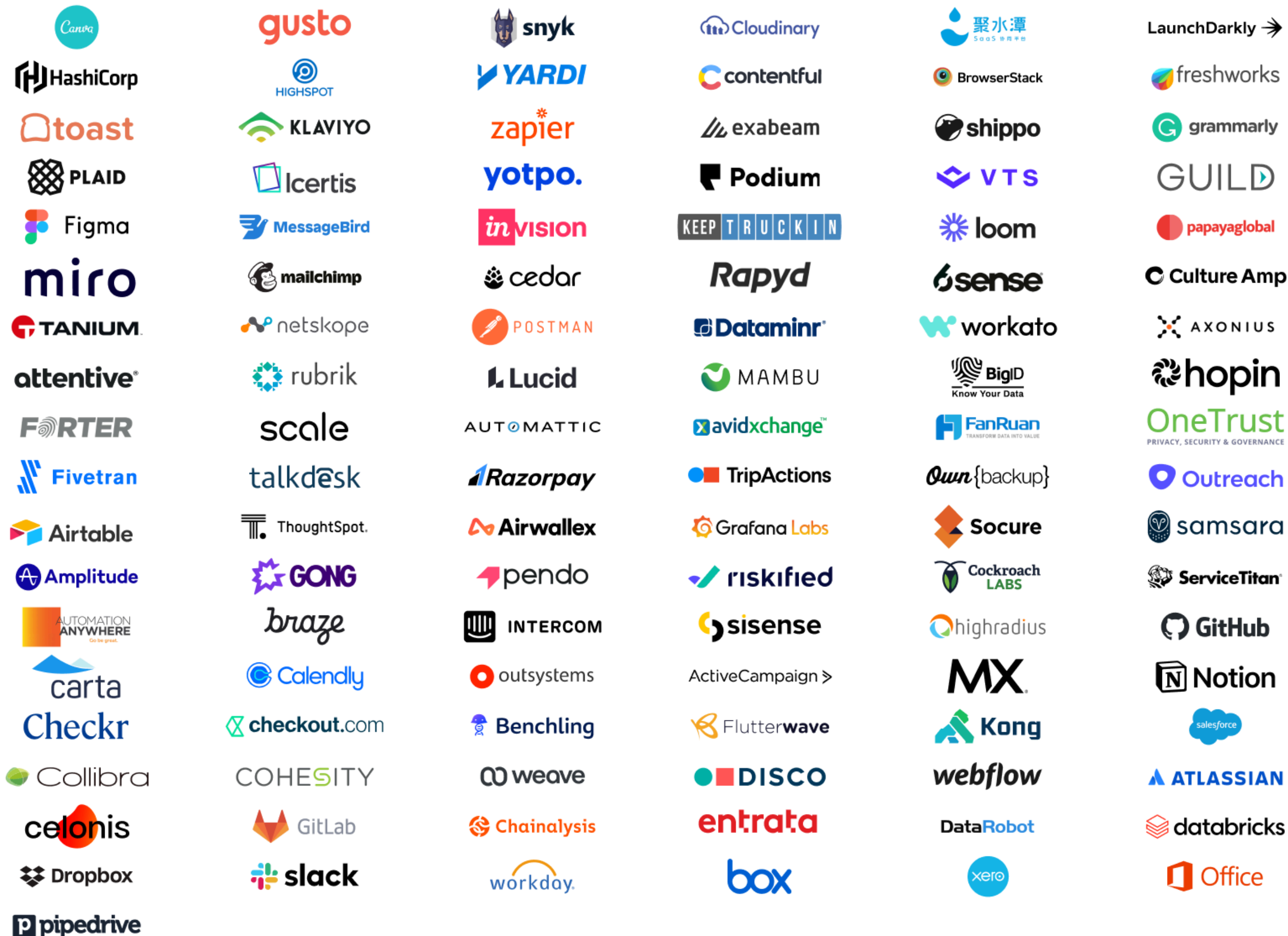
Scale of Usage?

- 95% of organizations use SaaS in their operations – (SC Magazine)
- 275 SaaS apps on average, but 53% of licenses go unused within 30 days (Zylo)
- SaaS apps contribute roughly 30% of the worldwide public cloud spending
- 65% of SaaS apps are unapproved by IT – No Visibility (Trellica)
- **55% of companies have experienced a SaaS security incident (SC Magazine)**





If You Haven't used
any of these?



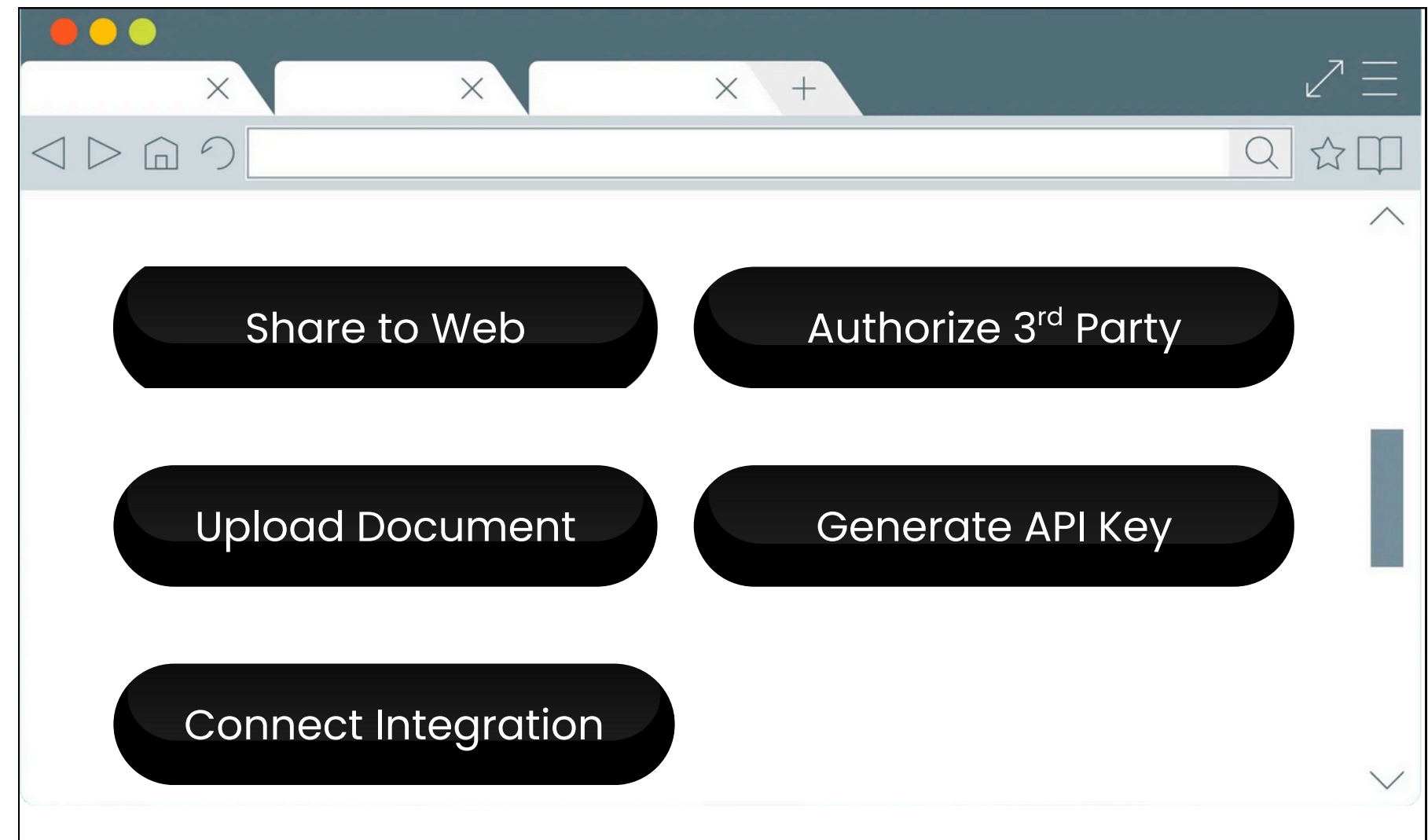


Shadow SaaS is Dangerous

- Uncontrolled Access & Low Visibility
- Public by Nature (Access controls are added)
- Persistent After Offboarding
- No Security Review
- Don't even touch your Network/Firewalls

The Threat Isn't Advanced. It's Ambient.

- No APT, no nation-state actor.
- A link shared without thinking.
- A token stored in a harmless-looking tool
- A SaaS app doing exactly what it was told to do, just publicly.



Decisions Made at the Browser Level are EASY BUT RISKY

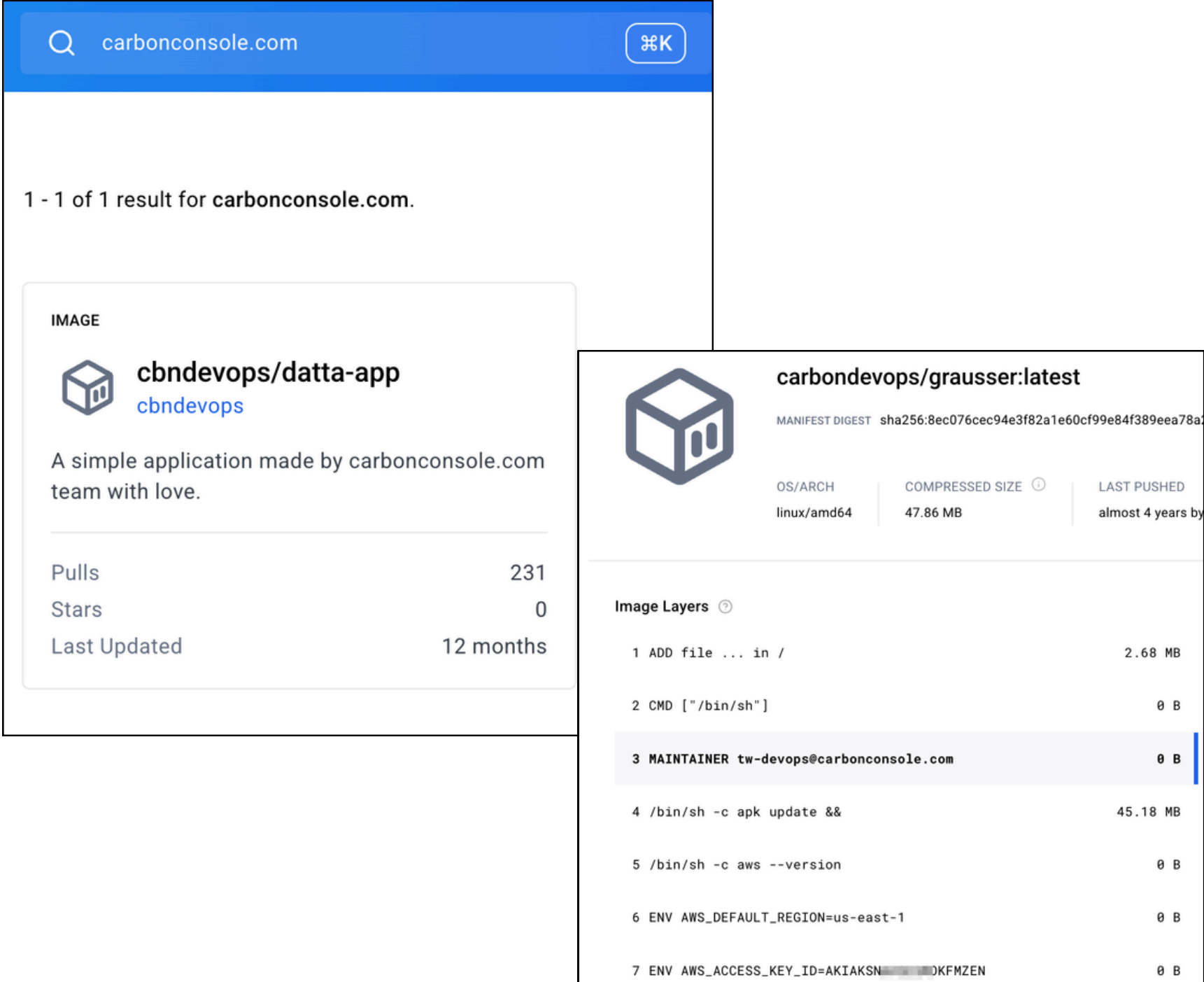
- web.archive.org/cdx/search/cdx?url=grafana.net&matchType=domain&fl=original...
- https://grafana.net/ws/?EI0=3&transport=polling&t=LV07xrS
https://grafana.net/ws/?EI0=3&transport=polling&t=LV08AiQ
https://a4smonitor.grafana.net/
http://abdimakonenchoroke.grafana.net/
http://abegel.grafana.net/
http://aborruso.grafana.net/robots.txt
https://acoustid.grafana.net/api/plugins/grafana-investigations-app/settings
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1710406
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1710448
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1715660
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1730693
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1731358
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1731420
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1731420
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1731427
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1731429
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1731441
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1732821
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1734085
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1734092
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1734796
https://acoustid.grafana.net/api/public/dashboards/1249b428418a494daf09e38d6f331d92/annotations?from=1734904

URL	Time	Response
TXT uber.com	5 min	"f621e431-a485-4094-8587-2f76f441ccab"
TXT uber.com	5 min	"facebook-domain-verification=fgnbsxqefh2pzugz14vcw82ylgagg"
TXT uber.com	5 min	"google-site-verification=9kww-dlf_5X0t8aHfK2xK-Cowpra8nHbfTRCa7HbK0"
TXT uber.com	5 min	"google-site-verification=bywbMPdGdGaSev-nAuHwbdYJziw9oPeGok8D5UyK0"
TXT uber.com	5 min	"google-site-verification=p2laddAHCIL7lBqVhN6P3leJNO2ob8edJtqICdXCj8"
TXT uber.com	5 min	"google-site-verification=yHvJ7x6qUkjrRfaPzS051u4270uSS0Q88xPFbBSU"
TXT uber.com	5 min	"mandrill_verify.5QnmY5yhD4mJwXJ0VP7w"
TXT uber.com	5 min	"mandrill_verify.UYz1FL51N9Ky3RCgCUZGQ"
TXT uber.com	5 min	"mixpanel-domain-verify=a35ee3f7-3848-4a0b-822e-d429b507c0c6"
TXT uber.com	5 min	"notion-domain-verification=ReKaEX54F5cGF2P3IKgylP2F7tjQ34Iua63ng0LHDC"
TXT uber.com	5 min	"openai-domain-verification=dv-wtb3V1y0DtnGs1QN4Dn24c7"
TXT uber.com	5 min	"paloaltonetworks-site-verification=f567a8ba5a35da704fble540c1e50bbaa33bc2ea6b87193c22e1c9a"

The image is a screenshot of a search engine results page. At the top, a search bar contains the text "site:grafana.net inurl:public-dashboards". Below the search bar, there are navigation tabs: "All", "Images", "Videos", "News", "Shopping", "Short videos", and "More". The "All" tab is selected. Below the tabs, there are three search results. Each result starts with the Grafana logo, followed by the word "Grafana". Below that is a snippet of a URL: "https://optimistic.grafana.net > public-dashboards". The first two results have a purple URL snippet: "https://optimistic.grafana.net/public-dashboards/c...". The third result has a blue URL snippet: "https://scada100relab.grafana.net/public-dashboards...". Below each URL snippet is the text "No information is available for this page." and a link that says "Learn why".

Finding SaaS is **NOT** EASY.

- No Public URL Structure (most of the time)
- Behind Authentication
- No Public Discovery Features
- No Direct Relation to Target Org
- Not available on Shodan / Censys
- Search is never exhaustive.
- **How to find them all? You may ask.**




The screenshot shows a search for 'carbonconsole.com' on Docker Hub. The search results page displays '1 - 1 of 1 result for carbonconsole.com.' Below this, there are two main entries. The first entry is 'cbndevops/datta-app' by 'cbndevops', described as 'A simple application made by carbonconsole.com team with love.' It shows 231 pulls, 0 stars, and was last updated 12 months ago. The second entry is 'carbondevops/grausser:latest' by 'carbondevops', showing a manifest digest, OS/ARCH (linux/amd64), compressed size (47.86 MB), and last pushed almost 4 years ago. Below this, the 'Image Layers' are listed, including 'ADD file ... in /' (2.68 MB), 'CMD ["/bin/sh"]' (0 B), 'MAINTAINER tw-devops@carbonconsole.com' (0 B), and several environment variables and commands.

carbonconsole.com

1 - 1 of 1 result for carbonconsole.com.

IMAGE

 **cbndevops/datta-app**
cbndevops

A simple application made by carbonconsole.com team with love.

Pulls	231
Stars	0
Last Updated	12 months

carbondevops/grausser:latest

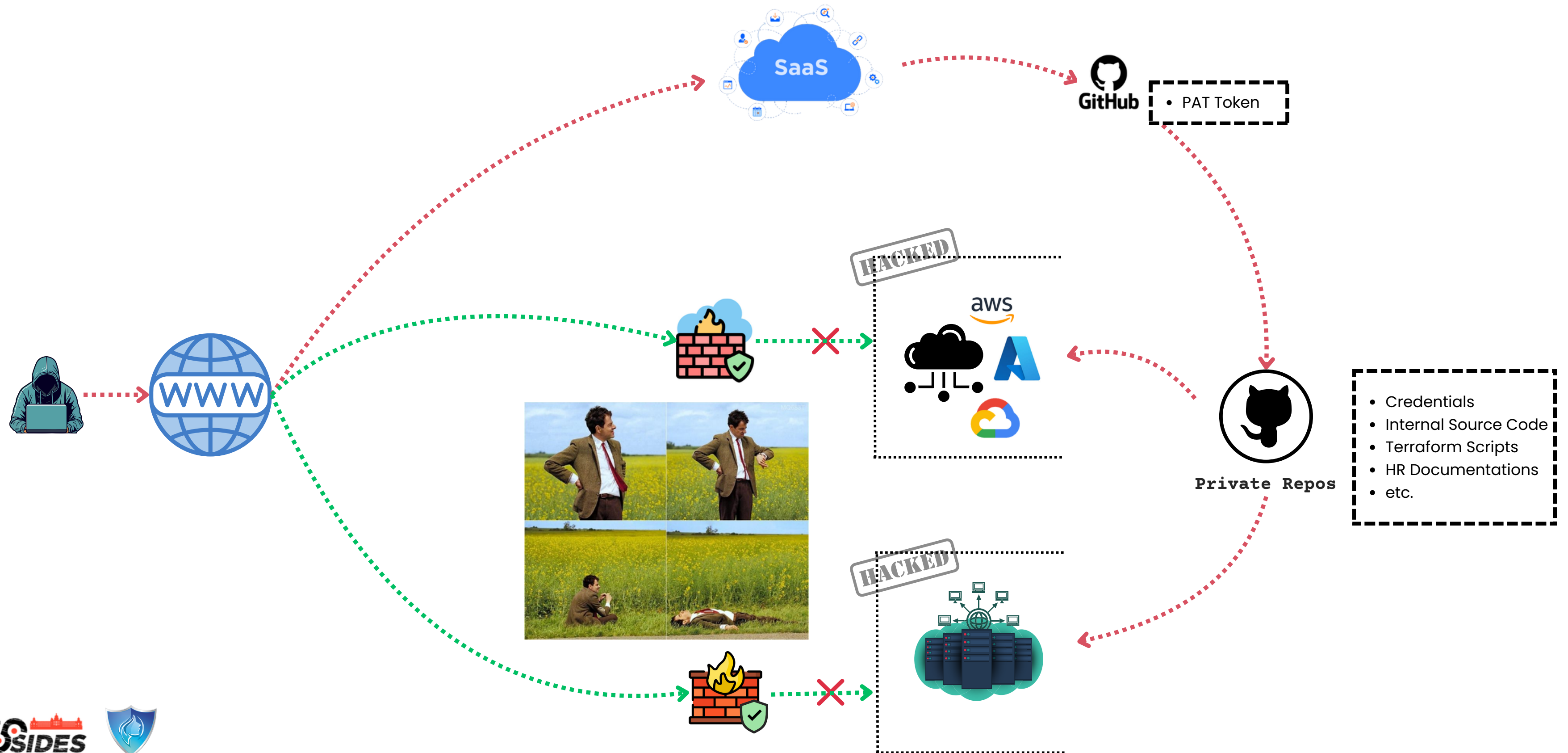
MANIFEST DIGEST sha256:8ec076cec94e3f82a1e60cf99e84f389eea78a

OS/ARCH	COMPRESSED SIZE	LAST PUSHED
linux/amd64	47.86 MB	almost 4 years by

Image Layers

1 ADD file ... in /	2.68 MB
2 CMD ["/bin/sh"]	0 B
3 MAINTAINER tw-devops@carbonconsole.com	0 B
4 /bin/sh -c apk update &&	45.18 MB
5 /bin/sh -c aws --version	0 B
6 ENV AWS_DEFAULT_REGION=us-east-1	0 B
7 ENV AWS_ACCESS_KEY_ID=AKIAKSN...	0 B

Why No Visibility



Real World Example






How a mistakenly published password exposed Mercedes-Benz source code

Mercedes accidentally exposed a trove of sensitive data after a leaked security key gave “unrestricted access” to company’s source code.

 TechCrunch / Jan 26, 2024

Real-World Scenarios

Off the Infra - Attack Path Examples

-  **Airtable** Airtable Link → Shared Publicly → Google-Indexed → PII Leak
-  **POSTMAN** Postman Collection → Environment Variable → API Token → Unauthorized Access
-  **Retool** Old Retool Link → No Auth → Still Live → Data Access
-  **Figma** Figma File → Public Design → Published API Key → Cloud Infra Breach
-  **Notion** Marketing shares Notion doc → “Anyone with the link” → Leaked via Slack snippet → Indexed → Sensitive roadmap exposed.

Most Incidents Are not Breaches Anymore

They didn't break in.
They just clicked a public link.

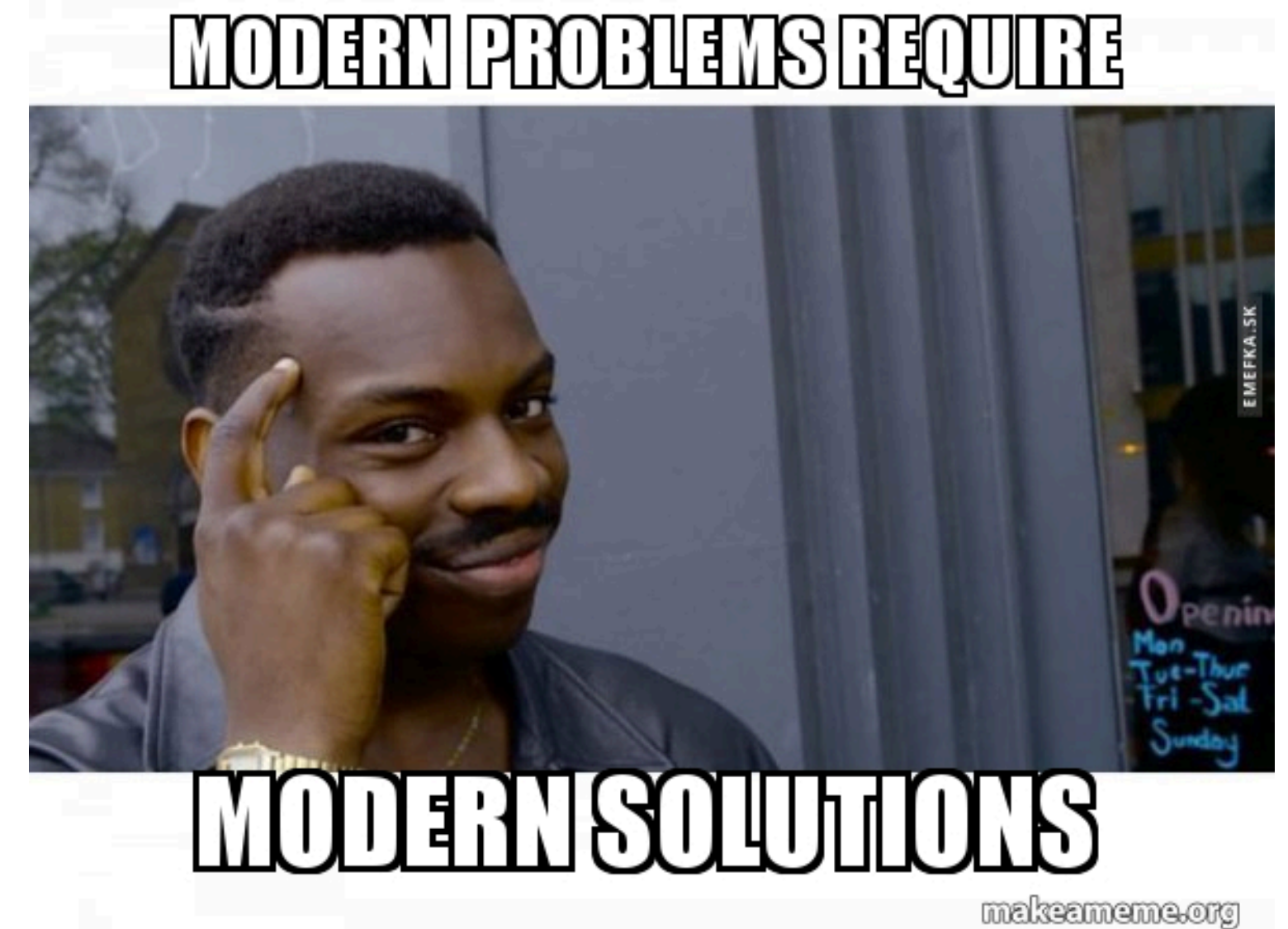
 *No firewalls were alerted in the making of this breach.* 

Problem with Traditional Defences



Solution

- Accept That You Can't Block It. Start Mapping It.
- Reducing unmanaged exposure, continuously
- Monitor for Insecure Defaults
- Implement Token Hygiene at the Org Level
- Implement Secret Management
- Educate the Right People (Hint: Not Just Engineers)
- Detect Misuse Using Passive Signals



Solution

Defensive Strategy – Visibility First

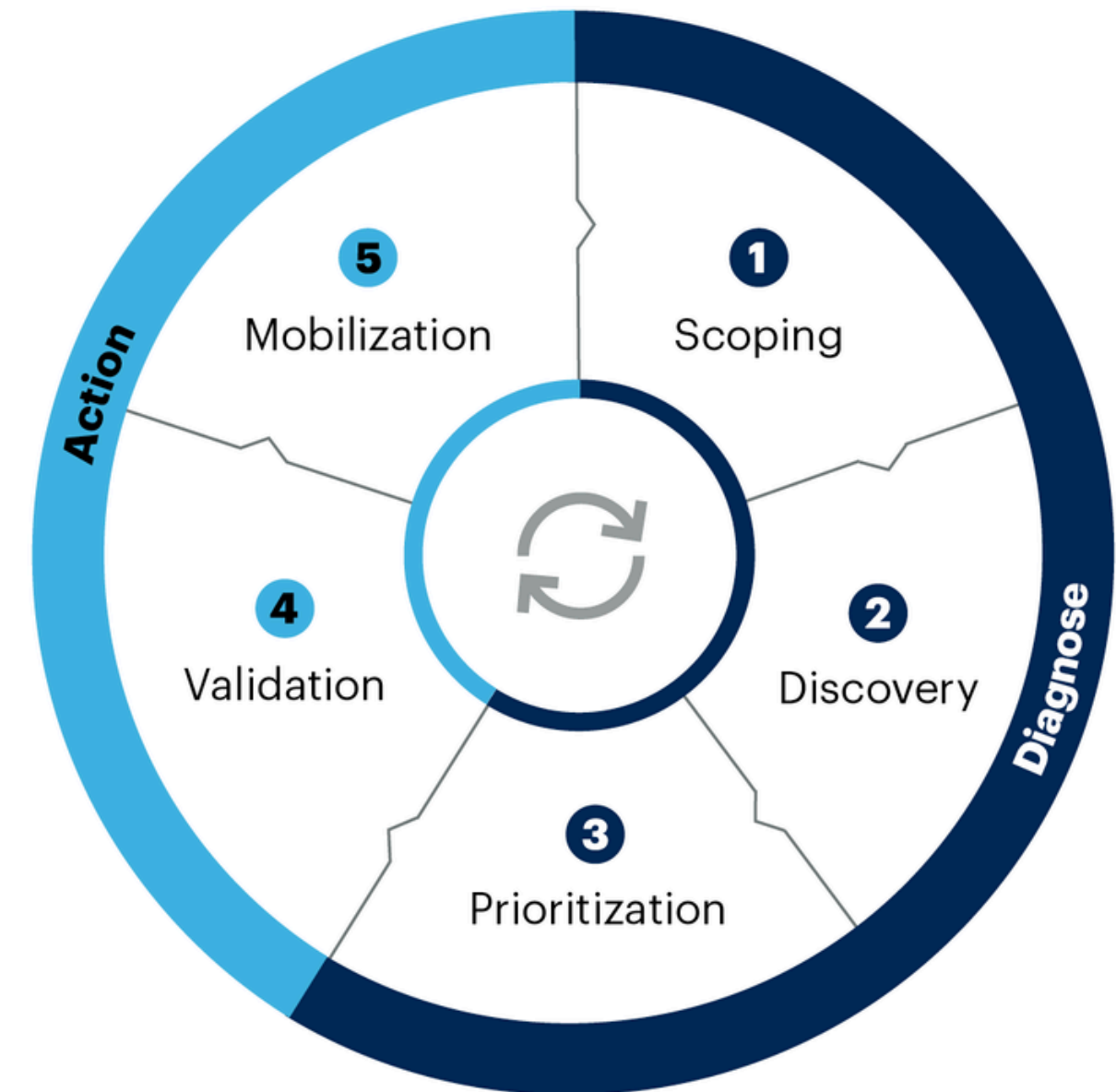
- Enumerate OAuth-connected apps across GSuite/O365
- Monitor public-sharing features (Sheets, Notion, Postman)
- Detect usage of unapproved SaaS via DNS/proxy/SASE logs
- Identify tools that contain secrets, access tokens, and customer data

Defensive Strategy – Configuration & Policy

- Disable public link sharing by default
- Enforce token expiration & rotation
- Limit OAuth scopes where possible
- Remove stale/unused integrations automatically

Defensive Strategy – Offboarding and Lifecycle

- Auto-expire tokens on user offboarding
- Alert on SaaS apps still tied to deactivated users
- Clean up orphaned assets periodically (e.g., shared docs, forms, scripts)



Source: Gartner

TL;DR

Shadow SaaS is everywhere – unapproved, unmonitored, and holding real data.

These apps live outside your perimeter

They hold tokens, PII, credentials, sensitive documents, and automation logic, with zero monitoring

You can't block it ALL. But you can map it, monitor it, and reduce risk

You don't need to **block** everything. You need to **know** everything.

Your Firewall is Not Broken.

It's Blind.



REDHUNT LABS

DISCOVER. ATTACK. REPEAT.

360° External Security Platform

CTEM | EASM | TPRM | CSPM | DRPS

Questions?

Thanks.

Email Address

shubham@redhuntlabs.com

Website

redhuntlabs.com