wallarm

DATA SHEET

PRODUCT DATA SHEET

Wallarm Infrastructure Discovery

Find everything in AWS. Know the moment it changes. Stay ahead of what's exposed.

SUMMARY

You probably have more in AWS than you think.

Across more accounts than your static inventory lists, in regions nobody thought to check, running services nobody approved. Wallarm Infrastructure Discovery gives you the complete picture: a live inventory of your entire AWS estate, immediate alerts when anything changes, and context that makes Security Hub findings actionable — placed on the exact asset they describe, with attack-path analysis that shows you what's actually reachable.

One inventory your security, platform, and audit teams can actually trust.

1	**0**	**10k+**
INVENTORY ACROSS EVERY ACCOUNT	AGENTS INSTALLED IN YOUR WORKLOADS	RESOURCES MAPPED PER ESTATE

OVERVIEW

Your AWS estate, mapped and watched — continuously.

Connect your AWS accounts once. Infrastructure Discovery inventories everything across every account and region you register, builds a live relationship map, tracks every change scan-to-scan, and places Security Hub findings on the exact asset they describe. Read-only by default. No agents in your workloads. No DevOps tickets to file.

THE WALLARM AI CONTROL PLATFORM

DISCOVERY IS THE TERRITORY MAP

PRODUCT 01
Infrastructure Discovery

PRODUCT 02
AI Hypervisor
RUNTIME AI BEHAVIOR, KERNEL-LEVEL ON EKS

KNOWS
What exists. What changed. Where findings go.

MAKES POSSIBLE
Scope-able AI Hypervisor deployment across the full AWS estate the cluster connects to

Infrastructure Discovery reads your AWS estate across every account and region you point it at, captures resources and the relationships between them, diffs each scan against the last, and ingests AWS Security Hub findings against the assets they describe.

Built for production AWS estates. Read-only by default: all collectors call AWS Describe and List APIs only.

SSO, cross-account roles with external IDs, static access keys, and Vault-backed credential storage — pick what each account allows. Azure CLI and service principal credentials are accepted as operator auth methods (not Azure estate scanning).

WHO IT'S FOR

AUTHORITATIVE ANSWER
Security
- What runs in AWS, who owns it, what changed — without standing up a CSPM project.

READ-ONLY ROLE
Platform / SRE
- A tool deployable with a Describe/List role, not the keys to the kingdom.

EVIDENCE TRAIL
Compliance
- Every finding, policy action, and resource change — timestamped and attributed.

CHALLENGES

Real problems. Concrete answers.

#	WHAT WE HEAR	WHAT INFRASTRUCTURE DISCOVERY DOES
01	"I don't actually know what we have in AWS."	Complete inventory of EC2, VPCs, IAM, Lambda, API Gateways, load balancers, EKS, and Bedrock resources — across every account and region you've registered. Continuously refreshed. "We'll get back to you" is no longer an acceptable answer.
02	"What changed since last week?"	Every scan diffs against the prior one. Field-level drift events surface with severity, before-and-after values, and CloudTrail attribution to whoever made the change.
03	"Security Hub fires alerts. We can't tell what they mean."	Findings from GuardDuty, Inspector, IAM Access Analyzer, Macie, and AWS Config are placed on the asset they actually affect — with full relationship context and plain-language descriptions. Every triage decision is logged for audit.
04	"A CVE dropped. I need to know our internet-exposed surface right now."	Attack-path analysis traces the route from every internet gateway through security groups and load balancers to the workload behind them. Built-in rules flag exposed resources automatically. No grepping CloudFormation templates, no asking each team.
05	"Our cloud map is out of date the moment we publish it."	There's no diagram to maintain. The inventory is the map, rebuilt from AWS on every scan. On-demand scans are a single click.
06	"Security, platform, and audit teams all want a different view of the same cloud."	One backend, multiple views: asset browser, relationship graph, drift stream, findings triage, and policy audit log. One source of truth for all three teams.

BENEFITS

For the three teams that share AWS.

FOR SECURITY

Current. Connected. Confident.

- Stop answering board questions with "we'll get back to you."
- Security Hub findings with full asset context — not just ARNs and account IDs.
- Know about configuration changes before they cause incidents or fail audits.
- Read-only posture that survives any security review.

FOR PLATFORM / SRE

One agent. Zero friction.

- One account onboarding. Every region covered from there.
- Flexible auth: SSO, cross-account role, access keys, Vault-backed.
- Attack-path and blast-radius analysis for on-call engineers — answer the question without reconstructing it by hand.
- REST API for every integration you actually want to build.

FOR COMPLIANCE

Evidence you don't have to build.

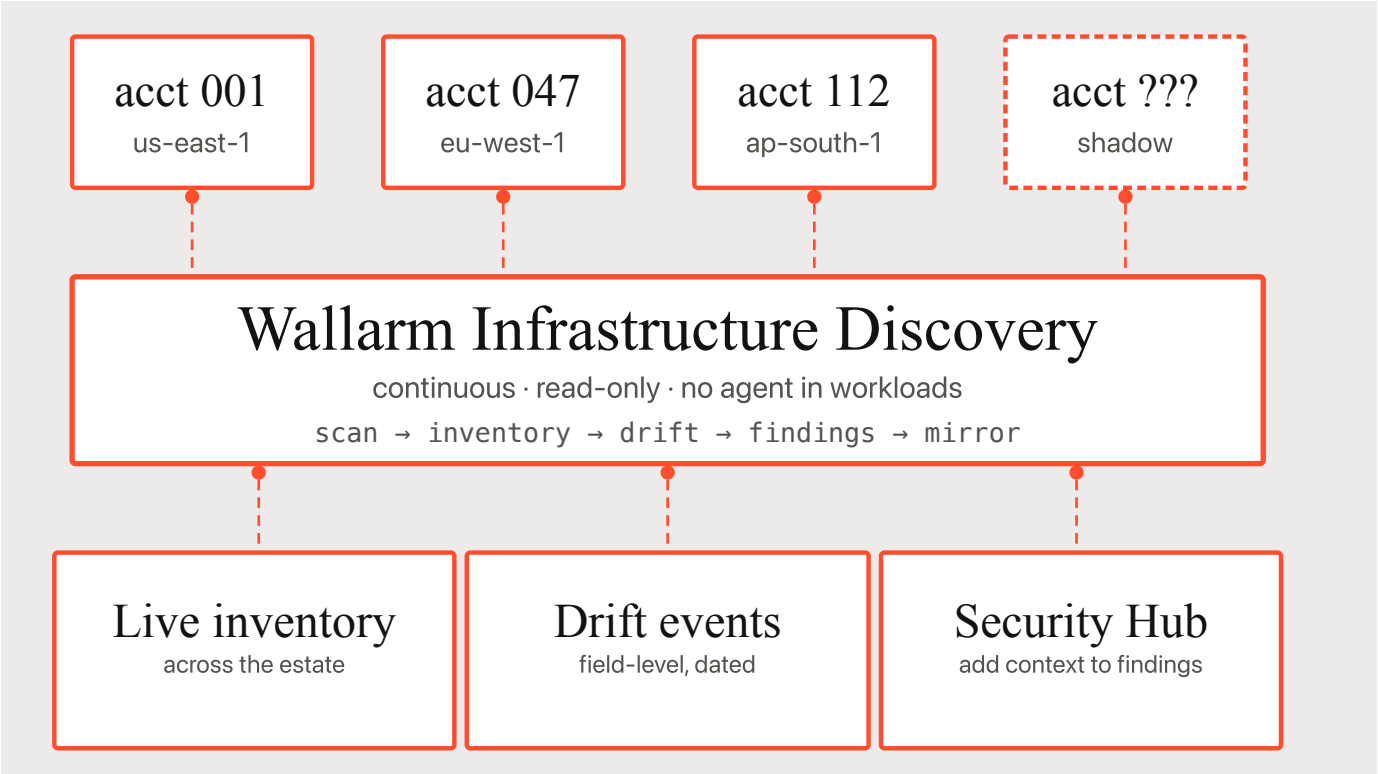
- Audit-ready trail for every finding, policy action, and retired resource.
- Policy audit log: every dismiss, downgrade, upgrade, and annotation, timestamped.
- Read-only IAM scope you can hand to an auditor and defend.
- Customer-defined and built-in rules, visible side by side.

SOLUTION

One agent. Everything it finds.

Point it at your accounts. It handles the rest.

Infrastructure Discovery connects to your AWS accounts through a read-only IAM role — no agents in your workloads, no changes to your applications. On the schedule you set, it scans every account and region you've registered: building a live inventory of what exists, comparing each scan to the last to surface what changed, attaching Security Hub findings to the assets they actually describe, and surfacing attack paths from internet gateways to workloads. By the time you open the console, the picture is already there.



NEXT STEP

See your AWS the way attackers already do.

A 30-minute walkthrough on your actual stack — accounts, regions, findings already in Security Hub. No agents to install before the call.

Try for Free →

WALLARM.COM / REQUEST-DEMO —— 30 MIN · LIVE