personam
AI Cyber Threat Hunter

Detect the threats your tools never see.

Behavior-based NDR that finds active attackers, compromised credentials, and insider threats — **fast, with near-zero false positives and zero endpoint agents**.

100% network coverage. Minutes-to-value.
Actionable alerts that tell your team exactly where to act.

- Deploys in hours — start detecting without agents or rules.
- Psychometric AI compares user, device, and host behaviors to their peers — catches low-and-slow attacks.
- Low noise, high confidence — <5 alerts per 1,000 devices per week.

Get a free 30-day pilot. personam.ai | sales@personam.ai | (703) 249-9585

The Problem

Modern defenders face three hard truths:

- Signature and rule-based tools miss novel and AI attacks and abused legitimate services.
- Endpoint agents can't monitor BYOD, IoT, or unmanaged medical/OT devices.
- SOCs drown in noise and never focus on the few things that matter.

The Solution

Personam turns that around by providing continuous, network-based behavioral monitoring that:

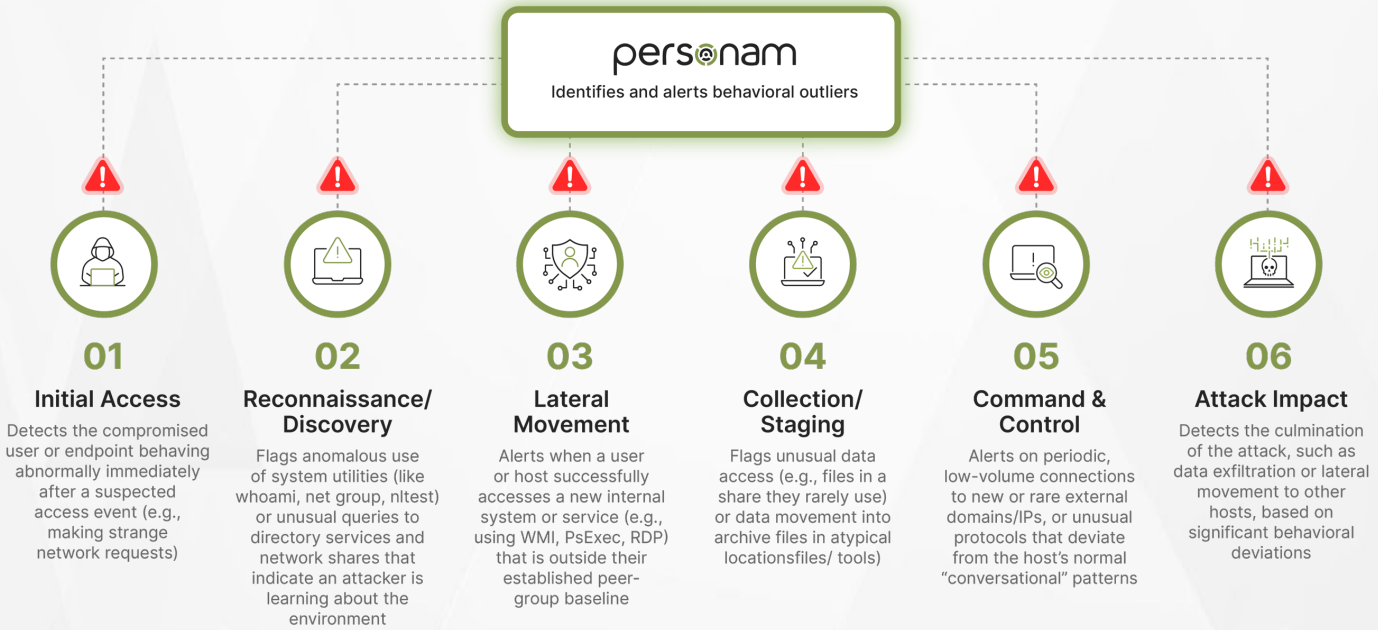
- Detects compromised credentials, active malware, AI attacks and insiders without signatures.
- Exposes data-leakage and misconfigurations that look "normal" to legacy tools.
- Cuts analyst time-to-investigate and eliminates alert fatigue.

PROOF POINTS

Time to detect:
<5 minutes

Time to respond:
<15 minutes

False positives:
<2%



Mapped across the kill chain — Personam flags every stage.

Behavior first. Evidence always.

Personam builds dynamic psychometric profiles for every entity on your network — users, devices, and hosts — and compares them to their peers. We then **surface the high-risk behaviors and package them as a single, actionable investigation for SOC teams**.

Lightweight collection

- **Input**: NetFlow, VPC flow logs, DNS, optional Syslog/auth events. No agents required.
- **Coverage**: East-west and north-south, cloud and on-prem, BYOD and IoT.

Psychometric AI

- We extract hundreds of attributes per session and cluster entities into cohorts.
- **Dual detection model**: out-of-character (historical change) + out-of-family (peer divergence).
- **Continuous, unsupervised learning** — no models to tune, no rules to write.

Actionable outputs

- Ranked threat list (dynamic threat score).
- **Forensics toolkit**: outlier transactions, staging/exfil targets, filenames (when available), and timeline.
- **Integrations**: Export alerts via CEF/Syslog, email, API, or SIEM/SOAR connectors.

How it helps SOC Teams

- Prioritize the 2–3% of entities that matter.
- Reduce false positives to <2% typical in pilots.
- Rapid triage: click from alert → entity profile → outlier transaction

Personam caught a nation state hack at reconnaissance/delivery stage, without any rule sets, within minutes of the attack starting.

Get a free 30-day pilot. personam.ai | sales@personam.ai | (703) 249-9585

Features that matter

- **Agentless, metadata-first detection** — works on encrypted networks.
- **Peer-aware threat scoring** — context reduces false alerts and surfaces real risk.
- **Fast time-to-value** — actionable signals within hours, stabilized profiles in days.
- **Forensics without packet capture** — metadata yields filenames, volumes, destinations when available.
- **Flexible operations** — cloud SaaS, multi-tenant MSP/OEM, or on-prem/bare-metal detectors.

Deployment models

On-prem Virtual Appliances

- Zero-touch install < 30 minutes
- Learns users/hosts automatically
- Zero network redesign

Software-as-a-Service

- Browser-deploy, < 30 minutes
- One console, unified view
- No server setup

Hybrid

- Plug-in VM or cloud install
- Zero-touch, < 30 minutes

Typical use cases

- Compromised credentials and account takeover
- Ransomware, AI attacks and persistent threat detection
- Data leakage and configuration error discovery (e.g., misconfigured servers)
- IoT/OT visibility for healthcare, manufacturing, and critical infrastructure
- Insider threat detection and litigation support

Integration & Specs

- **Inputs**: NetFlow/IPFIX, VPC Flow Logs, DNS, optional Syslog/SIEM feeds
- **Outputs**: CEF, Syslog, Email, API, SIEM connectors
- **Scalability**: detectors support tens of thousands of nodes (architecture scales via federation)
- **Privacy**: metadata-based detection — payload inspection only when traffic is unencrypted and needed for forensics

See Personam in your network. Start a pilot today — contact sales@personam.ai or schedule a technical call at personam.ai/demo