DemandFlow Sense

DEMANDFLOW®

Sell network sensing as a service on 5G-Advanced today and carry it into 6G

DATA SHEET

Wi-Fi gateways and 5G-Advanced radios can now sense the physical world: the presence and movement of people, a fall in a care home, a crowd building in a plaza, a drone approaching a perimeter. Integrated sensing and communication is a headline capability planned for 6G, and 5G-Advanced is its first step. The capability is arriving in the network faster than the means to sell it, and the operators who learn to sell it on 5G-Advanced will be the ones ready to sell it on 6G.

A detection is not a product. An enterprise customer buys an area covered to an agreed standard, at an agreed price, with evidence that the standard was met and that personal data was handled lawfully. Delivering that today means:

- no catalogue, tiers or prices to quote from, so every deal is a custom project;
- no check that the sites, antennas and backhaul can actually serve the zone before it is sold;
- no measurement against the tier the customer bought, so the SLA is a promise rather than a record;
- consent, retention and DPIA paperwork kept by hand, lagging the service and leaving the DPO carrying the risk;
- charges and service credits worked out in spreadsheets at month end.

What DemandFlow Sense is

DemandFlow® Sense is the sensing service management layer of the DemandFlow platform. It turns the detections your radios and gateways produce into a service you can sell, deliver, prove and govern: a priced catalogue, customer zones drawn on the map, feasibility against the real inventory, consent built in, KPIs measured every 15 minutes, incidents, charges, a customer portal, an API and signed webhooks.

DemandFlow does not perform the sensing. Your sensing sources detect; DemandFlow runs the business around the detections. Sources connect through adapters that share one common interface, so the service you sell does not depend on any one vendor or radio generation.

What an operator gets

- **A head start on 6G.** Integrated sensing and communication is a headline 6G capability. Build the catalogue, win the customers and prove the service on Wi-Fi and 5G-Advanced now; the same catalogue, zones, consent records and SLA history carry into 6G, through an adapter interface designed for 6G sensing functions.
- **A sellable sensing catalogue.** Six product families with priced KPI tiers: detection probability, false alarms, position accuracy, alert latency, update interval and availability.
- **Zones drawn on the map.** Each customer zone drawn over your real sites, carrying its client, product, tier, contract dates and price.
- **Feasibility before you quote.** Every zone checked against the sites, antennas, timing and backhaul in the inventory, with the sources that can serve it and the mode they would run in; re-checked when the network changes.
- **Consent and governance built in.** A human-sensing zone cannot be submitted without purpose, lawful basis, retention and DPIA status. Retention is enforced with a deletion log, there is a governance register, and a signed regulator bundle per zone.
- **Live delivery from your sources.** Adapters for Wi-Fi gateway clouds and 5G-Advanced sensing functions, plus a simulator so the service can be built, sold and demonstrated before the radios are live.
- **Provable SLAs.** Every active zone measured against its tier every 15 minutes; a sustained breach opens an incident on the SLA clock automatically and notifies the customer.
- **Revenue without spreadsheets.** Monthly charges per zone, pro-rated from activation, service credits from time in breach, revenue by product family and a contracted forecast.

Because Sense runs inside DemandFlow, it uses the sites, antennas, devices, links, clients, contracts, tickets, changes and finance records the platform already holds. A sensing zone is checked against the same inventory your network team maintains, a breach opens the same kind of ticket your operations team already works, and a charge reaches the same finance module as every other service.

- **For the end customer.** A customer portal with zones, KPI history and a monthly service report; a REST API; signed webhooks for alerts.

How it works

Sense is organised as a flow from order to charge. Sensing sources connect through adapters; the Sense core manages the catalogue, zones, feasibility, governance, assurance and charging on top of the DemandFlow inventory; and the results reach your customers, your operations team and your finance team through the outputs on the right.

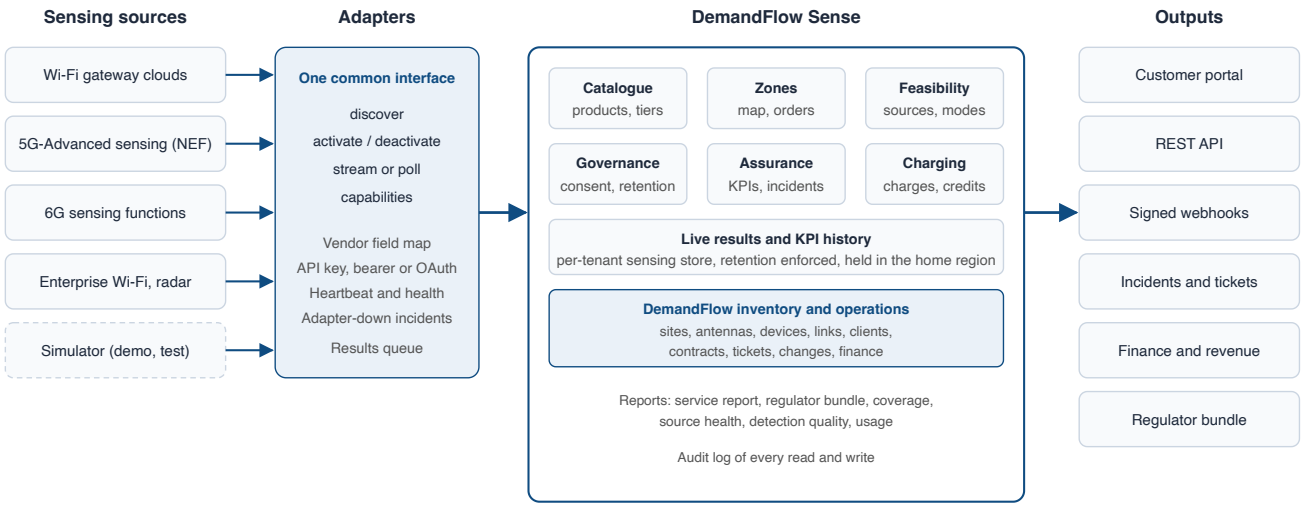


FIGURE 1. DEMANDFLOW SENSE: SOURCES, ADAPTERS, THE SENSE CORE ON THE DEMANDFLOW INVENTORY, AND OUTPUTS

Adapters: how sensing sources connect

An adapter is the connector between DemandFlow Sense and one sensing system. Every adapter implements the same small interface, so the Sense core never sees vendor detail: it asks an adapter to **discover** the sources it can reach, to **activate** a sensing task for a zone (and later deactivate it), and to deliver results either by **stream** (push) or by **poll** (pull). An adapter may also answer a **capabilities** query with its live figures for a source, which feasibility uses in place of the stored KPI model. A new vendor is a new adapter, not a new product.

Each adapter is a record in the tenant's own DemandFlow, with its endpoint, authentication and vendor field mapping held as configuration. Credentials are stored encrypted and are never logged. The adapter runtime runs on a schedule, one isolated run per adapter per tenant, so one vendor's outage or slowness never touches another. It activates requested tasks, pulls or receives results, records a heartbeat, keeps the adapter's health status (Up, Degraded, Down) and raises an incident when an adapter goes down.

Adapter type	What it connects	How it works
Gateway vendor cloud	Wi-Fi gateway sensing clouds: home and small-business gateways whose vendor offers a cloud API for presence, motion and fall sensing.	Generic REST connector. The vendor's endpoint, the paths to list sources, start and stop a task and fetch results, and a JSON field map from the vendor's records to the common shapes are entered as configuration when a vendor signs, not written as code. Pulls results on a cursor. Authentication: none, API key in a header, bearer token or OAuth 2.0 client credentials.
5G-Advanced sensing function	The operator's sensing function (SenF) reached through the network exposure function (NEF), on 5G-Advanced gNB cells.	DemandFlow acts as the application function: it subscribes to a sensing service for the zone through the NEF, and results arrive by push notification to a DemandFlow endpoint. Built on the published NEF northbound pattern (TS 29.122 and 29.522), the geographic area shapes of TS 23.032 and the Release 20 integrated sensing study. Message names are provisional until the operator's API is confirmed; a pilot needs an endpoint, an application-function id and credentials.
6G sensing function	The sensing-function exposure API planned for 6G.	A draft adapter against the current integrated sensing and communication exposure draft (TS 23.137): discover sensing functions, open a sensing session for the zone, stream result reports, close the session. Converts the zone's shape to the draft's sensing area. Switched on per tenant for trials and revised when the release is final.
Enterprise Wi-Fi controller, radar head end	Enterprise access points and dedicated radar sensors.	Adapter types defined in the catalogue of source types; connectors are built to the same interface as a vendor signs.
Simulator	No radio. Replays realistic tracks, events and per-minute aggregates inside the zone's geometry.	Implements the full interface, so the catalogue, zones, feasibility, live results, KPIs, incidents, charges and the customer portal all run end to end before any source is live. Used to sell and demonstrate, and in testing.

What an adapter reports about a source

Source type (Wi-Fi gateway, enterprise access point, radar, gNB cell, sensing function), vendor, capabilities (detect, track, classify, presence, fall detection, count), the acquisition modes it supports (monostatic, bistatic, multistatic), timing accuracy, backhaul latency, firmware, position and range, and the inventory device it corresponds to. Sources appear on the map alongside your sites and are linked to the equipment that carries them.

What an adapter delivers for a zone

Tracks (position, height, velocity, heading, position error, confidence, object class), events (detection, boundary alert, intrusion, presence, fall), per-minute aggregates (counts) and heartbeats. Every item carries the vendor's observation time and a reference to the raw vendor record for audit. Results are written to the tenant's own sensing store with the zone's retention applied as a time to live.

The road to 6G

Integrated sensing and communication is one of the headline capabilities planned for 6G: the network itself becomes a sensor. 5G-Advanced is its first step and is in networks now. The operators who build a sensing business on 5G-Advanced will arrive at 6G with a catalogue, customers, evidence and a governance record already in place. The ones who wait will start from zero.

Start on what you have

Wi-Fi gateway sensing and 5G-Advanced sensing functions connect today, and the simulator lets you build the catalogue, draw zones and demonstrate to prospects before any radio is live. The sensing business starts now, not at the 6G launch.

One interface for the next source

Every sensing source connects through one common interface, designed with 6G sensing functions in mind. A draft 6G sensing-function adapter, built against the current 3GPP exposure draft, is available for operator trials and will be revised as the release is finalised. A new source is an adapter, not a new product.

Nothing to migrate

Customers, zones, tiers, consent records, SLA history and charges belong to the service, not to the radio. When a zone moves from a 5G-Advanced source to a 6G one, its contract, its evidence and its customer stay exactly where they are. The radios change; the business does not have to.

Catalogue and KPI tiers

Sensing is sold as products, not projects. A product belongs to one of six families, states the modes it permits, the outputs it produces (tracks, events, counts and aggregates), the zone shapes it can be sold in (area, line, point and radius) and its governance profile. Each product carries one or more tiers, and a tier is the contract: the KPI thresholds the operator commits to and the price per zone per month.

Product family	Typical use
Drone detection	Perimeters, airports, critical sites; zones with a height band.
Perimeter intrusion	Fences and boundaries; line zones with boundary alerts.
Traffic and crowd flow	Plazas, stations, event spaces; counts and aggregates.
Industrial asset and safety zone	Yards, plants, exclusion zones around machinery.
Indoor presence and fall	Care settings, assisted living, offices; floor-based zones.
Emergency and rescue	Presence and movement in incident and rescue areas.

Tier KPI	Commitment
Detection probability	At least, per cent
False alarms	At most, per day
Position accuracy	Position error at most, metres
Alert latency	At most, milliseconds
Update interval	Seconds between updates
Availability	At least, per cent
Price	Per zone per month, in the tenant's currency
Incident priority	The priority a breach incident is raised at

Governance profiles: **No personal data** (for example drone detection), **Aggregate only** (counts only; no track or event detail leaves the system or reaches the API) and **Human sensing**, which requires an approved consent record before a zone can be submitted.

Zones, orders and feasibility

A zone is one customer's sensing service in one place. It is drawn on the map as an area, a line or a point with a radius, with a height band for drone zones and a floor for indoor zones, and carries the client, product, tier, contract dates and price. Zones move through draft, submitted, approved and active, with suspended and ended states, through the same contract and approval flow DemandFlow uses for other services: an order is a contract line, a tier change is a new line from the first of a month, and a renewal extends the term.

Feasibility runs against the real inventory. For the zone's geometry and the product's permitted modes, the engine finds candidate sources from the sites and antennas that cover it, chooses the acquisition mode (monostatic for one source; bistatic or multistatic for a set of sources whose timing accuracy and backhaul latency are within the product's limits), predicts each KPI from the KPI model or from the adapter's live capability figures, and compares the prediction with the tier. The result is Pass, Partial or Fail, with the chosen pairing, the excluded sources and the reason for each, and a confidence note.

Change-aware

When a network change is raised against a site or a device that carries a sensing source, the change's impact panel lists the sensing zones and customers it affects, with feasibility today and feasibility without the change's sources, and offers to re-run and save the feasibility for each. Sensing customers are considered before the work starts, in the change process the network team already uses.

Coverage report

For each product family, the area that could be sold across the estate, in which modes, where only one source stands behind it, and which site upgrades would add the most joint-sensing area. Built on the same rules as a zone's feasibility run, so sales and planning read the same answer.

Consent and governance

A human-sensing zone cannot be submitted until a consent record is approved. The record holds the purpose, lawful basis, data subjects, retention period, DPIA status and a review date; approval is recorded with who approved it and when. Consent status (not required, missing, awaiting approval, approved, expired) shows on the zone, on the zones list and on the Sense dashboard, and a zone whose consent has expired is flagged for review.

Retention is enforced, not advised. Results are deleted after the retention period (the consent's, else the zone's, else the product's default), and every deletion run is written to a deletion log with the cut-off, the count and the job reference.

The governance register lists every zone's governance profile, purpose, lawful basis, data subjects, retention, output restriction and DPIA status, with a review timeline and counts of zones missing consent, awaiting approval or due for review, and exports for a data protection audit.

The regulator bundle is one document per zone: the consent record, approvals, a daily roll-up of KPI history, incidents and the deletion log, as JSON with a SHA-256 manifest and as a PDF carrying the manifest hash, signed with a key the operator can verify through the API. Only summaries leave the system; no sensing results are included.

Assurance and SLAs

Every 15 minutes, for every active zone, the assurance job measures each KPI in the product's KPI set from the results of the last complete interval and compares it with

Detection probability in service is measured against ground truth: results reviewed and marked confirmed or false alarm by the operator's team. A rate with no

the tier's threshold. One KPI sample is written per KPI per interval, with the measured value, the threshold, the outcome, the sample count and the breach minutes. The zone's KPI health (healthy, at risk, in breach, not measured) is updated on the zone and the dashboard.

A breach sustained for the product's number of consecutive failed intervals opens one incident, as a ticket in the DemandFlow ticketing your operations team already works, at the tier's incident priority and on the SLA clock. The incident is idempotent: a continuing breach does not open a second ticket. The same event is sent to the customer's webhook subscribers.

reviewed results reports as not measured, never as 100 per cent. Availability is measured from the source's results and heartbeats in one-minute slots while a task is active.

Reports built on the same figures

- **Zone service report**: one zone, one month, each KPI against the tier, incidents and charges, as PDF and in the customer portal.
- **Source health**: uptime, result rate and last seen per source and day, rolled up by vendor.
- **Detection quality**: weekly false alarm rate, confidence distribution, detections by hour, source type and product.
- **Usage**: zone-days and results per customer per month, for licence metering.

Charging and revenue

Each month every active zone is charged at its tier price, pro-rated for partial months from activation to end date; a suspended zone still counts, a draft or submitted zone does not. Service credits are calculated from the zone's breach minutes in the month and written as credit lines. Charges and credits carry a key per zone, month and line type, so re-running a month is safe. Charges are reviewed on the Charges screen and posted to DemandFlow Finance when the operator is ready. The Revenue view shows revenue by product family by month, last month's revenue and credits, the contracted run rate and the forecast to the end of each contract, with a breakdown by customer, product, tier and zone.

For the end customer

Customer portal

Each customer signs in to a branded portal and sees only their own zones: the zone list with status, KPI health and tier; a zone's last 30 days of KPIs against the tier's thresholds and its open incidents; and the monthly service report for any month. Aggregate KPIs only: no sensing results and no tracks are shown.

REST API

Authenticated by an API key issued per client. `GET /v1/sense/zones`, `/zones/{id}/status`, `/zones/{id}/results` and `/zones/{id}/kpis`, with time filters and cursor paging. A key only ever sees its own client's zones. Aggregate-only zones return counts without track detail. Bundle verification and the public key are available for regulator bundles.

Signed webhooks

Customers subscribe to events for their zones: boundary alert, zone breach, fall event and KPI breach. Each delivery is a POST with an `X-DemandFlow-Signature` header, a stable event id for de-duplication, retries with back-off and a dead-letter queue. Aggregate-only zones receive events with position and track detail withheld.

Security, data residency and audit

- Sensing results, KPIs, reports and consents are stored only in the tenant's home region, in a sensing store that belongs to that tenant alone. There is no shared
- The customer portal and API answer "not found" for any zone outside the caller's client, so zone identifiers are never revealed across customers.

table across tenants and no fall-back to another region.
- Vendor and customer credentials are held encrypted; adapter and webhook code never logs a credential, a token or a payload.
- Every read and write of sensing data is written to the tenant's audit log, which can be verified through the API.
- Retention is enforced by the store itself and by the scheduled deletion job, with a log of every run.
- Sense is a module of DemandFlow and is switched on per tenant through the DemandFlow Admin application.

Summary of specifications

Item	Detail
Product families	Drone detection; perimeter intrusion; traffic and crowd flow; industrial asset and safety zone; indoor presence and fall; emergency and rescue
Tier KPIs	Detection probability, false alarms per day, position error, alert latency, update interval, availability; price per zone per month; incident priority
Zone shapes	Area (polygon), line, point and radius; optional height band and floor
Acquisition modes	Monostatic, bistatic, multistatic, chosen by feasibility from the product's permitted modes and the sources' timing and backhaul figures
Source types	Wi-Fi gateway, enterprise access point, radar, gNB cell, sensing function
Adapter types	Gateway vendor cloud (REST, configurable field map); 5G-Advanced sensing function via NEF; 6G sensing function (draft, trials); enterprise Wi-Fi controller; radar head end; simulator
Adapter authentication	None, API key in a header, bearer token, OAuth 2.0 client credentials
Result types	Tracks, events (detection, boundary alert, intrusion, presence, fall), per-minute aggregates, heartbeats
Governance profiles	No personal data; aggregate only; human sensing (consent required)
Consent record	Purpose, lawful basis, data subjects, retention days, DPIA status, review date, approval
Assurance	Every 15 minutes per active zone; one KPI sample per KPI per interval; incidents on sustained breach at the tier's priority
Charging	Monthly, pro-rated, per zone at tier price; credits from breach minutes; posted to DemandFlow Finance
Customer outputs	Portal (zones, 30-day KPIs, monthly report); REST API (zones, status, results, KPIs); signed webhooks (four event types)
Reports	Zone service report, regulator bundle (JSON with SHA-256 manifest and PDF), governance register, coverage, source health, detection quality, usage
Data residency	Per-tenant sensing store in the tenant's home region; retention enforced with a deletion log; audit log of every read and write
Status	Built and running in DemandFlow; demonstrated on request. Available for early access.

www.demandflow.com

Book a demo or talk to us about early access: www.demandflow.com/sensing-service-management/

DemandFlow® is a registered trademark of TOCLOCO LTD. Registered in England No. 09950859. 71-75 Shelton St, London, WC2H 9JQ. © TOCLOCO LTD. All rights reserved.