Changelog

All notable changes to Flintnet are documented here.

[1.0.0-beta] — 2026-05-21

This is the first public beta release of Flintnet. It is intended for evaluation and early adoption by MSPs and SMBs in non-critical environments. Features marked as deferred will be included in subsequent releases.

Agent

Packet Capture

- AF_PACKET-based high-performance packet capture with named threads
- Per-flow tracking with `FlowKey` (src/dst IP, src/dst port, protocol) and `FlowStats` (byte count, packet count, EWMA)
- Flow table exposed via REST API (`GET /flows`)

Device Discovery

- CIDR-based device discovery via `FLINTNET_CIDR` environment variable
- Device classification (router, switch, server, firewall, printer, unknown) inferred from SNMP `sysDescr`
- Device registry persisted to `/var/lib/flintnet/devices.json`
- Device inventory exposed via REST API (`GET /devices`)

SNMP Polling

- SNMPv2c polling for `sysDescr`, `sysObjectID`, interface byte counters (`ifInOctets`, `ifOutOctets`)
- Per-interface utilisation percentage calculation and publication via SSE
- SNMP trap listener

ARP Walking & Security Detection

- ARP table polling via `ipNetToMedia` MIB
- Per-device ARP history with `first_seen`, `last_seen`, and IP change log
- Rogue device detection — alerts on first sight of unknown MAC
- ARP spoof detection — one MAC claiming multiple IPs
- MAC spoof detection — one IP claimed by multiple MACs
- Duplicate IP detection — conflicting IP/MAC associations
- All security events published to internal event bus and exposed via SSE

Anomaly Detection

- EWMA-based traffic anomaly detection per flow
- Anomaly events published to event bus and exposed via SSE

Alert Store

- Per-device security alert ring buffer (20 entries per device, keyed by MAC)
- Recent alerts exposed via `GET /devices/:ip`

SMTP Email Alerting

- Email notifications for rogue device, ARP spoof, MAC spoof, duplicate IP, and anomaly events
- Per-device per-event-type 5-minute cooldown to prevent flooding
- Configurable via `FLINTNET_SMTP_*` environment variables
- Delivered via libcurl with STARTTLS

REST API

- `GET /version` — agent version
- `GET /stats` — packet capture statistics
- `GET /flows` — current flow table
- `GET /anomalies` — detected anomalies
- `GET /devices` — discovered device inventory
- `GET /devices/:ip` — per-device detail including ARP entries, IP history, and security alerts
- `GET /topology` — network topology node/edge data
- `GET /stream` — SSE endpoint for real-time event push
- Bearer token authentication via `FLINTNET_API_TOKEN`

Network Topology

- LLDP/CDP polling for neighbour discovery
- Topology data exposed via REST API for Flutter rendering

Flutter UI

- Login screen with agent URL and API token configuration
- Session persistence via browser `localStorage` — survives page refresh
- Logout button clears session and redirects to login
- Dashboard with real-time flow table, stats, and anomaly list
- Devices screen with device cards, SNMP status badges, and per-interface utilisation bars (colour-coded: green/amber/red)
- Device detail screen with ARP entries, IP history, interface utilisation, and security alert log
- Anomalies screen

- Security events screen
- Network topology diagram with LLDP-based node/edge layout
- Real-time updates via SSE with automatic reconnection

Infrastructure

- Docker Compose single-command deployment (`docker compose up -d`)
- Three services: `flintnet-agent`, `flintnet-ui` (nginx), `influxdb`
- `network_mode: host` with `NET_RAW`, `NET_ADMIN`, `NET_BIND_SERVICE` capabilities for the agent container
- Configuration via `.env` file

Known Limitations (v1.0.0-beta)

- Keygen license enforcement and Stripe billing are not included in this release
- Slack webhook alerting is not included in this release
- Alert threshold configuration UI is not included in this release
- Alert history screen is not included in this release
- CPU/memory SNMP polling (HOST-RESOURCES-MIB) is not included in this release
- Interface error rate monitoring is not included in this release
- TCP retransmission monitoring is not included in this release
- Docker Desktop on Windows and macOS is not supported — a Linux host is required

---

Roadmap

Version	Planned Features
1.1.0	Interface error rates, CPU/memory polling, TCP retransmissions
1.2.0	Slack webhook alerting, alert threshold configuration UI
1.3.0	Keygen license enforcement, Stripe subscription management
2.0.0	Multi-tenancy, cloud-hosted option