Flintnet

Fast, sharp network intelligence for MSPs and SMBs.

Flintnet is a self-hosted network monitoring agent that gives you real-time visibility into your network — traffic flows, device inventory, interface utilisation, ARP security detection, and anomaly alerting — all from a single lightweight deployment.

Features

- **Real-time traffic monitoring** — live flow table with packet and byte counts per flow
- **Device discovery** — automatic CIDR-based discovery with SNMP polling for device classification
- **Interface utilisation** — per-interface in/out bandwidth utilisation via SNMP
- **ARP security detection** — rogue device detection, ARP spoofing, MAC spoofing, and duplicate IP detection
- **Anomaly detection** — EWMA-based traffic anomaly detection per flow
- **SMTP email alerting** — email notifications for security and anomaly events with per-device cooldown
- **Network topology** — live topology diagram built from LLDP/CDP data
- **Device detail** — per-device ARP history, security alert log, and interface utilisation
- **Self-hosted** — your data never leaves your network

Prerequisites

Requirement	Details
Linux host	Ubuntu 20.04+ or Alpine 3.16+ recommended
Docker	Docker Engine 20.10+ (not Docker Desktop on Windows/macOS)
Docker Compose	v2.0+
Network privileges	Host must support `NET_RAW` and `NET_ADMIN` capabilities
Network access	Agent must be on the same Layer 2 segment as monitored devices
SNMP	Monitored devices must have SNMPv2c enabled

> **Important:** Docker Desktop on Windows and macOS cannot grant the network capabilities required by the agent. A Linux host or VM is required.

Quick Start

1. Download the deployment package

```
curl -L https://flintnet.io/download/docker-compose.yml -o docker-compose.yml
curl -L https://flintnet.io/download/.env.example -o .env.example
```

2. Create your `.env` file

```
cp .env.example .env
```

Open `.env` in a text editor and set at minimum:

```
FLINTNET_CIDR=192.168.1.0/24
FLINTNET_SNMP_COMMUNITY=public
```

3. Start Flintnet

```
docker compose up -d
```

4. Open the UI

Navigate to `http://<your-server-ip>` in Chrome or Edge.

Enter your agent URL (`http://<your-server-ip>:3000`) and API token on the login screen.

Environment Variable Reference

Required

Variable	Description	Example
`FLINTNET_CIDR`	Subnet to monitor in CIDR notation	`192.168.1.0/24`
`FLINTNET_SNMP_COMMUNITY`	SNMPv2c community string for your devices	`public`

Authentication

Variable	Description	Default
`FLINTNET_API_TOKEN`	Bearer token required to access the REST API	*(empty = no auth)*

SMTP Email Alerting

Variable	Description	Default
`FLINTNET_SMTP_HOST`	SMTP server hostname	*(empty = disabled)*
`FLINTNET_SMTP_PORT`	SMTP server port	`587`
`FLINTNET_SMTP_USER`	SMTP username / sender address	

Variable	Description	Default
`FLINTNET_SMTP_PASSWORD`	SMTP password	
`FLINTNET_ALERT_EMAIL`	Recipient email address for alerts	

InfluxDB

Variable	Description	Default
`INFLUXDB_URL`	InfluxDB connection URL	`http://influxdb:8086`
`INFLUXDB_DB`	InfluxDB database name	`flintnet`

Architecture

Flintnet consists of three Docker services:

Service	Description	Port
`flintnet-agent`	C++ monitoring agent — capture, SNMP, REST API, SSE	3000
`flintnet-ui`	Flutter web UI served by nginx	80
`influxdb`	InfluxDB 1.8 time-series database	8086

Supported Browsers

Chrome and Edge are recommended. Firefox may work but is not officially supported. Safari is not supported.

Support

- Documentation: https://flintnet.io/docs
- Support: https://flintnet.io/support