# NuajProtect

DISTRIBUTED THREAT
INTELLIGENCE & ENFORCEMENT

**NuajProtect stops network attacks on the hardware you already run.** When any network on the service sees an attacker, every other network blocks it within seconds, with no operator action.

### 30 seconds

From first sighting to fleet-wide enforcement.

### 600,000+

Threats already blocked the day you plug in.

### Zero

IP addresses on a bridge's inline path. Nothing for an attacker to connect to.

## HOW IT WORKS

An agent runs on your Linux servers, MikroTik routers and NuajBridge appliances. Every one of them is both **sensor and enforcer** — it finds threats on its own and blocks them on the spot, without waiting to be told.

They keep protecting while disconnected, so the service going dark cannot take your defences with it.

1. Threats are spotted locally — decoy ports, rate limits, reports from your apps.
2. The service checks that report against every other network's evidence.
3. Confirmed threats are pushed back to every agent within seconds.
4. Every network that joins makes the block list stronger for all of them.

## FIVE LAYERS OF DEFENCE

**1 — Trusted Sources**
Allowlist

Nothing you depend on can be blocked — not by a feed, not by a false report, not by another network. Listing your uplink takes you down without touching you.

**2 — DDoS Protection**
Flood Shield

Volumetric attacks absorbed at line rate. Limits are learned from your own traffic, and the replies your servers asked for are never throttled.

**3 — Intrusion Detection**
Gatekeeper

Decoy ports catch the slow, quiet scanning that rate limits miss. Repeat offenders are blocked fleet-wide; a one-off mistake ages out.

**4 — Threat Intelligence**
Blocklist

Commercial feeds and country blocking, curated and enforced as one list. You never manage a feed or chase a subscription.

**5 — Collective Defence**
Banlist

Built from every network on the service: one attacker, seen once, blocked everywhere. You set how many reports confirm a threat.

## WHERE IT RUNS

The mode decides **where** protection sits, never **how much** of it you get — all three run the same five layers of defence.

### Sentry

Protects the server it runs on. Any application on that server — your own or third-party — can report what it alone sees: failed logins, WAF hits, credential stuffing.

Linux Agent · MikroTik

### Relay

Protects the devices behind it by filtering the traffic they receive — sent directly or through a GRE, WireGuard or IPsec tunnel, so their real addresses need never be exposed.

Linux Agent · NuajBridge

### Bridge

Sits invisibly inside a network segment: no IP address, no re-addressing, no routing changes. Cable it in and traffic is filtered on the way through.

NuajBridge · MikroTik

**Linux Agent** — servers, VMs, containers | **MikroTik** — branch, CPE, RouterOS estates | **NuajBridge** — whole segments

## THE NUAJBRIDGE FAMILY

Purpose-built inline appliances. Same five layers, same IPv4 and IPv6 support, same signed updates — on every model.

| | 2.5G | 25G | 100G | 400G |
|---|---|---|---|---|
| Best for | Edge · small site | Core · multi-tenant | Large datacenter | Carrier · backbone |
| Traffic ports (WAN/LAN) [1] | **2.5G**<br>2 × RJ45 | **25G**<br>2 × SFP28<br>**2.5G**<br>2 × RJ45 | **100G**<br>2 × QSFP56<br>**10G**<br>2 × RJ45 | **400G**<br>2 × QSFP-DD<br>**10G**<br>2 × RJ45 |
| Blocked addresses held | 1 M | 4 M | 30 M | 30 M |
| Form factor | Compact desktop | 1U | 2U | 2U |
| Power supply | Single | Single | Dual, redundant | Dual, redundant |
| NuajProtect subscription | 1 year included | 3 years included | 3 years included | 3 years included |
| Every defence layer on every model — capacity follows the hardware, features never do | | | | |
| Availability | now | now | Q2 2027 | Q3 2027 |

**1** Models with two pairs run one at a time. Move to the faster pair by re-cabling — same appliance, same policy.

## HIGH AVAILABILITY

Redundancy uses **independent failure domains** — separate boxes, never two engines in one chassis. Nothing is put to a vote: your routing and your bonds keep deciding, and two units can never both take one path. **The cluster is one device** — members ring together on their peer ports and carry one policy, one blocklist and one approval set, with nothing to pair by hand. Three topologies: **paired** (standby takes the path), **routed** (failed path withdrawn) and **bonded** (member drops out).

## RUNNING IT

### OPERATIONS

- Embedded live dashboard
- Default policies every new endpoint inherits
- Per-endpoint overrides where you need them
- Multi-tenant isolation

### WITHOUT ASKING YOU

- Port scans spotted and blocked automatically
- Whole /24 ranges blocked when one host is not the problem
- Abuse reports filed with the network that owns the address
- Older Linux kernels protected without a kernel upgrade

## WHO IT IS FOR

### MANAGED SERVICE PROVIDERS

Every client site behind one dashboard, isolated from every other, with a default policy new sites inherit the moment they come online.

### DATACENTERS & HOSTING

Protect tenants you do not control, on hardware you do — and stop being the network everyone else's abuse desk emails about.

### MULTI-SITE NETWORKS

An attack on the branch office is blocked at head office before it arrives. One policy, every site, no per-site work.

### Start with the beta

NuajProtect is in open beta, with the 2.5G appliance. The service is free during the beta and for a full year after general availability. Appliances are purchased — beta members get priority access as each one ships.

**protect.nuaj.com**
sales@nuaj.com