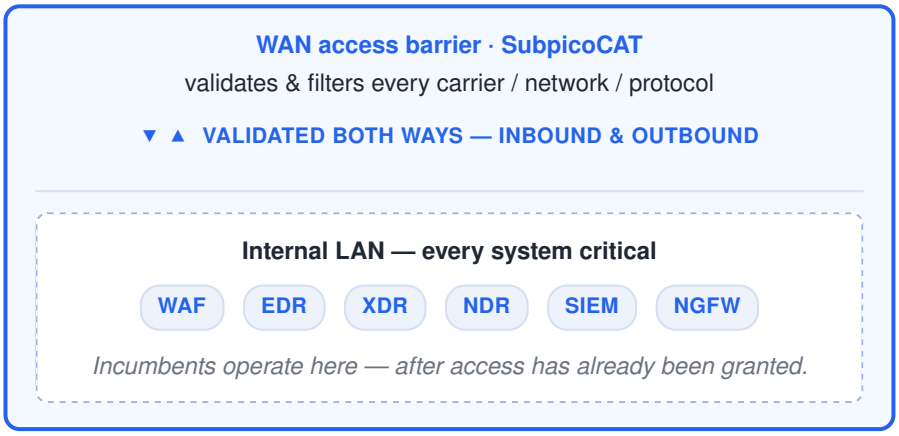
SubpicoCAT®

# A Better Way of Securing the Wire

**Why SubpicoCAT works at the WAN, not the LAN.** Every established cyber-security product — web application firewalls, endpoint and extended detection, network detection, SIEM, next-generation firewalls — operates *inside* the network it defends. SubpicoCAT works at the boundary those products sit behind: it validates and filters traffic at the WAN access layer, before anything reaches the internal network.

The LAN is an open system of low validity. Once a device is present, trust is largely implicit, and vendors compete to detect and respond *after* an adversary is already inside. That model concedes the first move. Advanced persistent threats and, increasingly, automated and AI-driven access exploits are built precisely to win that first move — against the home, office and branch router and Wi-Fi that most operations never think to defend.

SubpicoCAT treats the access boundary as the control point. It works the way a water filter does: impurities are removed before the water reaches the tap, not chased through the plumbing afterward. Hostile traffic — across any carrier, network or protocol — is validated and blocked at line rate before it can reach an internal system. And the same filter works in reverse: it rate-limits and validates what *leaves* the network too, so a compromised device behind it cannot be turned into a source of floods, exfiltration or abuse. Because every internal system is critical to the operation that depends on it, the access layer is where the decisive control belongs.



## Removing the SOC and MSP external activities: threat-hunting loads

Conventional cyber security is labour-intensive by design: a security operations centre — in-house or an outsourced MSP / MSSP — staffed around the clock, with analysts triaging alerts, hunting threats, and passing tickets back and forth. Much of that effort is redundant — chasing false positives, reconstructing events after the fact, and coordinating between tools, teams and providers.

SubpicoCAT's real-time machine learning does the detection *and* the decision on the wire, as traffic passes: threats are identified and blocked automatically, at line rate, without waiting for a person to open an alert.

- **From a queue to a record.** Your people receive a short, structured account of what was already handled — not a backlog of raw alerts to investigate.
- **No hand-off loop.** The redundant SOC ↔ MSP communication cycle largely disappears; skilled analysts are freed for the few decisions that genuinely need human judgement.
- **Protection that doesn't sleep.** It does not depend on someone watching a screen at 3 a.m. — the unit behaves the same under attack as it does on the bench.

| Dimension | LAN cyber (WAF · EDR · XDR · NDR · SIEM · NGFW) | SubpicoCAT WAN |
|---|---|---|
| **Where it operates** | Inside the perimeter — host, endpoint, application | The access boundary itself |
| **Trust model** | Implicit trust once inside an open LAN | Nothing trusted across the WAN edge |
| **Scope** | Single network, protocol-specific, vendor-bound | Multi-carrier · multi-network · multi-protocol |
| **Primary action** | Detect and respond *after* presence | Validate, filter and block *before* entry |
| **Direction of protection** | Chiefly inbound; outbound only via egress rules, DLP or after-the-fact alerts | Bidirectional — rate-limited flow control and protocol validation, *in and out* |
| **APT / AI-access exploits** | Chase lateral movement post-breach | Deny the access path — router, Wi-Fi, infrastructure |
| **Latency / determinism** | Agent and cloud overhead; variable | Sub-100 µs, line rate; deterministic RTOS |
| **Data-path integrity** | Software controls; back-channels exist | Physically one-way ports; no back-channel |
| **Footprint** | Per-host agents, inline proxies, SaaS SIEM | One fanless unit — standalone to fleet |
| **Sovereignty / offline** | Typically cloud-dependent | Runs air-gapped and sovereign |

*Categories, with representative vendors: WAF — Cloudflare, F5 · EDR — CrowdStrike, SentinelOne · XDR — Palo Alto Cortex · NDR — Darktrace, Vectra · SIEM — Splunk, Microsoft Sentinel · NGFW — Palo Alto, Fortinet.*

## What the WAN position gives you

- **You keep the first move.** Threats are filtered at the access boundary, not chased once they are already inside and trusted.
- **One barrier for every path.** Multi-carrier, multi-network, multi-protocol — the same protection whether traffic arrives over fibre, copper, cellular or private link.
- **Protection you can prove.** Ports set receive-only or transmit-only are one-way in hardware, so a one-way feed cannot carry a back-channel — enforced physically, not by policy.
- **Predictable under attack.** A deterministic RTOS holds a sub-100 µs response at 3 a.m. under load exactly as it does on the bench — no agents, no cloud round-trips in the path.
- **Real-time DDoS scrubbing, on the wire.** Floods are scrubbed at multiple layers, in real time, in the device on your access path — not diverted to a distant carrier or cloud scrubbing centre after the traffic has already left your control.
- **Protection both ways.** Rate-limited flow control and protocol dissection run on inbound *and* outbound traffic, so a compromised camera, sensor or host behind the unit cannot be conscripted into a flood, a reflection attack or a quiet exfiltration. You defend your own infrastructure — and everyone downstream of you — from one vantage point.
- **Yours, online or off.** Run fully air-gapped and sovereign, or manage a fleet from the Subpico Interlace platform — the protection is identical either way.

## Technology comparison — who is actually at the WAN access layer

The first table compares SubpicoCAT with the LAN-interior categories. This one addresses a harder question: of the technologies that *claim* the edge, which actually sit on the WAN access path? Cyber-security marketing leans heavily on the word “edge,” but most of these products still operate inside the customer’s boundary — in a DMZ behind the carrier link — or in the vendor’s own cloud, which the customer must route traffic *to*. Neither is the access barrier itself.

| Approach — with examples | Where it actually sits | What it is built to do | Why it is not the WAN access barrier |
|---|---|---|---|
| **SASE / SSE** — Zscaler, Palo Alto Prisma, Netskope, Cato, Cloudflare One, Fortinet FortiSASE | The vendor's cloud PoPs — you tunnel your traffic *to* them | Broker user-to-application access; inspect web / SaaS traffic in the cloud | A cloud service, not your device; traffic still crosses the open carrier to reach it; identity-centric, not a sovereign line-rate barrier |
| **Secure SD-WAN** — Cato, Versa, Fortinet | The branch router, cloud-orchestrated | Optimise connectivity between sites, with policy security added | A router with security bolted on; policy-based and cloud-managed — not line-rate validation of every path |
| **Carrier / cloud DDoS scrubbing** — NETSCOUT Arbor, Cloudflare Magic Transit, Akamai Prolexic | Upstream carrier / cloud scrubbing centres | Absorb volumetric floods before they reach you | Volumetric only, and reactive; traffic is diverted to a distant centre rather than scrubbed in real time on your own access path — SubpicoCAT does multi-layer scrubbing on the wire |
| **Unidirectional gateways / data diodes** — Waterfall, Owl, Advenica, OPSWAT, Oakdoor | Hardware at the IT/OT boundary | Enforce physically one-way transfer (telemetry, historian replication) | Single-purpose transfer; no active multi-protocol filtering or routing; bidirectional traffic still needs a firewall |
| **"Edge" / NGFW & DMZ firewalls** — Palo Alto, Fortinet, Check Point | Your DMZ / perimeter — *inside* your boundary, downstream of the carrier | Filter at the perimeter by rule and signature | The castle wall, not the moat: marketed as "edge," but LAN-facing and already behind the carrier link |
| **Network TAPs / packet brokers** — Gigamon, Keysight, Network Critical | Inline taps that feed other tools | Copy traffic for visibility | Passive — it sees everything and blocks nothing |
| **SubpicoCAT WAN appliance** | **On the WAN access path — a sovereign device you own and control** | **Validate, filter, block *and* route at line rate across every carrier, network and protocol — including real-time, multi-layer DDoS scrubbing on the wire — with optional shared intelligence over the Interlace network** | **This *is* the access barrier: active defence, routing and physically selectable one-way ports on one fanless box — standalone to fleet, no cloud dependency** |

**Reading the claims.** Three questions cut through the sleight-of-hand. **One:** does traffic reach a system *you* own on the access path — or must you route it to the vendor's cloud first? **Two:** does the device sit *before* your perimeter — or *is* it your perimeter, a firewall the carrier link already terminates behind? **Three:** does it actively validate and block every protocol at line rate — or only watch, scrub floods, or move data one way? On all three, SubpicoCAT is the only device that sits on the access path, under your control, doing the work.

## Both directions — what the market splits across four tools

There is no single product to compare this next capability against, because the market does not treat it as one problem. Almost everything defends *inbound*. Protecting *outbound* is left to a patchwork: egress rules on a firewall, data-loss prevention for content, network detection that alerts after the fact — and, for outbound floods, usually nothing at all. Each is a separate tool, and none applies real-time, rate-limited flow control to traffic leaving the network.

From its vantage point in the WAN, SubpicoCAT does both at once. Flow rate limits and protocol dissection and validation are applied inbound *and* outbound, at line rate, in one device — the work that would otherwise take an inbound anti-DDoS service, an egress firewall, a DLP product and a detection platform, none of which stops an outbound flood in real time. It is the difference between filtering only what comes in, and controlling everything that crosses the boundary in either direction.

---

**The contrarian position, plainly.** Everyone else defends the castle from inside its walls. SubpicoCAT holds the ground in front of them — clean traffic in, threats out, before the first internal system is ever exposed. Managed as a fleet from the Subpico Interlace platform, or run entirely offline; the protection is the same either way.

**brianparsons@subpicocat.com** · subpicocat.com



---

### LANDSCAPE REFERENCES

Category descriptions reflect the vendors' own published accounts of where their products operate and what they do, current as of August 2026. Cited for comparison; not endorsements.

1. **SASE / SSE — cloud-delivered, PoP-based architecture.** Gartner Peer Insights, *Security Service Edge* market — gartner.com/reviews/market/security-service-edge · Forrester, *The Secure Access Service Edge Services Landscape, Q1 2026* · Zscaler, *What is SASE?* — zscaler.com/resources/security-terms-glossary/what-is-sase · Palo Alto Networks, *What is SASE?* — paloaltonetworks.com/cyberpedia/what-is-sase.
2. **Carrier / cloud DDoS scrubbing — upstream, volumetric mitigation** via provider scrubbing centres (e.g. Cloudflare Magic Transit, NETSCOUT Arbor, Akamai Prolexic). Positioned by their vendors as always-on or on-demand traffic diversion to a scrubbing network, distinct from SubpicoCAT's real-time, multi-layer scrubbing performed on the wire at the access path.
3. **Unidirectional gateways / data diodes — hardware-enforced one-way transfer** at the IT/OT boundary. Network Critical, *Data Diodes for OT and ICS Networks 2026* — networkcritical.com/blogs/data-diodes-for-ot-and-ics-networks · 4-Secure, *Data Diode Vendors: 2026 Buyer's Guide* — 4-secure.com/data-diode-vendors · OPSWAT, *MetaDefender Optical Diode* — opswat.com/products/metadefender/optical-diode.