protectiONE DR — Features Overview

A turnkey appliance that gives Internet Service Providers an all-in-one passive device for legally compliant traffic-data retention and day-to-day operational security visibility. protectiONE DR captures and analyses traffic from mirrored LAN and WAN interfaces on the operator's NAT device, with no inline element in the data path — connection latency and throughput are unaffected. And for deployments where interface mirroring is not available there are IPFIX and NetFlow v9 collectors.

Data retention & flow storage

- Captures every IPv4 and IPv6 flow from mirrored interfaces — each probe captures packets from the LAN and WAN sides of the NAT device so NATed flows are reconstructed too.
- Accepts IPFIX and NetFlow v9 from third-party routers and switches as a supplementary source, useful where mirroring isn't available or in distributed deployments. IPFIX or NetFlow v9 is required because of the NAT source-address and source-port fields.
- Flows are stored in an hourly-partitioned database schema, retained for as long as operational and legal policy require. Per-hour partitions enable fast retention rollover.
- All retained flow data is queryable through the WAMP API or the operator UI — by IP, prefix, port, protocol, ASN, time interval, and free combinations of those filters — without writing SQL.
- **Flow visualisation & analytics.** Interactive time-series and distribution charts cover traffic volume, packet rates, top source / destination talkers, and per-protocol / per-port / per-ASN / per-country breakdowns. Click-to-filter on any chart drills down to the matching flows; prev/next interval navigation walks the timeline without losing the active filter; every view exports to PDF / CSV / JSON.
- **Real-time traffic analyzer.** Live bandwidth, packet-rate, and connection-rate counters refresh every couple of seconds — operators get a moment-by-moment view of what is happening on the wire right now, alongside the historical flow analytics over stored data. Per-interface counters with operator-configurable absolute or relative-to-baseline modes.
- Native IPv4 and IPv6 throughout: separate partitioned flow tables, full dual-stack analysis.

Attack detection and mitigation

- **Real-time attack detection** over the mirrored traffic, with normalised events feeding the Attack Log, Map, and Live Feed views already wired in the UI.
- **Threat-intelligence feeds.** Real-time tagging of flows whose endpoints appear on any active threat feed.
- **Aggregated traffic-data mode** for deployments where full retention exceeds operational or legal need — per-source / per-destination summaries instead of every flow.

Security visibility

- **Vulnerability scanning.** Automated scanning of operator subnets with operator-tunable cadence and intensity. Two built-in profiles (fast / full); operator-configurable port lists, timing templates, and chunk sizes. Two scan modes: `scan_all` (every IP in a subnet) and `scan_seen` (only IPs actually seen in recent traffic — far less wasted scanning).
- **Severity-aware scoring.** Every detected vulnerability scored against CISA's Known Exploited Vulnerabilities (KEV) catalog and the EPSS (Exploit Prediction Scoring System). Operators see at a glance which findings are actually being exploited in the wild versus theoretical CVEs.
- **Vulnerability analytics.** Interactive charts — risk distribution, detections timeline, top scripts, top CVEs, per-host density. Time-range navigation with prev/next interval history; click-to-filter on any chart; PDF / CSV / JSON exports.
- **ASN enrichment.** Every source / destination IP is tagged with its Autonomous System Number and owning organisation. Lets the operator see attack origins by network and organisation, not just by IP.

Operations

- **Web UI.** Modern web interface (SvelteKit-based), Czech, English and German localisation, role-based access. All operator-facing actions are RPCs over WAMP — no shell access, no SQL, no direct config-file editing required.
- **User-visible log.** Every relevant event from the daemons surfaces in a live ring in the UI with severity filters, free-text search, and CSV / JSON / PDF export. Survives WAMP reconnects.

- **Monitoring integration.** Built-in Zabbix server-active configuration page, plus Grafana + Prometheus and Nagios templates for operators with existing monitoring stacks.
- **Multi-user with audit.** Named operator accounts via the standalone authentication daemon. Tracks per-user creation timestamp and last-login.
- **Documentation in-product.** Guides and configuration examples viewable directly in the UI with syntax highlighting, download, and PDF export.

Compliance & deployment profile

- Data retention model aligns with the Czech telecommunications regulation: Act 127/2005 §97(3) and Regulation 357/2012. Retention modes are operator-configurable to match the legal interpretation in the jurisdiction.
- Standalone appliance, Linux base. Two service ports (eth0 with firewall, eth1 for primary configuration) plus 10/40/100 GbE mirrored-traffic interfaces per real-time probe. No outbound dependency on operator infrastructure beyond NTP and the configured threat-intel update sources.