INTRUDECT

Technical Datasheet

Modular network monitoring and intrusion detection platform

Self-hosted · No telemetry · EU-built

intrudect.com
info@intrudect.com

Overview

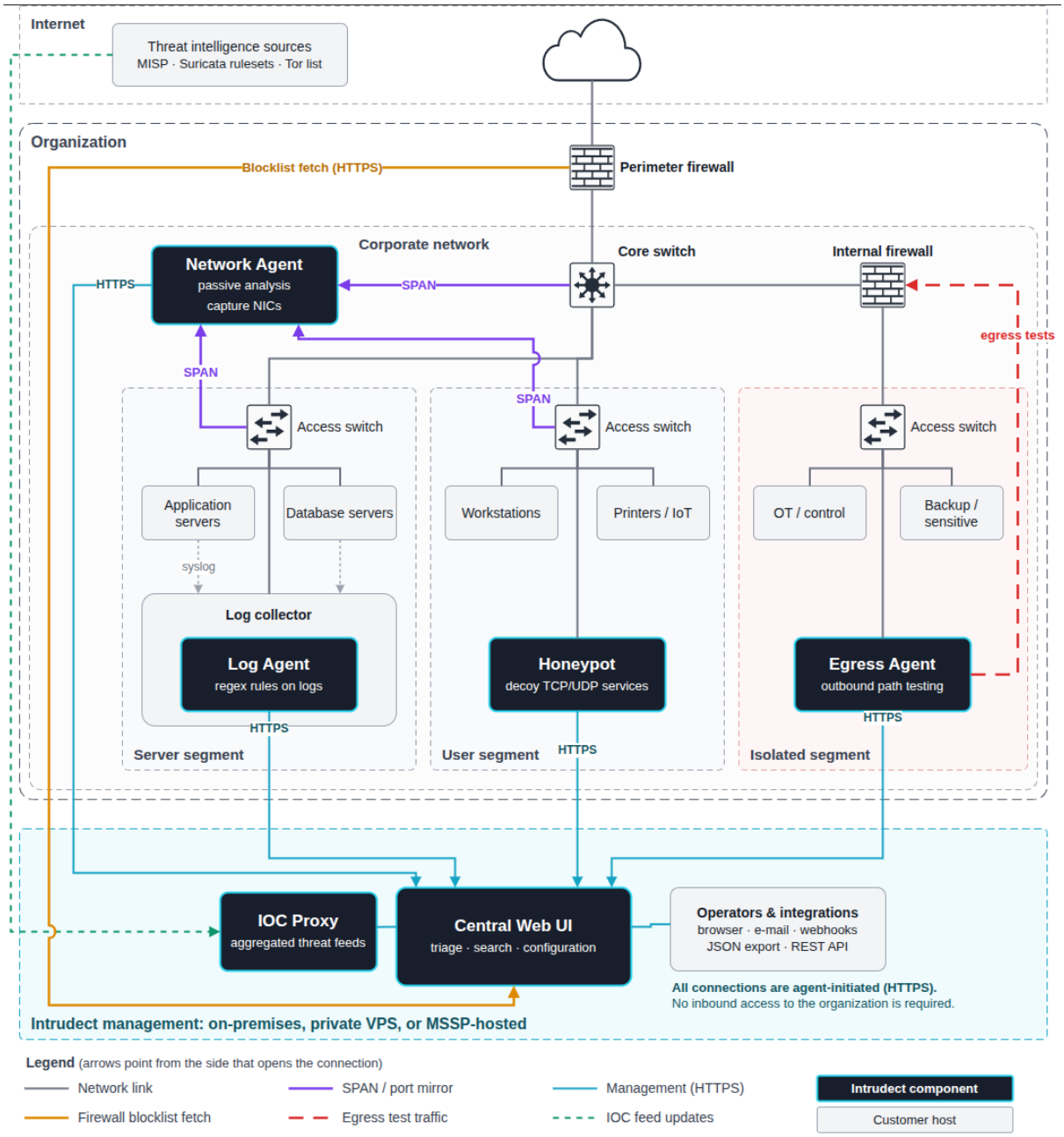
Intrudect is a modular, self-hosted security monitoring platform for internal network visibility. It combines passive network metadata analysis, isolated-network egress validation, decoy-service monitoring, and regex-based log monitoring in one centrally managed system, with optional automated blocking on supported firewalls.

The platform detects internal reconnaissance, lateral movement, unauthorized services, policy deviations, and outbound paths that should not exist. The emphasis is on actionable metadata and operational usability rather than broad packet-signature matching.

Architecture

Agents collect metadata and generate alerts in the monitored environment. Users interact only with the central Web UI for management, investigation, and configuration.

Component	Purpose
Network Agent	Passive traffic analysis, detection of internal attack behavior, service exposure, and policy violations
Egress Agent	Validates whether isolated or restricted segments can unexpectedly reach outside networks
Honeypot	Emulated TCP/UDP services on IP addresses and ports with no legitimate use. Any connection or scan generates an alert. Deployment: one instance per segment, or one instance with interfaces or VLAN subinterfaces in multiple segments.
Log Agent	Regex-based monitoring of system and application log files
IOC Proxy	Aggregates MISP, Suricata rules, user-defined IP/DNS blocklists, and the Tor list into unified threat feeds; agents fetch locally without direct internet access
Central Web UI	Alert triage, search, dashboards, configuration, user management, integrations, exports and beacon document generation



Key Differentiator

Intrudect is the only NDR platform on the market that includes a built-in network honeypot and an egress isolation verification agent as native components – not add-ons or separate products.

Positioning

vs Enterprise NDR (Vectra AI, Darktrace, ExtraHop, Corelight)

- Lower price point with comparable internal visibility coverage
- Faster deployment and operational start
- No vendor lock-in or cloud dependency

vs Open-source stacks (Security Onion, Zeek, Suricata, Snort)

- More out-of-the-box functionality, less custom integration
- Fewer moving parts, lower operational maintenance
- Behavior-based detections with actionable metadata context

Network Agent – Detection Coverage

The Network Agent passively analyzes traffic metadata and selected protocol activity. It requires port-mirrored (SPAN) traffic from network switches.

Reconnaissance and Discovery

Detection	Description
Port scanning	Single-target and multi-target scan pattern detection
ARP scanning	ARP-based host discovery detection
DNS scanning	Dictionary-based host discovery and PTR-based network mapping
Unused IP scanning	Detection of probing against unused IP address space
LDAP/AD mapping	Active Directory enumeration and domain mapping anomalies

Lateral Movement and Segmentation

Detection	Description
Lateral movement	Movement on administrative protocols (SSH, WinRM, RDP, etc.) to unauthorized destinations. Protocol list and exceptions are user-managed.
Inter-segment policy	User-defined cross-segment traffic policy matrix. Unauthorized traffic initiation generates an alert.
Password spraying	Sequential short/low-packet connections on administrative protocols (SSH, RDP, etc.).

Policy and Threat Intelligence

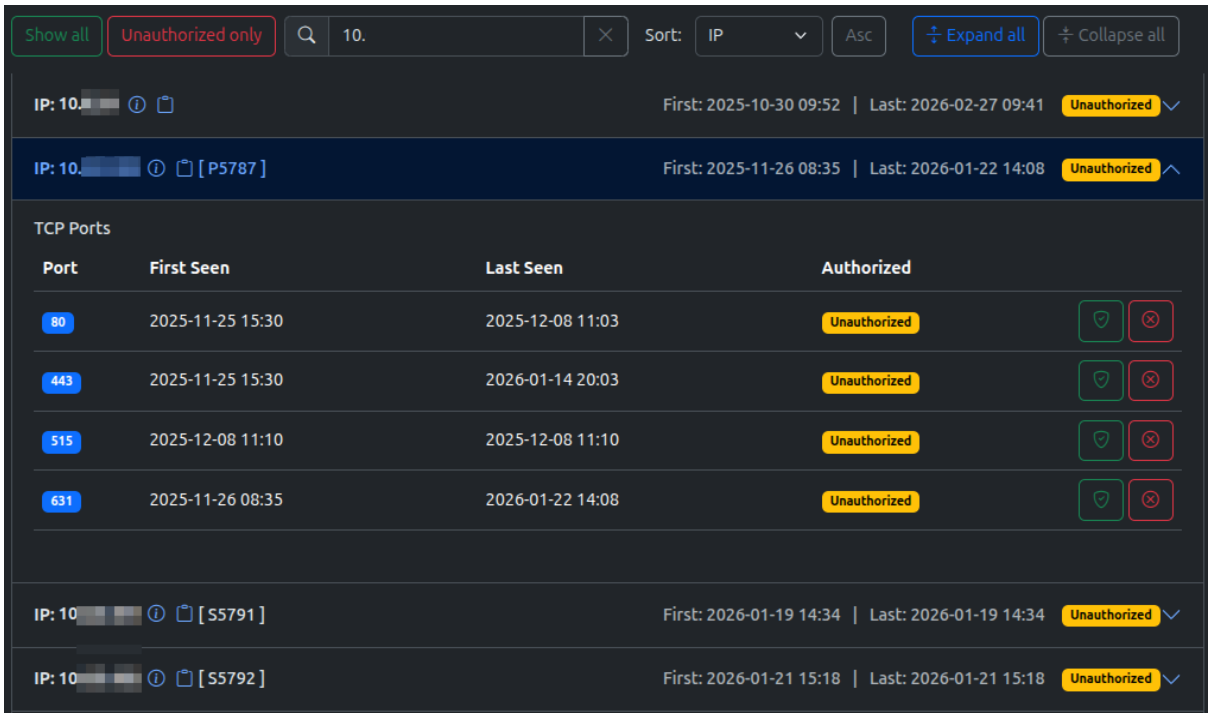
Detection	Description
IOC matching	Known-bad IPs, DNS names, and device names from aggregated IOC Proxy feeds.
Suricata rules	User-pointed Suricata rulesets applied to HTTP, TLS, and DNS traffic.
HTTP User-Agent	Alerts on suspicious, non-standard, or known offensive-tooling user-agent values. User-configurable exceptions.
TOR traffic	Detection of traffic to/from the TOR network
SMB to internet	Alerts when SMB traffic is directed to external destinations

DNS and DHCP Security

Detection	Description
DNS tunneling / C2	Detection of DNS-based command-and-control communication patterns
DGA domains	Detection of domain generation algorithm query patterns
Rogue DNS servers	Alerts on DNS queries directed to non-authorized DNS servers
Rogue DHCP servers	Unauthorized DHCP server detection
DHCP anomalies	Excessive request volume, same MAC with different hostnames, same hostname from different MACs, known offensive tool hostnames in DHCP requests

Asset and Service Visibility

Capability	Description
Device inventory	All network devices discovered from DHCP and traffic analysis. IP, MAC, vendor, hostname, first seen, last seen. Exportable. IP history for devices.
New device alerting	Configurable per network segment. Alerts when a previously unseen device appears.
Service discovery	Passive discovery of TCP/UDP services from observed traffic. Each service tracked with first seen and last used timestamps.
Unauthorized services	Alert when an unauthorized TCP/UDP service is detected on the internal network.
Virtual sandbox	Per-device outbound traffic policy using DNS, ASN, and IP-based destination rules. Traffic outside the defined pattern generates an alert.



Device inventory with service discovery and authorization status

Egress Agent

Validates whether an isolated or restricted network segment can unexpectedly reach outside networks. Runs 24/7, actively attempting outbound communication using multiple transport methods. Test methods and frequency are user-configurable.

- DNS channels (A / AAAA / TXT record queries)
- IPv4 and IPv6 pathways and fallback routes
- ICMP-based egress leak detection
- Proxy abuse and discovered gateway testing
- Temporary firewall or routing exceptions
- Local read-only status web UI and JSON API on the agent

Alerts identify the leaking network segment and the specific method that achieved outbound connectivity.

Honeypot

Decoy TCP/UDP services deployed on selected IP and port combinations. Any interaction is unexpected in normal operation and raises an alert.

- Configurable TCP and UDP port listeners
- Protocol emulation for common services: SSH, Telnet, FTP, SMTP/POP3/IMAP, HTTP, Redis, PostgreSQL/MySQL/MSSQL, LDAP, VNC, SMB, Modbus
- Multiple IP address support per honeypot instance
- PCAP capture on connection for forensic evidence
- Alert on connection initiation, full session PCAP on disconnect
- Scan detection: both SYN (half-open) and full connect scans raise alerts

Beacon Documents

Decoy Microsoft Word and Excel documents that contact a public Intrudect callback endpoint when opened. They detect document theft and exfiltration, including access that happens outside the organization after the data has left the network.

- Generated and managed in the Web UI
- Each document is unique, so an alert identifies the exact file and where it was placed
- Callback data: timestamp, source IP

A callback is only triggered if the document is opened on a system that can reach the callback endpoint and loads external content. Offline analysis, Protected View, or blocked outbound traffic can prevent the callback.

Log Agent

Extends platform coverage into host and application logs using user-defined regular expressions. Can be deployed on a central log collector or on individual servers.

- Unlimited concurrent log file monitoring per agent
- Custom alert message and severity per rule
- Syslog, application logs, web server logs, database logs, audit logs

Example use cases: web server 404/403 status codes, SQL injection patterns in database query logs, non-standard or known bad user agents, password-based logins where key-based is expected, file access monitoring of sensitive files with auditd.

Investigation Metadata

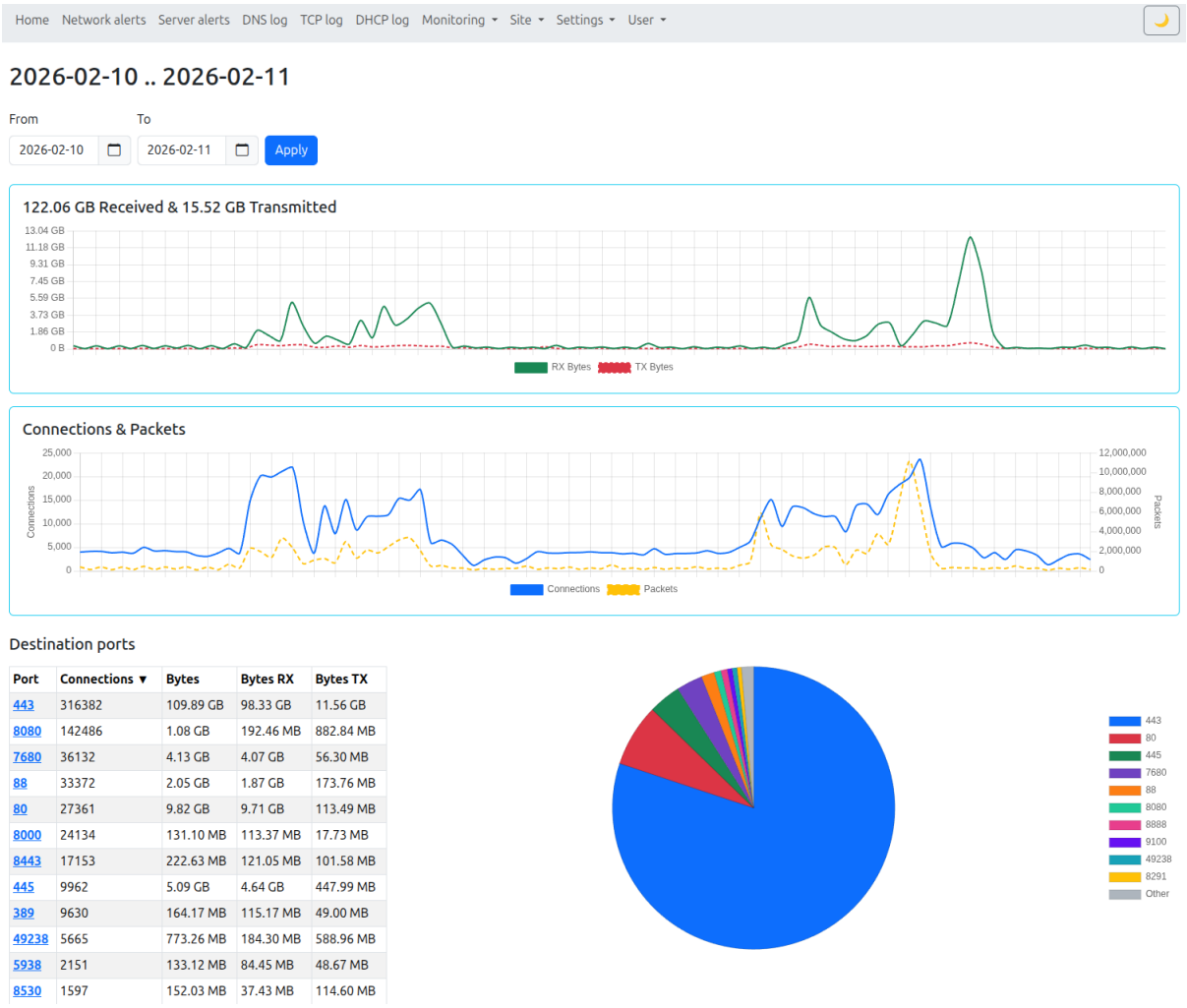
Intrudect stores detailed metadata to make alerts actionable without requiring full packet capture review for every event.

Data Type	Stored Context
All traffic	Timestamp, source/destination IP, MAC, port, reverse PTR value, ASN
DNS	Query content, record type (A, AAAA, CNAME, etc.), query values, DNS server
TCP sessions	Connection duration, bytes and packets in both directions, SNI from TLS, PTR and ASN enrichment
UDP flows	Flows grouped by source/destination IP and port, SNI extracted from QUIC, same search and report views as TCP

DHCP	Requests and responses, hostname values, assigned IP addresses
HTTP	Request URL, host header, user-agent value
Devices	IP, MAC, vendor, hostname, first seen, last seen
Services	Observed internal TCP/UDP services with first seen and last used timestamps
Forensics	Optional PCAP snippets attached to qualifying alerts

Analysis and Dashboards

- Search and filter by time range, source/destination IP, port, MAC address, hostname
- Wildcard and list-based search support
- Aggregated daily overview: alerts, newly detected devices, traffic volumes, top initiators, destinations, DNS queries
- Ranked views and graphs for traffic destinations, ports, ASN/country breakdown
- DNS statistics: top domains, query types, DNS servers, volume graphs
- Data export: CSV, XLSX, JSON



Network dashboard – aggregated daily overview with traffic statistics and alert summary

Alerting and Integration

Alerts flow from agents through two filtering layers before reaching operators, reducing noise from long-running or repetitive events.

Alert Routing

- Agent-level pre-filtering: aggregation prevents repetitive flood from sustained attacks
- Web UI routing layer: filter by weekday, work hours, alert category, and priority
- Unlimited routing rule combinations
- Configurable data fields per export channel

Firewall Integration

Intrudect can add the source IP address of an alert to a blocklist on a supported firewall. Supported platforms: MikroTik RouterOS and Fortinet FortiGate.

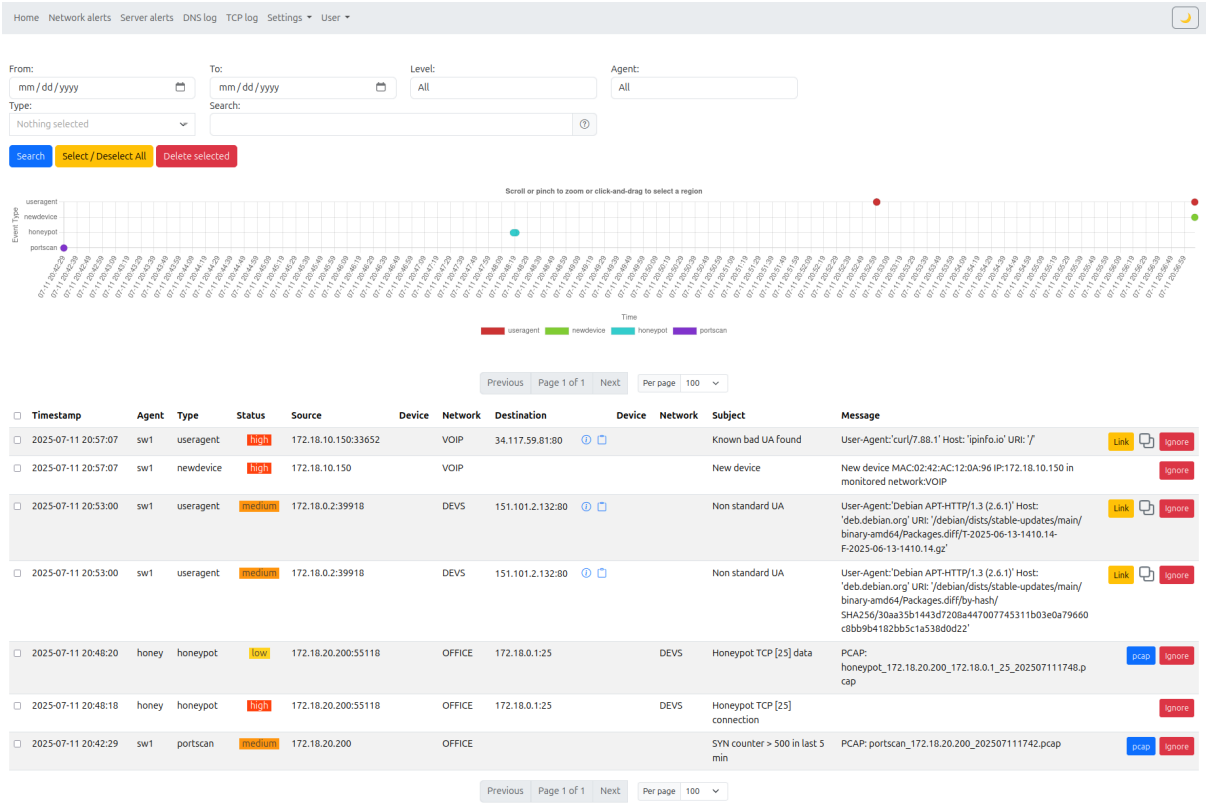
When an alert matches at least one include filter and no exclude filter, its source IP address is written to the configured blocklist on the firewall.

- Filters based on alert type, priority, agent, network segment, source IP/CIDR
- Exclude filters prevent blocking of known infrastructure, such as vulnerability scanners, management hosts, or critical servers
- Blocklist entries expire after a configurable time or are removed manually
- Each blocklist addition is recorded in the audit log

Enforcement is done by the firewall's own policy rules that reference the blocklist. Intrudect manages only the blocklist contents, not the firewall rules.

Delivery Channels

- Web UI (triage, snooze, search, delete)
- E-mail notifications
- Webhooks (Slack, Microsoft Teams, Mattermost, Discord, and others)
- JSON export to downstream systems (Elastic, Wazuh, Security Onion, etc.)
- Public REST API (/api/v1, bearer-token) for alert and metadata search, export, and automation



Network alerts view – alert triage with filtering and search

Central Web UI

Management

- Agent creation, deletion, and configuration
- Detection module enable/disable per agent
- Threshold and exception tuning for all detection modules
- Network segment and allowed service management
- Agent health monitoring: alerts when an agent stops checking in or sending metadata
- Remote agent updates (signed packages uploaded centrally, agents self-update)
- Firewall integration configuration and include/exclude filter management
- REST API for automations or agentic triage.

Access Control

- LDAP authentication against central AD
- Password-based local authentication with MFA (TOTP and YubiKey)
- Role-based permissions: control what each user can view or modify
- Audit log of all authentication events and configuration changes

Deployment and Operations

Area	Details
Packaging	Debian (.deb / APT) and RHEL (.rpm / DNF)
Architectures	amd64 / x86_64 and arm64
OS support	Ubuntu 24.04, RHEL 10
Configuration	JSON-based, generated and managed centrally through the Web UI
Connectivity	Agents require only outbound HTTPS to the Web UI. No telemetry or call-home from the platform. Optional features use external endpoints: Egress Agent tests and beacon document callbacks.
Updates	APT repository, manual, or centrally via Web UI (GPG-signed packages)
Licensing	Per-agent licensing. No feature tiers - every agent includes its full detection capability.
Deployment model	Self-hosted. Supports single-site, multi-site, and reseller/SaaS operation.

Hardware Requirements

All components can run as virtual machines or directly on hardware.

Component	CPU	RAM	Storage	Notes
Web UI	8 cores	32 GB+	100 GB+	NVMe/SSD required. 16 GB RAM absolute minimum. ~10 GB/month per 100 devices.
Network Agent	4 cores	8 GB	20–40 GB	Dedicated capture NIC(s) for SPAN traffic. Bare metal preferred.
Honeypot	2 cores	4 GB	20–40 GB	Separate management IP recommended.
Egress Agent	2 cores	4 GB	20–40 GB	No special hardware requirements.

Log Agent	2 cores	4 GB	20–40 GB	Can run on central log collector or individual servers.