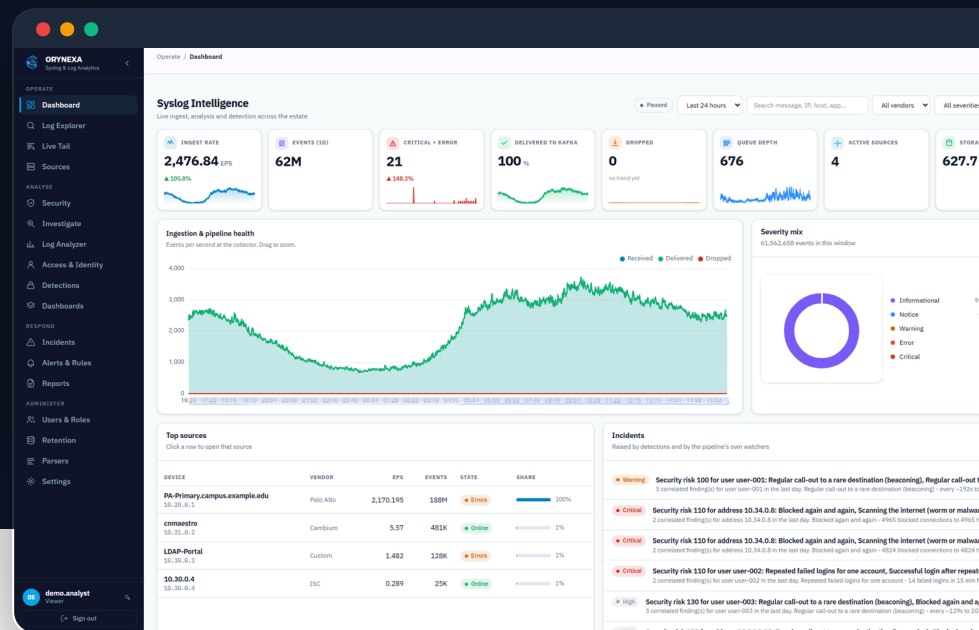


Orynexa Syslog Analyzer

The syslog server and security analyzer for your whole network. Every log from every firewall, switch, wireless controller and server — any vendor — turned into answers: who is doing what, which device has gone quiet, and who is trying to break in.



Any vendor

Recognised from the logs themselves — no code for a new device

20,000/s

Events per second end to end on one server, tested with no loss

17

Security detections every five minutes, tied to the user

On-prem

Runs on your server; logs never leave your network

THE PROBLEM

Logs everywhere, answers nowhere

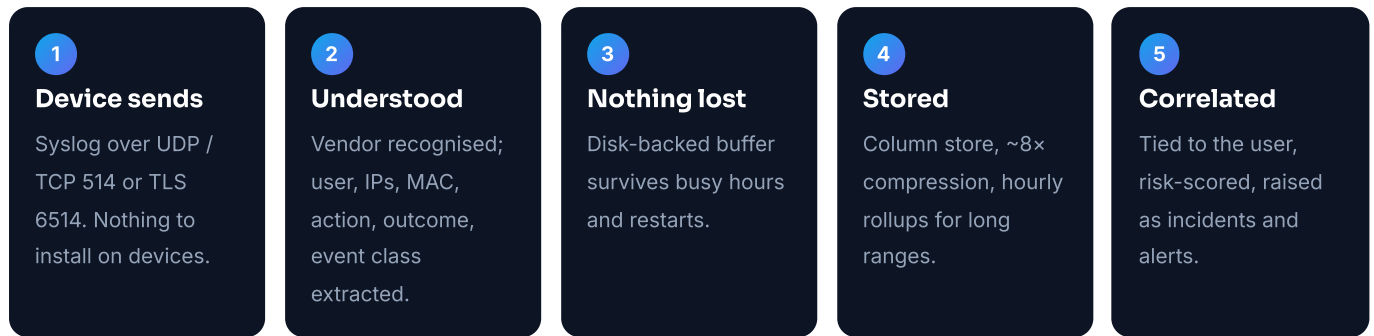
Each device writes its own log format, and the log is the only record of who logged in, what was blocked and what was changed. When an incident, a complaint or an audit arrives, teams search device by device — if the logs were kept at all.

THE ANSWER

One record, searchable in seconds

Orynexa keeps every log from every device in one compressed store, months long, and answers the questions directly: investigate any user or address, watch every device against its own normal, correlate attacks, alert the right people and hand auditors their report.

From a log line to an answer



CAPABILITIES

Everything your NOC & SOC need

- 

Any device, any vendor

Rule packs for firewalls, switches, wireless and servers. Unknown devices still yield addresses, users, MAC, action and severity; a rule built in the console goes live in 30 seconds without a restart.



Device health that learns

Each device judged against its own history: silent after its usual gap, quiet below 20% of its usual volume for that hour. Unregistered senders listed with a sample line and a vendor guess.



Security correlation

Seventeen detections every five minutes across all devices; findings linked to the logged-in user, risk scores that fade over 24 hours, incidents at high risk, suppressions for known scanners.



Incidents & alerts

Ready rules and your own, tested on real traffic before they are switched on. Email, Telegram or webhook; one alert per problem, resolved automatically when it stops.



Audit trail

Every console sign-in (failed too), change, search, export and investigation with user, client address and result; secrets are never recorded. Filters and CSV for auditors.



Search & live tail

Filter by time, device, severity, class, user, IP, MAC, interface or any field a device sends. Saved searches for the team, CSV export, and events followed live as they arrive.



Investigate any user or IP

Addresses used, logins and VPN sessions, applications and websites, destinations, blocks, firewall threats and every finding — with hourly timelines and one-click pivots.



Log analyzer

Vendor-free views: traffic, top talkers and denies, logins and failures, link and spanning-tree events, DHCP, system messages, and the messages nothing has classified yet.



Reports & compliance

Analyzer and compliance reports as PDF, daily, weekly or monthly, emailed on schedule — privileged logins, configuration changes with who and from where, failed logins, VPN users.



Operations built in

System Health page, container watchdog, nightly backups with a restore check and off-server copy, upgrades that roll back by themselves, cluster and HA planning page.

SUPPORTED DEVICES

Reads logs from

Firewalls	Palo Alto Networks, Fortinet, Cisco ASA / Firepower, Sophos, Check Point, Juniper SRX, SonicWall, WatchGuard, Huawei, pfSense / OPNsense
Switches & routers	Cisco IOS / NX-OS, Juniper, HPE Aruba, Huawei VRP, Dell OS10, MikroTik
Wireless	Cisco WLC / 9800, Aruba, Ruckus, Ubiquiti, Meraki, Cambium
Servers & apps	Linux, Windows Security events (via forwarder), VMware ESXi, DHCP, LDAP and any RFC 3164 / 5424 sender

REPORTS

Analyzer report

Top sources, events by class and severity, denied clients, authentication failures, interface issues, unclassified share, alerts and incidents.

Compliance report

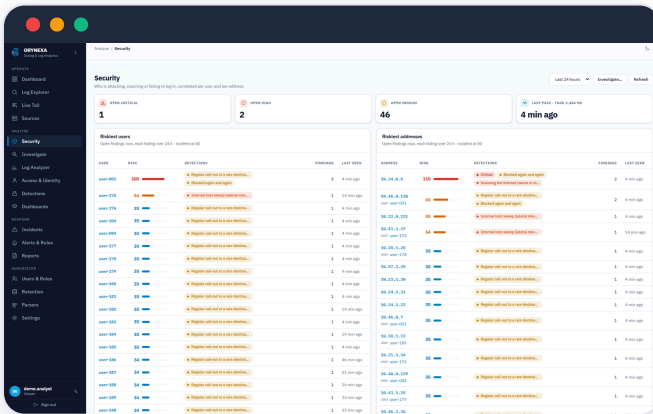
Privileged account activity, configuration changes with user, action, what changed and the admin's machine, failed logins by account and address, VPN users, console activity, exports and findings. For ISO 27001, PCI DSS and CERT-In.

SECURITY DETECTIONS

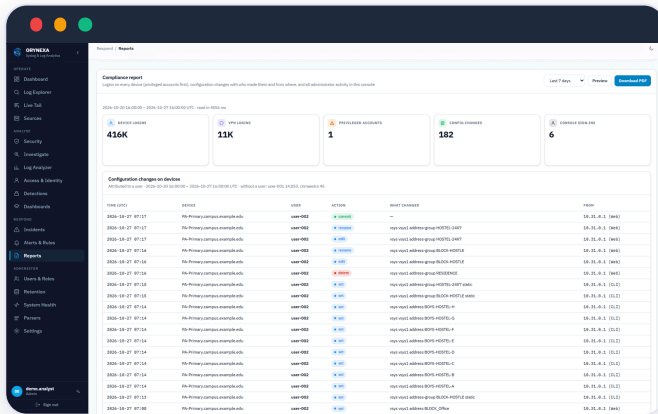
What it catches

- **Brute force** against an account or from an address
- **Password spraying** across many accounts
- **Success after failures** — a guessed password
- **Privileged login** (admin, root...) from a new address
- **Port scan** and **internal host sweep** (lateral movement)
- **Internet scanning** on worm ports — an infected PC
- **Deny storm** and **inbound flood**
- **Beaconing** — regular call-outs to a rare destination
- **Firewall threats** and **bad URL categories**
- **New message type** or **message rate spike** on a device
- **Error spike** and **volume spike** against the usual hour

Risk per user and address; an incident opens at risk 80 or on any critical finding, with notification.



Security: riskiest users and addresses and the detections behind them.



Compliance: every configuration change, who made it and from where.

Specifications

Deployment	On-premises, on your server or VM; containers supervised by systemd. One-command installer; no cloud dependency
Operating system	Rocky / Alma / RHEL / CentOS Stream, Fedora, Ubuntu, Debian (64-bit)
Log input	Syslog UDP 514, TCP 514 (octet-counted or newline framing), TLS 6514 (RFC 5425); RFC 3164 and 5424
Architecture	Collector → Kafka (disk buffer) → loaders → ClickHouse column store; PostgreSQL for configuration; HTTPS web console
Performance	20,000 events/s end to end with zero loss on 16 cores / 64 GB (tested); ~29,000 events/s per collector
Storage	~215 bytes per event on disk (~8× compression); retention from days to years, per severity or event class
Search	Time-bounded queries on indexed fields; any parsed field as a filter; saved searches; CSV export; live tail
Alerting	Email (SMTP), Telegram, webhook; rule test against recent traffic; deduplication and auto-resolve
Reports	PDF analyzer and compliance reports; on demand or scheduled daily / weekly / monthly by email
Access control	Viewer, engineer and admin roles; hashed passwords; full audit trail of sign-ins, changes, searches and exports
Security	Only 443, 514 and 6514 exposed; databases on localhost; secrets generated per install; your own TLS certificate
Resilience	Service supervision and watchdog; nightly backup with automatic restore check and off-server copy; upgrades with automatic rollback
Scale-out & HA	Cluster-ready from install: replicas for high availability, shards for capacity, additional collectors and Kafka brokers
Time	NTP servers set and applied from the console, with live sync status, source and offset

SIZING

AVERAGE EVENTS / S	SERVER	DISK PER DAY	DISK FOR 180 DAYS
Up to 1,000	8 cores, 32 GB RAM	~19 GB	~4.2 TB
Up to 5,000	8 cores, 32 GB RAM	~93 GB	~21 TB
Up to 15,000	16 cores, 64 GB RAM	~280 GB	~63 TB
Above 15,000	Cluster of 2–3 servers	Sized with you from a day of your own traffic	

The 180-day column includes 25% headroom for merges. Shorter retention for traffic logs (for example 30 days) and longer for logins and changes often halves it.

See your own network in a day

We install Orynexa on your server, connect your firewalls, switches and controllers, and walk your team through it. Ask for a demo or a trial.

Optimus Secure

info@opsec.co.in

+91 95901 37009

opsec.co.in