

WIRETRACE INTEGRATIONS OVERVIEW

Connects to the tools you already run, in formats they already understand

What WireTrace sends, what it receives and what your tools can request from it, organised by direction and purpose, with each integration stated exactly as it works.



For: Security architects, SOC engineering, network and identity teams

WireTrace is the intelligence and decision layer in your security stack, not a replacement for it. Its value reaches people through the tools they already run: alerts into the SIEM, data into automation, rule proposals to firewall teams and asset context to network access control. This overview lists every integration by **direction** (what WireTrace receives, sends, or lets your tools request) and by **purpose**.

01 Principles

Open formats first

Syslog, JSON, SNMP, STIX 2.1, CSV and plain-text rule syntax. Any tool that understands the format can consume WireTrace without a vendor-specific app.

On your appliance

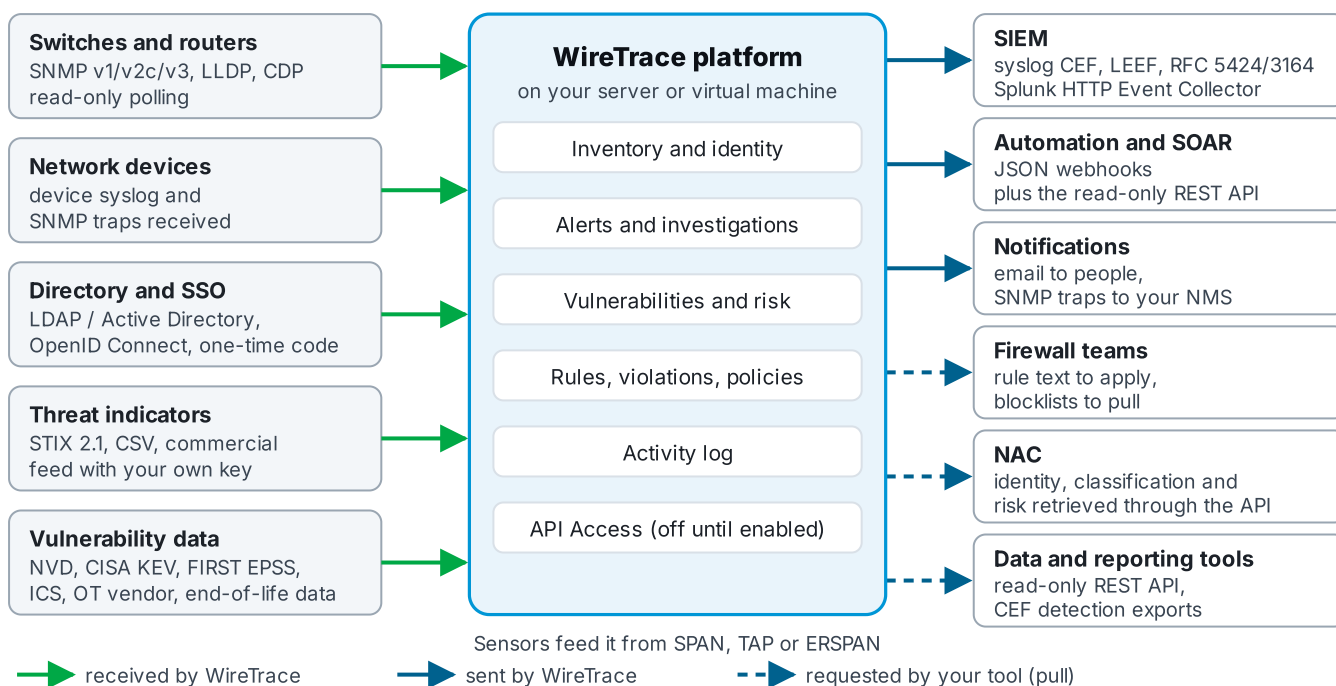
Integrations, including the REST API, run on your WireTrace platform. Nothing is relayed through a vendor service.

Your controls enforce

WireTrace supplies identity, risk, intent and proposed rules. Your firewalls, NAC and switches remain the enforcement points.

INBOUND: CONTEXT, SIGN-IN, INTELLIGENCE

OUTBOUND: ALERTS, DATA, HAND-OFF



WireTrace integration map. Inbound integrations add context, sign-in and intelligence; outbound integrations deliver alerts and decisions, or answer requests from your tools. Every integration runs from your own WireTrace platform.

02 Security operations: alerts and notifications out

Integration	What it does	Formats and transport
SIEM over syslog	Forwards alerts to any SIEM, filtered by alert type and minimum severity.	CEF, LEEF, RFC 5424, RFC 3164; UDP, TCP or TLS
Splunk HTTP Event Collector	Native Splunk HTTP Event Collector output.	HTTP Event Collector
IBM QRadar	Ingests WireTrace alerts through standard syslog formats.	LEEF over syslog
Microsoft Sentinel	Ingests WireTrace alerts through standard syslog formats.	CEF over syslog
Webhooks	Sends events to automation and SOAR workflows. SOAR platforms consume WireTrace through webhooks and the REST API.	JSON
Email	Alerts, policy notifications and user invitations.	SMTP
SNMP traps	Trap notifications to your network management system.	SNMP traps

03 Data access: what your tools can request

API Access is a read-only REST API that exposes assets, changes, risk, vulnerabilities, alerts, threat matches and exports. It is designed to be safe to switch on:

- **OAuth 2.0 client credentials:** each consuming application has its own client.
- **Read-only:** the API cannot change anything in WireTrace.

- **Scoped tokens:** a client is granted only the data areas it needs.
- **Per-client rate limits and IP allowlists.**
- **On your appliance:** it runs on your WireTrace platform, not a vendor service.
- **Off until enabled** by an administrator.

IP, domain and URL blocklists and CEF detection exports are available for tools to pull on their own schedule.

04 Enforcement hand-off

WireTrace provides the intelligence, policy intent and continuous validation layer for segmentation; your existing firewalls, NAC and switches enforce it. The hand-off is explicit and reviewable:

To	What WireTrace provides	How
Firewall teams	Proposed block rules derived from traffic rules and violations, for review and application by your team.	Text in iptables, nftables, Cisco IOS or pf syntax
Firewalls	IP, domain and URL blocklists from threat-indicator matches.	Pulled by the firewall through the API
Network access control	Asset identity, classification and risk, so a NAC can enrich its own policy decisions.	Retrieved by the NAC through the REST API

What WireTrace does not do. It does not push configuration to firewalls, NAC or switches. Rules leave as text for your team to review and apply, and blocklists and context are pulled by the receiving system. Changes stay under your existing change control.

05 Network enrichment in

What WireTrace receives

- SNMP v1, v2c and v3 from switches and routers, read-only
- LLDP and CDP neighbour information
- Device syslog and SNMP traps sent to WireTrace

What it adds

- Port-level connectivity: which device is on which switch port
- Neighbour relationships between network devices
- Hardware details of switches and routers

Polling needs SNMP targets and read-only credentials configured by an administrator, and runs from the platform's management interface. WireTrace never writes configuration over SNMP.

06 Identity and access

Users sign in through **LDAP/Active Directory** (over LDAPS or STARTTLS), **OpenID Connect single sign-on** with your identity provider, for example Microsoft Entra ID or Google Workspace, or an **email one-time passcode**. Whichever method is used, role-based access control in WireTrace decides what each user can see and do, and tenants on a multi-tenant platform keep their own users and permissions.

07 Intelligence inputs

Input	Sources	Used for
Threat indicators	Public threat-intelligence feeds; STIX 2.1 import and export; CSV indicator lists; commercial feeds using your own key.	Matching observed IPs, ranges, domains, URLs, file hashes and TLS fingerprints.
Vulnerability intelligence	NVD, CISA KEV, FIRST EPSS, CISA ICS advisories, OT vendor advisories, and end-of-life data that also works offline.	Matching device software, firmware and OT products, prioritised by exploitation.

Connected appliances refresh automatically; air-gapped sites import a checksummed offline bundle.

08 Integration classes

The class states what is built into WireTrace and what relies on a standard format or the API.

Class	Meaning	Integrations
Supported	Built in, configured in the console.	Syslog, Splunk HEC, webhooks, email, SNMP traps, inbound syslog, SNMP/LLDP/CDP, LDAP/AD, OIDC SSO, one-time passcode, STIX 2.1, CSV and commercial feeds, vulnerability sources, REST API, rule-text export
Via standard formats	Ingests a standard format; no dedicated connector.	IBM QRadar (LEEF over syslog), Microsoft Sentinel (CEF over syslog), other SIEMs over syslog
Through the API	Requests data from the REST API or consumes webhooks.	SOAR platforms (webhooks and API), network access control (identity, classification and risk), firewalls and security tools pulling blocklists and CEF exports

Limits, stated plainly

- WireTrace hands off to enforcement; it does not push rules or configuration to firewalls, NAC or switches.
- QRadar, Microsoft Sentinel, SOAR and NAC integrations use standard formats or the API; there is no dedicated app or connector.
- The REST API is read-only and off until enabled. Switch enrichment is read-only and needs SNMP access you configure. Single sign-on uses OpenID Connect.
- Some vulnerability and advisory sources need internet access; on air-gapped sites the offline bundle refreshes threat indicators and NVD, CISA KEV and EPSS data.

Map WireTrace onto your tooling

A technical session maps your SIEM, automation, firewall, NAC and identity tooling to WireTrace integration points, and an evaluation shows the alerts and data your teams would receive.

Book a demo at wiretrace.io/request-demo or email sales@wiretrace.io