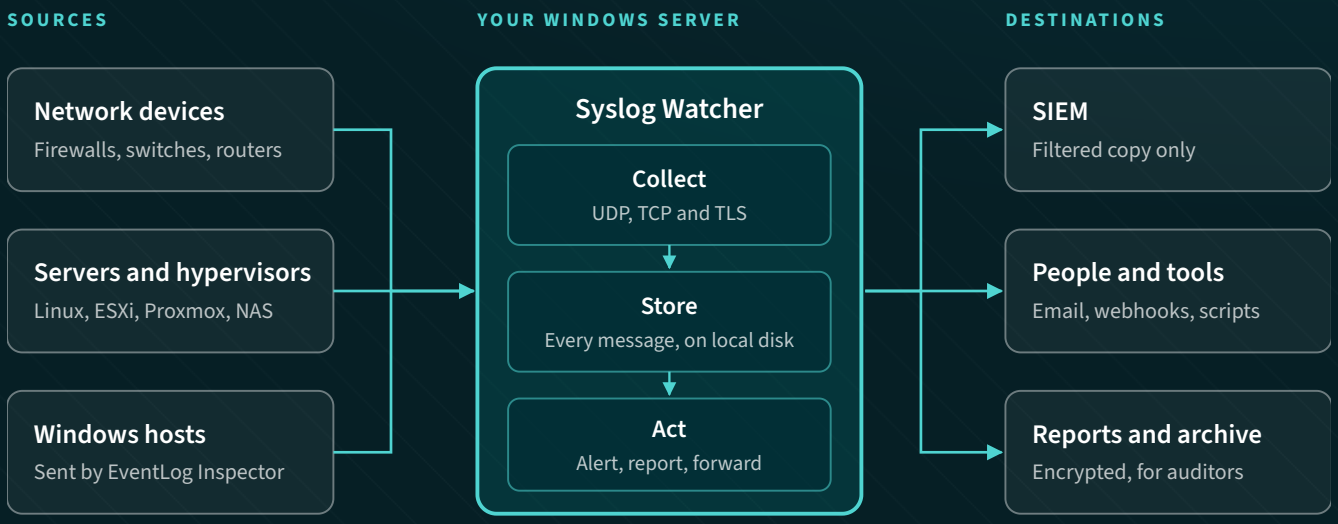
EZ5

WHITE PAPER

Syslog Watcher

Centralized Log Management on Windows Server

Collect, keep, search, alert on and forward the syslog from every firewall, switch, server and appliance on the network, on the Windows Server you already run.



01

Executive summary

Syslog Watcher gives a Windows-based IT team one place to collect, keep, search, alert on and forward the syslog from every firewall, switch, server and appliance on the network, for a one-time license fee.

Windows ships with no syslog server. Without one, device logs stay scattered on the devices that wrote them, roll over within hours, and are missing when an incident or an audit needs them. Cloud log platforms solve that, but bill per gigabyte ingested and move the data off the network.

Syslog Watcher runs on the Windows Server or desktop the team already manages. It receives syslog over UDP, TCP and TLS, stores it in a local SQLite-based store that writes over 35,000 messages per second, and keeps an encrypted, compressed archive for retention rules such as PCI DSS, HIPAA, SOX and GDPR. Filters, alerts and reports help staff find and act on problems, and filtered forwarding sends only the relevant messages to a SIEM.

The result for the business

Faster troubleshooting

One searchable timeline across all devices instead of logging in to each one.

Audit-ready retention

Logs kept on-premises, encrypted, for as long as policy requires.

Lower SIEM cost

Noise is filtered out before it reaches a per-GB ingest bill.

Predictable spend

A perpetual license with 1, 3 or 5 years of maintenance, no per-GB fees.

23,000+	89	35,000+	2007
licenses sold to administrators	countries	messages per second written to storage	version 1.0 released

02

The problem: device logs are scattered and short-lived

Every firewall, switch, router, access point, hypervisor and NAS on a network writes a running record of what it does, almost always as syslog. Each device keeps that record in a small local buffer, so on a busy firewall the evidence of an event can be overwritten within hours.

Windows-based teams often miss this. Windows servers keep their own Event Log, but Windows has no syslog server, so nothing collects the logs from network devices. As a result:

Logs are scattered

To trace one outage an admin logs in to the firewall, then the switch, then the VPN appliance, and lines up timestamps by hand.

Logs are short-lived

Device buffers roll over, and a reboot often clears them. The record of last month's incident is gone.

Logs are unwatched

A failing disk, a brute-force attempt or a config change is written to a log that nobody reads until something breaks.

Logs can't be shown to auditors

An auditor asks for 12 months of firewall logs, and there is no central, protected copy to show.

> Windows has no syslog server, so nothing collects the logs from network devices.

03

Why it matters to the business

Scattered device logs cost time during outages, put audits at risk, and, once a cloud SIEM is involved, cost money by the gigabyte.

Concern	What goes wrong without central syslog	What a central syslog server changes
Downtime	Root cause is traced device by device, by hand	One timeline across all devices, searchable by time, device and text
Compliance	No retained, protected copy of device logs for the audit period	Encrypted archive kept for the period the policy sets (PCI DSS, HIPAA, SOX, GDPR, CCPA)
Security	Brute-force attempts and config changes go unseen	Alerts by email or HTTP when a matching message arrives
SIEM cost	Every heartbeat and debug line is billed at ingest	Only the messages worth indexing are forwarded; the rest stay on local disk
Data control	Cloud logging moves device logs off-site	Logs stay on a Windows server inside the network

SIEM cost is usually the easiest saving to measure. Platforms such as Splunk bill on daily ingest, and much of that volume is traffic nobody searches. One customer put it this way:

65%

less Splunk ingestion

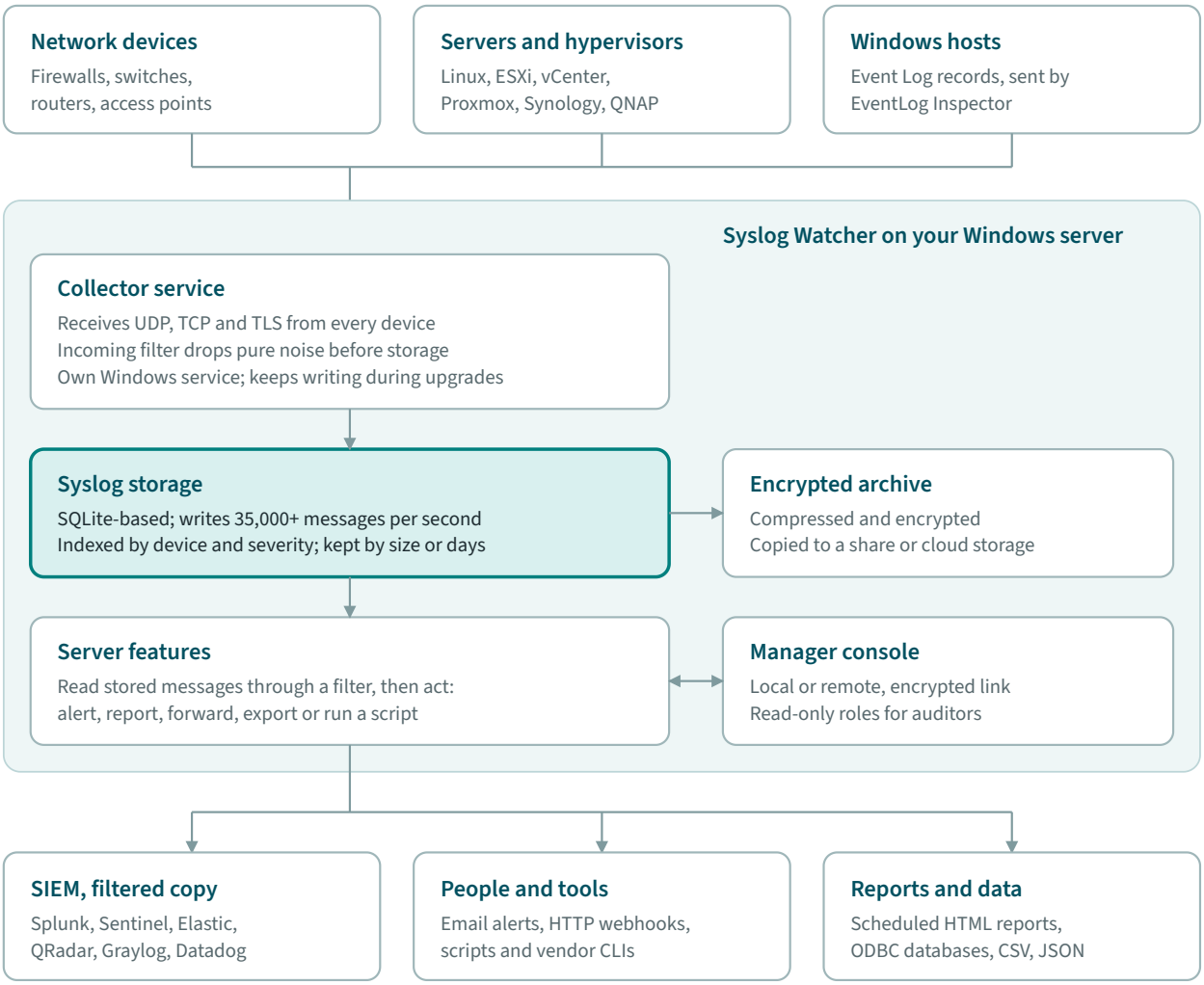
"Since deploying Syslog Watcher, we cut our Splunk ingestion by 65% without losing visibility on critical events—and trimmed our annual license cost."

— IT Manager, Swiss financial services company

04

How Syslog Watcher works

Syslog Watcher is Windows software in three parts: a collector service that receives messages, a local store that keeps them, and a Server that acts on them.



The collector writes to storage before any feature reads it. A SIEM outage, a paused forwarding rule or a Server upgrade therefore loses nothing: each feature resumes where it stopped, backlog included. The Manager console connects locally, or over an encrypted link from an admin's own workstation.

04

How Syslog Watcher works (continued)

Together, these parts provide eight functions:

Function	What it does	Key specifics
Collect	Receives syslog from any device	UDP (RFC 5426), TCP (RFC 6587), TLS (RFC 5425); IPv4 and IPv6; relayed messages; incoming filter by severity, keyword or regex
Store	Keeps every message on local disk	SQLite-based; 35,000+ msg/s write, 250,000+ msg/s sequential read; indexed by originator and severity; retention by size or days
Archive	Keeps a long-term copy for audits	Compressed to hold about 10× more messages in the same space; optionally encrypted; a script after each archive sync can copy it to cloud storage or a network share
Parse	Turns raw text into named fields	RFC 3164 and RFC 5424, CEF, UTF-8; regex parsers per originator; built-in parsers for Cisco, Fortinet, Juniper, Netgear, Palo Alto, SonicWall, Sophos, Ubiquiti
View and search	Finds the messages behind a fault	Virtualized grid for millions of rows; filter row; color rules; saved view presets; Storage tab with a calendar of message volume
Alert	Notifies staff and other systems	Email (SMTP) to alert groups, with several alerts combined into one email; HTTP POST/PUT to webhooks and ticketing APIs; run a script or program per message
Report	Summarizes activity for managers and auditors	HTML/CSS/JavaScript templates; SQL-backed data commands; scheduled one-time, weekly or monthly runs
Forward and export	Sends messages to other tools	Filtered forwarding over UDP/TCP/TLS to Splunk, Sentinel, Elastic, Graylog, QRadar, Datadog, Sumo Logic; export to ODBC databases or CSV, XML, JSON files

05

Deployment

Installation takes about five minutes on a Windows host the team already runs. It needs no Linux VM or cloud account.

~5 min

to install on a Windows host you already run

Item	Requirement or default
Operating system	64-bit Windows Server 2012 R2, 2016, 2019, 2022, 2025; Windows 8.1, 10 or 11
Hardware for Syslog Watcher itself	64-bit CPU, 1 GB RAM; disk sized to the retention period
Where it runs	Bare metal, Hyper-V, VMware, or a Windows instance on AWS, Azure or GCP
Account	Local administrator to install; the collector service runs as Local System

06

Use cases

The same installation serves the network team, the security team, the auditor and the SIEM.

Network troubleshooting

A VPN tunnel drops at 02:14. The admin opens the Storage calendar, narrows to that minute, and filters to the firewall and the core switch. The link-down message on the switch, one second before the tunnel event, is the root cause. Nobody had to log in to the devices one by one.

Security monitoring

An alert rule matches repeated authentication failures on the firewall's admin interface. Syslog Watcher emails the on-call group and posts the event to the ticketing system over HTTP. A script action can block the source address through the vendor's CLI.

Compliance and audit

Device logs are collected over TLS, kept in an encrypted, compressed archive, and copied nightly to a network share or cloud storage. A scheduled monthly report summarizes configuration changes and login activity for the auditor, who can also connect with a read-only account.

SIEM cost control

All traffic lands in Syslog Watcher first. Only authentication events, configuration changes, VPN sessions and high-severity faults are forwarded to Splunk or Sentinel. Heartbeats and debug output stay on local disk, searchable but never billed.

Branch offices and small sites

A branch with one Windows server and no Linux host collects its own firewall and switch logs, with no new operating system to patch.

07

Licensing

Syslog Watcher is bought once and sized by the number of devices, so its cost is a fixed line in the budget rather than a usage bill that rises with log volume.

Professional	Enterprise	Ultimate
Up to 50 devices (syslog originators)	**Up to 250** devices (syslog originators)	**Unlimited** devices (syslog originators)
500,000 messages per hour	**5,000,000** messages per hour	**Unlimited** messages per hour
A single site or a small business network	Several sites, or a mid-size network	Large or fast-growing networks, with no cap to plan around

What the license covers

- **Perpetual use.** The license never expires and is not a subscription.
- **Maintenance for 1, 3 or 5 years.** Version upgrades, security updates and technical support for the term you choose. Maintenance can be renewed or extended.
- **No usage fees.** Nothing is charged per GB ingested, per user or per stored message.

08

Getting started

The lowest-risk way to evaluate Syslog Watcher is on your own network, at no cost.

1. Download the installer and request a free 30-day evaluation of the license tier you plan to buy. The evaluation is the full feature set, and technical support is included.
2. Buy when ready. The 30-day money-back guarantee extends the risk-free window to up to 60 days.

CONTACT

EZ5 Systems Ltd.

The lowest-risk way to evaluate Syslog Watcher is on your own network, at no cost.

DOWNLOAD

ezfive.com/syslog-watcher

Installer and 30-day evaluation

DOCUMENTATION

Syslog Watcher User Guide

docs.ezfive.com

SALES AND MAINTENANCE RENEWALS

sales@ezfive.com

TECHNICAL QUESTIONS

support@ezfive.com

EZ5

© 2026 EZ5 Systems Ltd. All rights reserved.
Splunk, Microsoft Sentinel, Elastic and other names mentioned are trademarks of their respective owners.