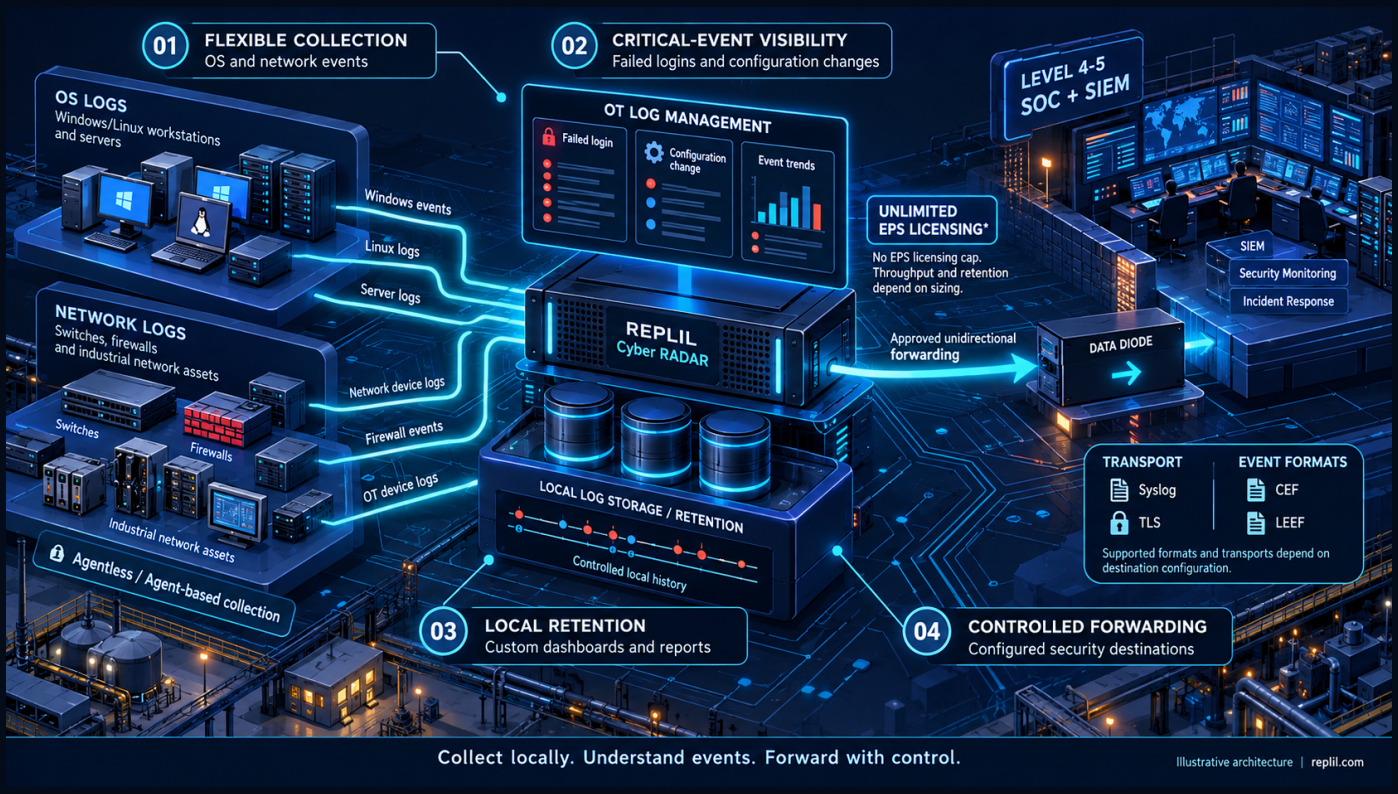
Collect locally. Forward with control.

Bring operating-system and network events into local retention, custom dashboards and configured security destinations.



Illustrative workflow. Connections and permissions follow the approved deployment.

PRODUCT WORKFLOWS / KEY CAPABILITIES

01 Flexible event collection

Collect OS and network logs with agentless and agent-based options.

02 Critical-event visibility

Review failed logins, configuration changes and relevant event trends.

03 Retention and reporting

Retain events locally and build customized dashboards and reports.

04 Controlled forwarding

Use approved one-way diode paths to SIEM where deployed. Separate event formats from transport configuration.

BUILT AROUND INDUSTRIAL OPERATIONS

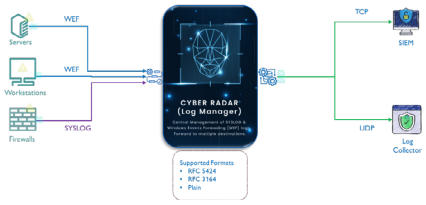
Description / capabilities / deployment

CyberRadar

DataSheet

Introducing **REPLIL-CyberRadar**, our cutting-edge Log Management Engine is designed to efficiently handle Windows Event Forwarding (WEF) and syslog events while providing unparalleled reliability and scalability.

REPLIL-CyberRadar is the ideal solution for organizations seeking a robust, scalable, and secure log management platform capable of handling diverse event types and forwarding them to various destinations. Ensure your logging infrastructure is ready for any challenge with our state-of-the-art solution.



Key Features

Comprehensive Event Handling:

- Seamlessly manage and process WEF and syslog events from diverse sources.
- Ensure that all log data is captured and organized for easy retrieval and analysis.

High Availability:

- With high availability feature our Log Management Engine ensures uninterrupted log collection and processing.
- Redundant systems and failover mechanisms guarantee continuous operation, even in the face of hardware or network failures.

Scalability Without EPS Limitations:

- Our engine is designed to handle an unlimited number of events per second (EPS), making it ideal for environments of any size.
- Scale effortlessly as your logging needs grow, without worrying about performance bottlenecks.

Flexible Log Forwarding:

- Forward logs to single or multiple destinations, including SIEM systems, databases, and other analysis tools.
- Ensure that critical log data is always available where it is needed most, enhancing your overall security and operational visibility.

Enhanced Security and Compliance:

- Store and archive logs securely to meet regulatory compliance requirements and ensure data integrity.
- Benefit from advanced security features that protect your log data from unauthorized access and tampering.

User-Friendly Interface:

- Access and manage your logs through an intuitive, web-based interface that simplifies configuration and monitoring.
- Customize dashboards and reports with ease using our drag-and-drop builder and next-generation report designer.

7969 NW 2nd Street #1013 Miami
33126 Unites States

(+1) 805 742 4848

sales@replil.com

www.replil.com

CyberRadar

DataSheet

REPLIL™

System Requirements:

HARDWARE OR SOFTWARE	REQUIREMENT
Operating System	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016
CPU	1.2 GHz Dual Core processor
Memory	16 GB
Hard drive space	350 MB
Database Server	PostgreSQL v16

Port requirements for CyberRadar:

PORT	PROTOCOL	SERVICE	DIRECTION	DESCRIPTION
514 (default)	UDP	Syslog Service	Inbound	Syslog messages listened for and received by the Syslog Server
5144 (default)	TCP	Syslog Service	Inbound	Syslog messages listened for and received by the Syslog Server
8080 (default)	TCP	Web Server	Inbound	Standard secure port for HTTPS

Estimated EPS Throughput Requirements:

EPS	vCPU	RAM
0-1K	4	16 GB
1-3K	8	16 GB
3-5K	14	24GB
5K-10K	28	32GB
10K-20K	28	64GB
20K-30K	48	64GB

7969 NW 2nd Street #1013 Miami
33126 Unites States

(+1) 805 742 4848

sales@replil.com

www.replil.com