

SyskeyOT and Phoenix Contact Security Solutions

Raptor Switching platform with integrated Scribbler Log Manager – a highly secure, scalable, and reliable centralized log management solution for OT



Overview

Today, secure operation of Industrial Control Systems is mandatory to protect critical infrastructures around the world. Mission Critical Networks, such as power utilities, nuclear facilities, water utilities, and oil and gas, must deploy multiple security measures following defense in depth principles. OT environments often operate in harsh, remote, and inaccessible locations, adding to the complexity of implementing security measures.

One critical component of OT cyber security systems is log management. Phoenix Contact and SyskeyOT have established a strategic partnership to address the challenges of managing log data in a heterogeneous environment with a wide array of devices such as intelligent electronic devices (IEDs), remote terminal units (RTUs), routers, switches, computers, and other specialized devices. Integrating SyskeyOT's Scribbler log manager onto Phoenix Contact's leading edge Raptor series L2/L3 multiservice platform provides an efficient logging solution, requiring no additional hardware.

Scribbler Log Manager is a highly secure, scalable, and reliable centralized log management solution for enterprises that value their log data. An invaluable tool for administrators for identifying and diagnosing problems with their infrastructure, it consists of multiple components for collecting, filtering, storing, analyzing, and forwarding logs in real time. Its web-based analytical dashboard provides deep insight about the log data, the progress, and the state of the system.

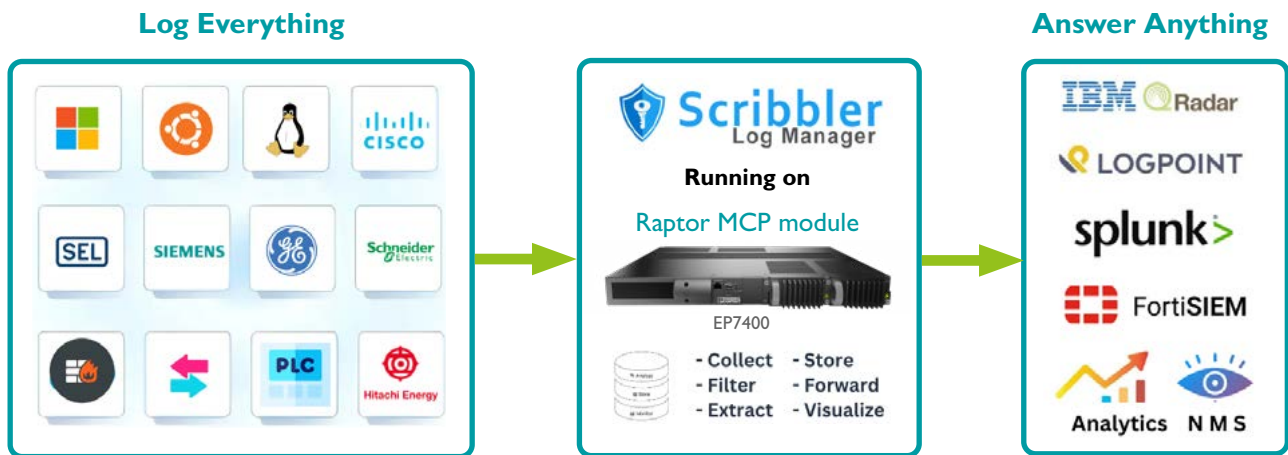
| | |
|-----------------|--|
| Benefits | <ul style="list-style-type: none">• Network Connectivity – singular multiservice platform solution with network communications, and facility log management on a single appliance• Reliability in the harshest environments – compliant with IEC61850 and IEEE 1613 standards• Ease of implementation – simplified GUI management, smaller footprint, single power source, simple integration• Collects logs from heterogenous devices• Compatible with industry leading Security Information and Event Management (SIEM) solutions• Supports encrypted backup, tamper prevention, and detection• Secured Transport Layer Security (TLS) transportation of logs to security operations centers (SOC)• Powerful log filter for reducing SIEM ingestion cost• Simple, competitive, and straight forward pricing |
|-----------------|--|



Solution

The Raptor is an intelligent cybersecure hardware platform with 64 Gb/s full line speed with up to 4 x 10Gb/s + 24 1Gb/s ports running a feature rich embedded OS. The Raptor embedded OS is an all-encompassing operating system that supports L2/L3 switching and routing on a single platform. Its modular system of field replaceable modules, redundant hot-swappable power supplies, and ability to run third party software applications makes it a very flexible platform for today and the future. Combined with SyskeyOT Scribbler, Raptor will enable industrial networks to have a “best in breed” log management solution right to the outer edge of OT networks.

Scribbler Best-in-class Log Collection & Integration



Scribbler Key Features




- **Visibility & Analytics** – collects, filters, stores, forwards, and searches logs in real time. A web-based analytical dashboard provides detailed insight about the logs.
- **Powerful REGEX Filter** – rule engine for filtering out junk logs from the system, thus saving cost on both hardware resources and network bandwidth.
- **Role-based access control** and active directory single sign on; supports encryption at REST.
- **Performance** – Scribbler was designed from the ground up to be efficient and with high performance. Log collection and search have very fast response times.
- **Backup** of logs to a local drive or an external network attached storage (NAS) over server message block (SMB).
- **Built in SNMP agent** – reports service health status to an external asset monitoring solution.
- **Standards compliant** – Syslog over UDP/TCP/TLS, CEF, LEEF, SNMP Traps RFC 3164, RFC 5424, RFC 5425, RFC 5426, RFC 6587.
- **SNMP traps** – collects and forwards SNMP traps to upstream NMS, and transforms the traps to Syslog which can be stored and forwarded to any upstream SIEM.
- **Windows Event Logs** – Scribbler supports both Agent based and Agentless Windows Event Log Collection methods.
- **Central Management** – Remote Scribbler instances support Central Management Console which handles Configuration, Patch Updates, and Health Status Monitoring of Scribbler instances.

Scribbler Value Proposition

- **Interoperability & integration** – Scribbler is compliant with all Syslog standards and protocols and integrates with all SIEM solutions for log ingestion through Syslog.
- **Perpetual validity** and standard 3 years support with FREE upgrades
- **Unlimited log sources and log volume**

Related Products



| Chassis | Description | Designation | Item No. |
|---|---|------------------------------|----------|
|  | FL SWITCH EP7400 Series Chassis. IEC 61850-3 / IEEE 1613, Layer 2/3 Switch, -40°C to +85°C Operating Range. Supports up to 28 ports total. | FL SWITCH EP7428R-L3F1 | 1144353 |
| | FL SWITCH EP7400 Series Chassis. IEC 61850-3 / IEEE 1613, Layer 2/3 Switch, -40°C to +85°C Operating Range, Supports up to 24-ports PoE, 28 ports total. | FL SWITCH EP7428R-L3F1P | 1539668 |
| Chassis | Description | Designation | Item No. |
|  | FL SWITCH EP7500 Series Chassis Security enabled. IEC 61850-3 / IEEE 1613, Layer 2/3 Switch, -40°C to +85°C Operating Range. Supports up to 28 ports total. | FL SWITCH EP7528R-L3F1 | 1539667 |
| MCP Computing Module | Description | Designation | Item No. |
|  | MCP Computing Module , Ubuntu, 256GB storage | FL SWITCH EP7400-MCP-L-256GB | 1539661 |
| | MCP Computing Module , Ubuntu, 512GB storage | FL SWITCH EP7400-MCP-L-512GB | 1539663 |
| | MCP Computing Module , Ubuntu, 1TB storage | FL SWITCH EP7400-MCP-L-1TB | 1539665 |
| | MCP Computing Module , Ubuntu, 2TB storage | FL SWITCH EP7400-MCP-L-2TB | 1539666 |

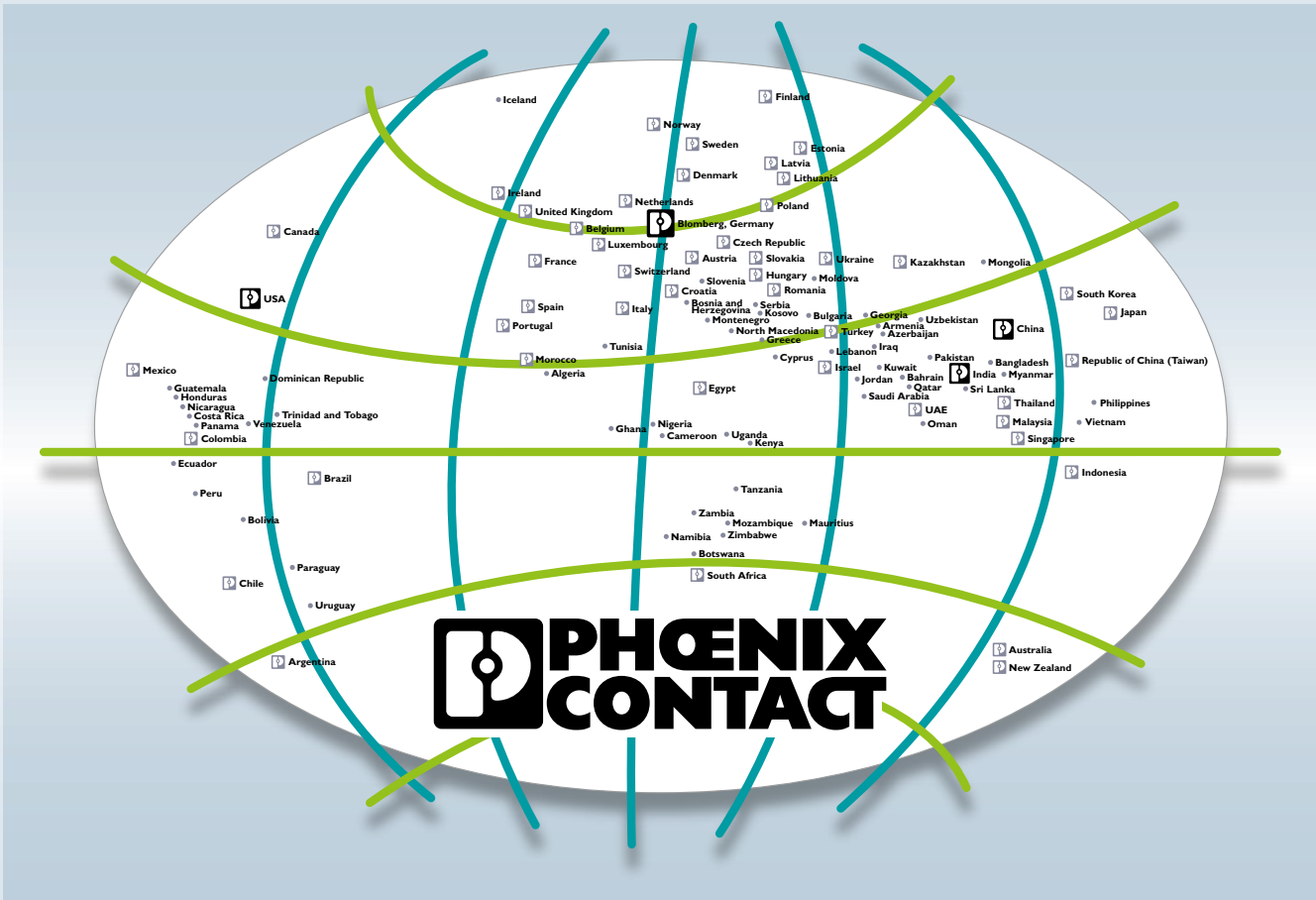
About Syskey Softlabs

Syskey Softlabs Pvt Limited (Doing Business As 'SyskeyOT') is a global provider of cybersecurity software products / solutions for Operation Technology / Industrial Control Systems (OT/ICS) networks. SyskeyOT helps verticals such as energy, water, oil & gas, transportation, and other industrial sectors to meet the growing demands for cybersecurity solutions with highly secure and scalable Centralized OT Log Management Solution, OT Asset Inventory & Vulnerability Management Solution and OT Network Management Solution. SyskeyOT builds competitive advantage with cuttingedge technology, security focused solutions, quality technical support and customer centric products. Visit <https://syskeyot.com> to learn more.

Support: support@syskeyot.com

Sales: sales@syskeyot.com

Address: Syskey Softlabs Pvt Ltd, GF-31, TIDEL Park, ELCOT SEZ, Coimbatore-641014, Tamil Nadu, India



Open communication with customers and partners worldwide

Phoenix Contact is a global market leader based in Germany. We are known for producing future-oriented products and solutions for the electrification, networking, and automation of all sectors of the economy and infrastructure. With a global network reaching across more than 100 countries with over 22,000 employees, we maintain close relationships with our customers, something we believe is essential for our common success.

Our wide range of innovative products makes it easy for our customers to implement the latest technology in a variety of applications and industries. This especially applies to the target markets of energy, infrastructure, industry, and mobility.

You can find your local partner at

[phoenixcontact.com](https://www.phoenixcontact.com)