



RingShield™

Secured Industrial Network Data Management Platform

RingShield™ integrates firewall, operation audit, security monitoring, data switching and network management solutions into one highly compact and reliable form factor that can fit into most of any industrial applications where highly secured data switching and management is mandatory. This line of products are equipped with many options of IP67, wide temp -40C - 75C, layer 2 and layer 3 data switching, MTBF of 50+ years, in addition to the following security features:

A Firewall Function

- 1. Data Link data filtering**
 - Use checking and measuring method to bundle IP and MAC addresses to filter IP, TCP, UDP, ICMP, etc. and other layer 3 protocols. They can also filter ARP, 802.1q and other layer 2 protocols.
- 2. Network Attack Check and Measurement**
 - Support checking and measuring the network attacks such as ICMP Flood, Ping of Deat, UDP Flood, Land, Tear Drop, SYN, etc.
 - Support SYN Cookie RST technology.
- 3. Deep Protocol Filtering**
 - Support worldwide popular industrial fieldbus protocols forwarding over layer 2 and layer 3 networks;
 - Support worldwide popular industrial fieldbus protocols deep analysis, filtering such as OPC, Modbus, IEC60870-5-104, IEC61850 MMS, IEC61850 GOOSE, DNP3, EnIP, CIP, Profinet, Siemens S7, OMRON Fin, etc.
 - Support OPC dynamic port open.
 - Support self-defined protocol filtering
- 4. Daily Syslog Audit**
 - Work with security monitoring functions to dynamically upload daily log information
 - Support self-defined and standard remote daily log output
 - Record to perform detailed auditing of connection, port dynamic opening, etc.
 - Report unauthorized data and messages and alarm to the authority

B Security Monitoring Function

- 1. Syslog Collection**
 - Collect specialized syslog data for network devices, servers, standard syslog data
 - Support buffering mechanism for large volume of syslog data
- 2. Syslog Categorization**
 - Support syslog data categorization for different equipment and different events with expedited statistics and fast positioning of targeted data
 - Provide syslog types, node port definition for easily managing network devices
- 3. Related Searching Function**
 - Provide searching capabilities with multiple conditions to rapidly locate the targeted syslogs needed
- 4. Node Management**
 - Automatically identify the syslog content to form the related node for efficiency
 - Can check live node status
 - Node can independently set up different grades of alarming

Henrich Electronics Corporation

7421 El Vallencito Drive

Walnut, CA 91789

United States

Cell Phone (708) -704 -9196

Phone (860) -487 -9869

Fax (860) -487 -9478

Email don@henrich-inc.com

www.henrich-inc.com

- 5. Security Audit and Report**
 - Equipped with multiple format and different style of reports to provide easy-to-read network status
 - Independent configurations for alarms, events into different date and time
 - Import and export of the syslog data
- 6. Real-Time Alarm**
 - The alarm parameters can be configured into node and event on the real time basis
- 7. Reporting**
 - Provide reporting functions with monthly statistics for the network status
 - Provide statistics for potential high risk events, equipment failures, etc.

C Operations Audit Function

- 1. Identity**
 - Support different levels of passwords, password validity, password locking, user re-initiation, etc.
 - Support management of different groups of users
- 2. Authorization Distribution and Control**
 - Provide authorization based on user to resources
 - Provide authorization based on user groups to resources
 - Provide authorization based on user to resources groups
 - Provide authorization based on user groups to resources groups
 - Provide authorization rules based on client address, visit time, visit time period
 - Provide authorization rules to limit the targeted IP addresses
- 3. Account and Command Management**
 - Provide integrated one-stop account and command management for Windows, Unix, network, and security devices
 - Provide automatic log-in functions using Telnet, SSH, RDP, VNC, etc.
 - Provide the collection, filtering and management functions for Unix system accounts
- 4 Resources Management**
 - Provide the establishment and maintenance for IT systems
 - Provide the detailed services for different IT systems
- 5. Operations**
 - Support Telnet/SSH to manage code-based operation systems
 - Support operations on image based operation systems through RDP/VNC
 - Support filtering for resource groups, IP, etc.
 - Support priorities for resource names, IPs, and resource groups
- 6. Alarm and Interruption**
 - Provide configuration and interruptions on sensitive operations
 - Support warning through emails
 - Send alarming to the client for interrupting or stopping the sensitive communications
- 7. Operation Audit**
 - Identify and mark with easy-to-ready colored marks for different level of sensitive events
 - Provide search on user, client address, resource, time and key words(except RDP protocols)
 - Provide replay function on image based conversation with pause, dragging capabilities; support time based position of replay functions
 - Support search on command exchange by sentences with key word searching capability
- 8. Record Output**
 - Provide video output for image auditing records using H.264 coding
 - Provide ttyrec based video output for the code protocol audit
 - Provide document-recording output for RDP operation data
 - Provide complete document output for code protocol content
 - Provide content output for SSH protocol SFTP channel documents
- 9. Remote Syslog**
 - Work together with security management functions to output live syslog data
 - Support self-defined and standard remote syslog output

D Network Security Functions

- 1. Network Device Discovery**
 - Support auto or semi-auto discovery of network devices with identification of network device types and vendor model number
 - Provide the connectivity relationship among the network devices using forwarding and routing table
- 2. Network Monitoring**
 - Support monitoring the live status of the network devices and the utilization of resources of those devices
- 3. Syslog Data**
 - Provide live alarming messages to the platform by working with the security management functions

Henrich Electronics Corporation

7421 El Vallencito Drive
Walnut, CA 91789
United States

Cell Phone (708) -704 -9196
Phone (860) -487 -9869
Fax (860) -487 -9478
Email don@henrich-inc.com

www.henrich-inc.com