VALIANT COMMUNICATIONS

Cyber Security Suite

The VCL **"Beyond the Firewall"** cyber-security solutions are designed to assist organizations to detect, prevent and secure their network against firewall breaches and cyber-attacks in real-time and to conduct forensic analysis and trace the attack route in real-time.

Most network administrators rely solely on a **"Firewall"** to secure their IP networks. Some network administrators go one step further and also deploy an additional **"Network Sniffer"** which monitors and flags the transmitted and received data anomalies. However, very few network administrator actually plans for an eventuality after a **"Firewall"** has been breached and the **"Network Sniffer"** has recorded anomalies in the data that is being transmitted and received.

VCL Cyber Security solution is very different from other security solutions which report a network security breach long after the event - when the damage has already been done.

The VCL **"Beyond the Firewall"** cyber-security solutions function behind the **"Firewall"** to provide the last-line-of-defence in the event of a network security breach to automatically initiate a series of defensive actions that would have been planned by the network administrator, in the event of a network security breach.

Such actions would include:

i) Generating "Audio-Visual Alarms",
ii) Sending "SNMP Traps",
iii) Sending "Network Security Alerts" to a centralized NMS,
iv) Initiate a "Fail-Over" to a standby "Firewall" / "Network", and
v) "Disconnect the Local Area Network from the Wide Area Network".

The VCL **"Beyond the Firewall"** cyber-security solutions provides a fully customizable roadmap to develop an advanced network defence strategy to detect network intrusions in real-time and to generate network alerts as well as audio and visual alarms, while a cyber-attack is in progress.

The VCL-2754: Cyber-Smart Rack Monitoring and Control Unit transforms any in any standard 19-Inch Rack into an intelligent entity that can **"securely"** communicate with the network administrator management system (NMS) in real-time to report all the physical parameters of the 19-Inch rack, as an when they change; or as and when an event or an alarm occurs. Various other **"Beyond the Firewall"** Cyber-Smart Rack Elements are used to protect the organization's IT network and to and fortify its security against hack-attacks and other un-lawful intrusions aimed at sabotaging or disrupting services; and stealing sensitive user data.

VCL cyber-security solutions may deployed by the network administrator to also automatically isolate the network; or to alternately provide an automatic switchover to a redundant network / redundant firewall whenever a hostile intrusion or firewall breach is detected in the user's primary network elements.

The VCL-UNMS, Unified Network Management System (UNMS) is completely scalable to securely monitor '000s of racks and its various **"Beyond the Firewall"** Cyber-Smart Rack Elements In real-time. Description of each of the **"Beyond the Firewall"** Cyber-Smart Rack are described below.

VCL "Beyond the Firewall" Cyber-Smart Rack Elements include:

VCL-2457: Cyber-Smart Rack Monitoring and Control Unit:

- Monitors DC voltage (range 15VDC to 60VDC).
- Monitors the Rack Temperature in 3 separate temperature zones in a rack and alerts network administrator the user defined temperature threshold is exceeded in any zone.
- Controls the operation of up to 3 rack-ventilation fans (or their multiples) by switching ON / switching OFF, as required. Extends fan MTBF life. Extends equipment MTBF life by alerting against over-heating due to failure of ventilation fans. Alerts if any of the rack fans fail; or if it is not operating at its specified RPM and requires service / replacement.
- Includes "6" binary inputs for monitoring up to 6 dry contact relay open loop / closed loop inputs. These inputs can be also connected to equipment alarm; rack-door open alarm; smoke alarm etc.
- Includes NTP/SNTP synchronization. Ensures that all alarms and events being reported / logged are accurately time-stamped.
- Centralized Network Management System (NMS) for monitoring the health of multiple racks in the network, from single central location.

VCL-2143: Network-MouseTrαpTM (Network Decoy Server):

- The Network-MouseTrαpTM alerts the network administrator of a network intrusion / cyber-attack in real-time. Alerts of a network intrusion or cyber-attack in real-time with an audio and visual alarm.
- This device can be programmed by the user to emulate (i.e. to appear to an attacker) as a Server, Router, Switch, SCADA Server, Relay, IEC-61850 Protection Relay, IEC 60870-5-104 Remote Terminal Unit (RTU), MODBUS RTU, Data Storage Device, ATMs and other devices used by financial organizations etc.
- Multiple Network-Mouse-Trαps™ may be installed by the network administrator at various vantage points in their network to attract the "hostile" elements / network infiltrators.
- Assists in identifying and isolating the source of problem / points of customer network vulnerability by providing intrusion or attack trace route and forensic analysis in real-time.

VCL-5001: Network Traffic Sniffer:

- This device detects network intrusions that could lead to Data Theft, Ransomware Attack, Denial of Service (DoS) or a Cyber-Attack aimed to bring-down the target network.
- Flags unusual traffic flows for both inbound and outbound traffic by providing an advance warning mechanism of the data traffic anomalies.

VCL-5000 : 1+1 Redundant Firewalls:

- 1+1 redundant configuration firewalls, with automatic fail-over switching. Industrial and ruggedized VCL-Firewall can be used in 1+1 redundant configuration to thwart and protect customers from cyber-attacks with a seamless option to switch to a back-up Firewall in case of breach of primary Firewall.

VCL-2778: SafeComm-E: 1+1 Ethernet Failover Protection / AB Fallback Switch:

- This device provides 1+1 Automatic Ethernet Failover / AB Fallback Protection between an "active" and "standby" terminal equipment; or between "main" and "standby" networks / firewalls and routers.
- Fail-Safe. The equipment never becomes a point of failure, even in a power down condition.
- Provides equipment (e.g. Server, Router, Switch) or network redundancy (i.e. Network uplink) for applications which require 99.99% up-time.

VCL-2702: Network Kill Switch:

- The Network Kill Switch becomes the last line of defence after the Firewall breach, to "repel" and "block" a cyber-attack - while it is progress.
- The Network Kill Switch is designed to connect to and monitor the various "Beyond the Firewall" security elements and send "alerts" of a network intrusion or cyber-attack to the network administrator in real-time.
- It also generates with audio and visual alarms to "alert" the maintenance staff and call for local administrative action.
- This device provides manual and automatic isolation from network, to initiate defensive counter-measures in an event of a cyber-attack.
- Can be used with VCL-5001 Network Traffic Sniffer; VCL-2143, Network-MouseTrαpTM (Decoy Network Servers) to isolate the network in the event of the detection of a network intrusion / breach of the cyber-security perimeter / hostile intrusion in the demilitarized security zone.
- The Network Kill Switch may be connected to though a wide variety of communication interfaces that include "Secured Ethernet", RS232, RS485 and Dry Contact Relay Inputs to monitor the various "Beyond the Firewall" security elements if any "hostile intrusions" are being reported.

VCL-UNMS: Cyber-Smart Rack Unified Network Management System:

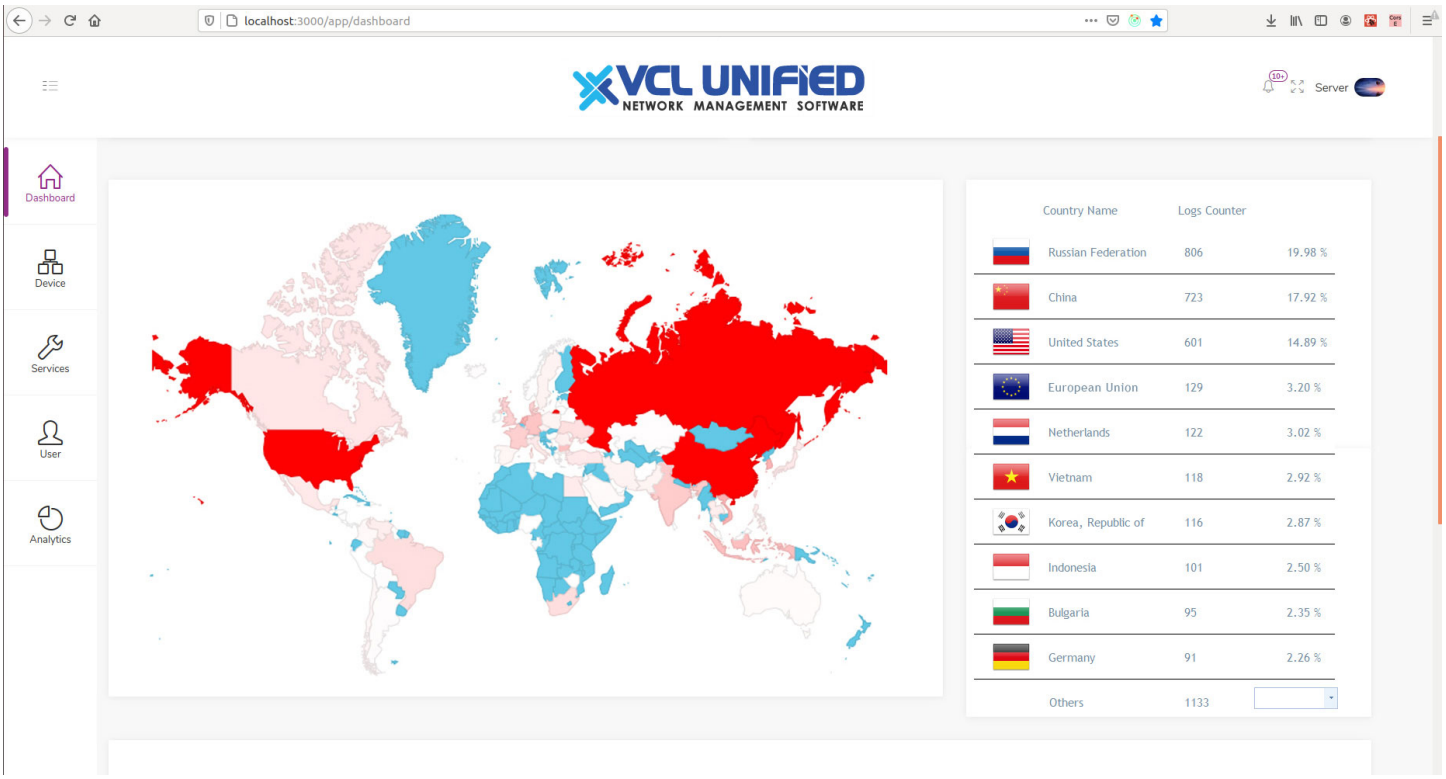
The VCL-UNMS: Cyber-Smart Rack Unified Network Management System is a comprehensive "Network Management Software" that can used by network administrators to communicate in real-time with all of the above "Beyond the Firewall" network security elements to enhance and fortify the organizations IT infrastructure through improved surveillance and real-time management and control.

VCL-UNMS Key Features:

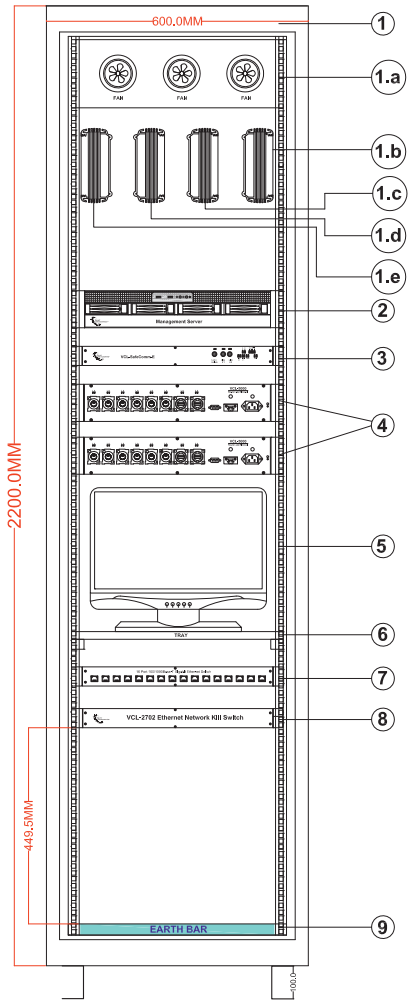
- LDAP/Active Directory user authentication
- MAC based device validation
- Simple and fast device on-boarding
- Device connectivity analytics
- Real-time alerts and notifications
- Network administrator defined role-based access control
- Secure sign-on with password strength monitoring
- Rich, visual appearance with high-definition graphics
- Graphs and charts for network overview and easy problem identification
- On-premise installation for secure deployment.
- Does not require any proprietary hardware. May be installed in any "Server Grade" computer.

VCL-UNMS Highlights include:

- Secure (supports TLS/SSL for encrypting connections between devices)
- Permission-based security
- Uses Software Defined Perimeter (SDP), the username/password login are replaced with Single-Packet Authorization (SPA) and the receiving device cannot be seen by hackers. This introduces an additional layer of security and is beneficial with or without SSL/TLS.
- Guaranteed message delivery (no data loss or duplication of data)
- Scalable (from few devices to thousands of connected devices)
- High-throughput and low-latency, low bandwidth usage for transmission
- Server/client 1+1 redundant architecture availability
- Supports architecture to make it possible to use in a 1-to-1; 1-to-Many; Many-to-1; or Many-to-Many communication / messaging network architecture.
- Ideal for monitoring IT Infrastructure, Sub-Stations, SCADA networks, Oil and Gas pipelines and Distributed Assets installed in remote locations through low-bandwidth radio / satellite links.
- Supports TCP/IP network.



Front View of Rack



Structured Network Reliability and Security Solution

For Applications where Cyber Security and Network reliability matters

IT No.	Description	Qty.
1.	Cyber Smart Rack 19" (2200 H x 600MM W x 600MM D)	1
1.a	3 FAN Unit	1
1.b	VCL-2457 Smart Rack Control Unit	1
1.c	VCL-3048 GPS - NTP Server	1
1.d	Network-MouseTrap #1	1
2.	VCL-5001 Network Traffic Sniffer and Management Server	1
3.	VCL-SafeComm - Ethernet Failover Switch	1
4.	VCL-5000 - Firewall (1+1 Redundant)	2
5.	Display Unit (With Keyboard, Keyboard Stand & Mouse)	1
6.	Base Tray	1
7.	16 Port 100/1000Base-T Gigabit Ethernet Switch	1
8.	VCL-2702 - Ethernet Network Kill Switch	1
9.	Grounding / Earth Bar	1

Technical specifications are subject to changes without notice.
Revision – 1.8, June 25, 2020

U.S.A.
Valcomm Technologies Inc.
4000 Ponce de Leon Blvd.,
Suite 470, Coral Gables,
FL 33146, U.S.A.
E-mail: us@valiantcom.com

U.K.
Valiant Communications (UK) Ltd
Central House Rear Office,
124 High Street, Hampton Hill,
Middlesex TW12 1NS, United Kingdom
E-mail: gb@valiantcom.com

INDIA
Valiant Communications Limited
71/1, Shivaji Marg,
New Delhi - 110015,
India
E-mail: mail@valiantcom.com