VCL Cyber Security Suite

Valiant's Cyber Security Suite - Unique Features:

- Automatically executes a counter-defense strategy if a network intrusion / cyber-attack is detected by isolating the critical infrastructure digital assets.
- Provides audio-visual alerts in the event of detection of a network intrusion / cyber-attack.
- Monitoring and visualization of all cyber-security equipment, alarms, and events in real-time.
- Assists in providing forensic analysis in near real-time.
- 1+1 redundancy with automatic failover of LAN equipment and WAN networks.
- No single point of failure in the network for enhanced resilience.

VCL-2702, Network Isolation Equipment: Provides manual and automatic isolation of the Local Area Network from Wide Area Network, in an event of a network security breach / cyber-attack or ransomware attack.

Features include:

- Network Isolation in a cyber-attack.
- Isolate NAS, Data Storage, Back-up servers.
- Create LAN / WAN isolation.
- Create operational isolation zones.
- Provides manual and automatic isolation of the Local Area Network from Wide Area Network, in an event of a network security breach / cyber-attack ransomware attack.
- Create Operational Zones or secure parameter zones with the external network isolate the network in the event of the detection of a network intrusion / breach in the cyber-security perimeter of the network's demilitarized zone.
- External triggers using dry-contact alarm relay.
- Failsafe. The unit itself should never becomes a point of failure, even in power down condition.

VCL-2778, Automatic Ethernet Failover Failsafe Equipment:

- 1+1 Automatic Ethernet Failover Failsafe Protection Switches that provide 1+1 Automatic Ethernet Failover / AB Fallback Protection between an "active" and "standby" equipment
- 1+1 Failover between "main" and "standby" networks are connected to the network through an IP/Ethernet interface
- Fail-Safe. The equipment never becomes a point of failure. It automatically reverts to the "primary network" / even in a power down condition
- Monitors end-to-end link connectivity
- Provides equipment or network redundancy for applications which require 99.99% up-time.

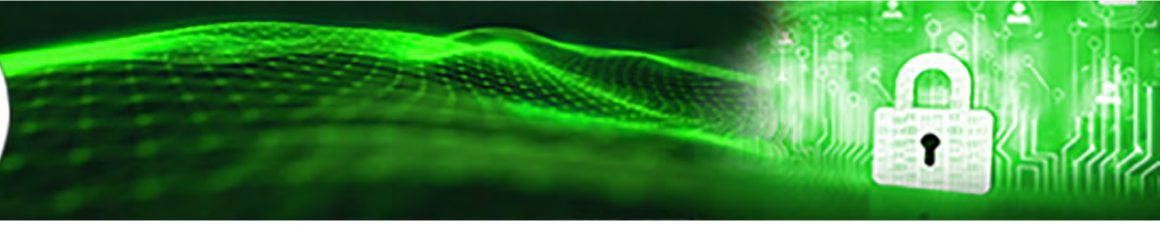
VCL-NAS & Data Storage: VCL Network Access Storage for IT/OT data storage and on-location / off-location critical data back-up.

- Ransomware resilient NAS and Data Storage Servers, up to 1.2 petabytes with Network Isolation Equipment
- Quantum-Safe Encryption
- Vaulted Data Storage through Data Diode
- EMP Protected Data Storage.

Web Site: www.valiantcom.com

Valiant Communications

VALCOMM



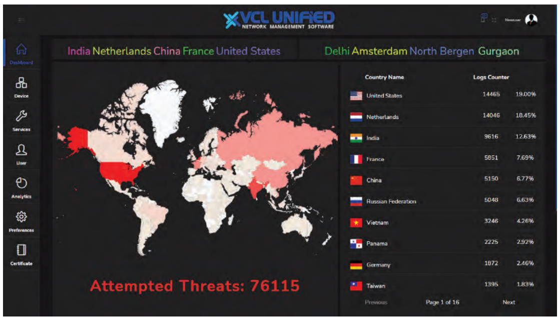
VCL Cyber Security Suite

VCL-2143: Network-MouseTrap™ an Advanced Honeypot:

This is an essential network security and forensics tool that enables users to detect firewall breaches and unauthorized network intrusions in their network, in real-time. It provides alerts in real time - including audio and visual alerts – on detection of a network security breach / ransomware attack.

Features include:

- Early warning systems with detection and alerting of cyber breaches and network intrusion
- Detect network intrusion and firewall breach.
- Detect moles and trojans within existing network
- Intrusion / Network breach detection alarms
- Integrated real-time audio and visual alarms
- Attacker trace root with forensics
- Maintain complete log with timestamp of intruder credentials such as IP address, domain and the originating location details
- Create automated daily, weekly or monthly intrusion detection reports
- Out-of-band access and security alerts
- White-list / black-list option
- Port based, IP Address based, and IP Domain based programmable filters
- Graphical User Interface (GUI).



India Netherlands China France United States

Delhi Amsterdam North Bergen Gurgaon

Country Name	Logs Counter	
United States	14465	19.00%
Netherlands	14046	18.45%
India	9616	12.63%
France	5851	7.69%
China	5150	6.77%
Russian Federation	5048	6.63%
Vietnam	3246	4.26%
Panama	2225	2.92%
Germany	1872	2.46%
Taiwan	1395	1.83%

Attempted Threats: 76115

VCL-3048, NTP Time Server: This is a compact NTP Server that is directly locked to a GPS / GNSS reference to provide time synchronization to private networks such Electric Sub-Stations, Power Distribution and Transmission companies, Oil and Gas Utilities, that are required to maintain a complete isolation from public networks for security reasons. Provides the following outputs - NTP, 1PPS, IRIG-B (Unmodulated BNC, RS-232, RS-485 / RS-422).

VCL-2243, RTU Firewall IEC - 104 and MODBUS TCP/IP: VCL-2243 is a high-security, high- reliability, ruggedized, failsafe transparent RTU Firewall that is designed to be installed between the RTU and the SCADA server without having to reconfigure any element of the network. VCL-2243 firewall supports IEC 60870-5-104 (IEC 104) and MODBUS TCP/IP protocol options with extremely advanced features that may be installed to secure and protect RTUs (Remote Terminal Units) in critical infrastructure.

VCL-MX-5050-R-ES, Router with Enhanced Security: VCL-MX-5050-R-ES is an integrated ruggedized router with enhanced security, encryption and advanced cyber security features that may be installed to secure critical infrastructure such as utilities, sub-stations, SCADA networks, smart-grid distribution systems, airports, railways, IT Networks of financial institutions such as banks and corporate networks. This product is supports for Ethernet, Fast Ethernet, Gigabit Ethernet, Optical Ports with redundant power supply options.

VCL-MX-5050-R-ES provides Inclusion Policy access control based upon Whitelist IP addresses, MAC address and IP Domain and Exclusion Policy access control based on Black-List continuous monitoring of the TLS connection to nullify MitM attacks. Features and capabilities include IPv4, IPv6, Layer 2, Layer 3 routing, Routing Protocols including RIPv1, RIPv2, OSPFv2 and OSPFv3, BGPv4, SNMPv2, SNMPv3, ACL Layer 2, Layer 3 Security, QoS, remote access via RADIUS and SSH with encrypted password protection.

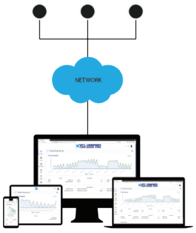
VCL Cyber Security Suite

VCL-2457, Smart Rack Control Unit: Compact size, DIN rail mount unit provides monitoring of the health of the telecom racks, alarms including Fan Control Unit for fan management and fan failure alarms for maintaining ambient temperature, 6 additional binary inputs for sensing dry contact relays (open loop / closed loop status) I/Os to monitor, smoke alarm, high temperature alarm, water-logging alarm, Equipment failure alarm etc. May be fully integrated with VCL-UNMS, Centralized Network Management System (NMS) for monitoring the health of multiple racks in the network, from single central location.

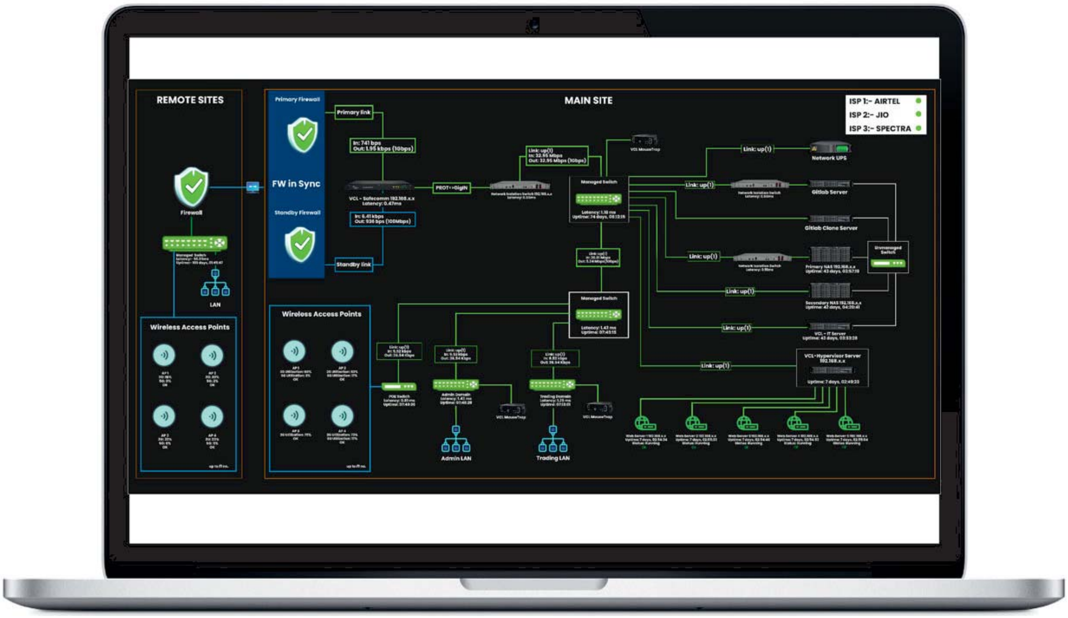
VCL-2142, Enigmatron Xcöde: IEC 60870-5-104 and DNP Protocol Encryptor: This is low data rate encryption equipment with extremely advanced features to secure and protect RTU data in critical infrastructure, Smart Grid Distribution Systems, Oil and Gas Infrastructure and Railway Signalling Networks. Provide secure communications between multiple RTU Terminals and their corresponding IEC 60870-5-104, MODBUS-TCP and DNP central server (s).

UNMS (Universal NMS): All these above listed elements can be monitored from Our (UNMS) Universal NMS. NMS and network visualization options include:

- UI - User Configuration and Management Utility
- UNMS - Network Monitoring Software for monitoring all elements of a structured NAS
- NVMS - Secure wide network monitoring software for monitoring multiple NAS deployments across the network



Install once
access anywhere



Revision 1.8, January 03, 2025

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, U.K.
E-mail: gb@valiantcom.com

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