Valiant Communications Limited
(An ISO 9001:2015 and ISO 14001:2015 Certified Company)
Regd. Office : 71/1, Shivaji Marg, New Delhi 110015, India
Corporate Identity No. : L74899 DL1993 PLC056652 | GSTIN : 07 AAACV4250G 1ZJ
T : +91-11-2592 8415, 2592 8416, 2541 0053 | F : + 91-11-2543 4300, 4105 5604
E : admin@valiantcom.com | W : www.valiantcom.com

VALIANT COMMUNICATIONS

Ref: VCL/IND/SEC/BSE/369

Date: 21-07-2020

The Secretary,
BSE Limited
Phiroze Jeejeebhoy Tower,
25th Floor, Dalal Street,
Mumbai – 400 023

Ref: Press release on "Comprehensive Cyber Security solution from Valiant Communications Ltd."

Dear Sir/ Madam,

With above reference, please find enclosed herewith the press release in compliance with SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.

We hope you find the same in order.

Sincerely,
For Valiant Communications Limited

Valiant Communications Ltd.
71/1
Shivaji Marg
New Delhi
110 015
India

Manish Kumar
Company Secretary

PRESS RELEASE For immediate use

VALIANT COMMUNICATIONS

Comprehensive Cyber Security solution from Valiant Communications Ltd.

Valiant Communications (VCL) provides a comprehensive Cyber Security solution designed to assist organizations to *detect, prevent and secure* their network against firewall breaches and cyber-attacks. Valiant's Cyber Security Solution functions in real-time to alert the user against a network security breach and to take appropriate corrective measures, according to user's custom defined network security policy.

All the products featured below are completely designed and manufactured in India by Valiant Communications Limited. Valiant is a domestic Indian manufacturer. These product are being offered to VCL customer for Indian and international market.

VCL ***"Beyond the Firewall"*** Cyber Security solution detects firewall breaches, network intrusions and cyber-attacks in "real-time". It provides the user, the data, to conduct forensic analysis and trace the attack route which assists the user to identify the points of network vulnerability.

The VCL customer is able to identify the attacking entity, the IP address and the country from where the attack is originating in real-time and to take appropriate defensive measures against such attacks, as and when they occur. VCL Cyber Security solution is very different from other security solutions that report a network security breach long after the event - when the damage has already been done.

VCL's cyber-security solution can be used by the network administrator to build an elaborate, 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. VCL's 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.

VCL provides a comprehensive and advanced range of "Cyber Security" solutions that consist of a "Cyber Smart-Rack" and "Beyond the Firewall" network security devices that include "Network Traffic Sniffers", "Network Decoy Servers" and "Network Kill-Switches" that assist its users to implement and deploy advanced comprehensive defence measures against cyber-attacks.

VCL-CSR: Cyber-Smart Rack

- Provides alarms and multiple alert options including rack open door alarm (up to 6 binary I/Os), smoke alarm, high temperature alarm, water-logging alarm, fan management and fan failure alarms and NTP/SNTP synchronization.
- Centralized Network Management System (NMS) for monitoring the health of multiple racks in the network, from single central location.

VCL-5001: Network Traffic Sniffers:

- 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-2143: Network Decoy Servers

- This device alerts 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.
- 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-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:

- This device provides manual and automatic isolation from network, in an event of a cyber-attack.
- Can be used with VCL-5001 Network Traffic Sniffer; and / or with VCL-2143, Network Decoy Servers / Network Decoy Elements 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.

VCL-2143: User Interface:

Provides a Unified Management System for monitoring of all Network Devices that are installed and central monitoring from a single location to detects firewall breaches, network intrusions and cyber-attacks in “real-time”. This platform provides the user, the data, to conduct forensic analysis and trace the attack route which assists the user to identify the points of network vulnerability.

The VCL “Beyond the Firewall” Cyber Security Solution does not negate or invalidate the role of the “Firewall” in any manner. The Firewall still remains the primary element of defense against cyber-attacks. However, cyber-attacks succeed because firewalls get breached. The deployment of the VCL “Beyond the Firewall” Cyber Security Solution provides next line of defense against firewall breaches, resulting in the enhanced network security and resilience against cyber-attacks in real-time.

About Valiant Communications: Valiant is a manufacturer and exporter of a wide range of communication, transmission, synchronization and cyber security solutions. It is an approved manufacturer by various utilities including defense, airport and power.

New Delhi, July 21st 2020