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 : +91-11-4105 5601, 4105 5602, 4105 5603, 2592 8415, 2592 8416, 2541 0053
F : +91-11-2543 4300, 4105 5604
E : admin@valiantcom.com | W : www.valiantcom.com

VALIANT COMMUNICATIONS

Date: 27-07-2026

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

Ref: Press Release titled "Zero-Day Attacks Mitigation — A Solution from Valiant Communications."

Dear Sir / Madam,

With the 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

MANISH KUMAR

Digitally signed by MANISH KUMAR
DN: c=IN, st=Delhi, 2.5.4.20=f8edcf657137457d93b17a1edcd18195cefb71ed2525fd086a42a5ecf81910f4, postalCode=110015, street=71/1 Shivaji Marg Delhi, pseudonym=e46a97fd-b81e-4050-8832-00c8d89f8dfc, serialNumber=78667909cac1632b9441ec49656322a483976e102d509a6bc7998b933e4e0f38, ou=COMPANY, o=VALIANT COMMUNICATIONS LIMITED, cn=MANISH KUMAR
Date: 2026.07.27 11:20:37 +05'30'

Manish Kumar
Company Secretary

PRESS RELEASE For immediate use

27 July 2026

Zero-Day Attacks Mitigation — A Solution from Valiant Communications

The Threat Is Real, Escalating, and Outpacing Conventional Defences

More than 23,600 vulnerabilities were published in the first half of 2025 alone — a 16% increase over 2024. Sophisticated threat actors, including nation-state groups and ransomware operators, are weaponising unknown vulnerabilities faster than ever before. Nearly 30% of Known Exploited Vulnerabilities were weaponised within 24 hours of public disclosure — some before patches were even available.

Zero-day exploitation has shifted from occasional high-profile incidents to a persistent element of the threat landscape. Nearly 90 zero-day vulnerabilities were observed in active exploitation during 2025, continuing the elevated trend first seen after 2021. Ransomware incidents spiked by 36%, with attackers increasingly targeting edge devices and unconventional endpoints. Nearly 50% of attackers in recent campaigns were linked to state-sponsored or hacktivist groups, and state-backed campaigns focusing specifically on industrial and operational technology (OT) environments.

The financial consequences are severe. The average cost of a data breach for US companies reached an all-time high of $10.22 million in 2025. Globally, the average stands at $4.44 million — and nearly two-thirds of breached organisations are still recovering from the incident long after it has been contained.

This is precisely the threat environment where hardware-based isolation outperforms software-based security — and where VCL's Network Isolation Kill Switch and VCL-Network MouseTrap deliver demonstrable, measurable protection.

A Zero-Day Attack Exploits the Fundamental Weakness of Signature-Based Security

A zero-day attack exploits an unknown vulnerability — one for which no patch, signature, or antivirus definition yet exists. Every conventional software-based defence — firewalls, intrusion prevention systems, endpoint protection — relies on knowing what to look for. Against a zero-day, they are blind.

In 2025, 48% of tracked zero-days targeted enterprise-grade technology, marking a new high. The increased exploitation of security and networking devices highlights the critical risk posed by trusted edge infrastructure. In 2024, 20 of 33 enterprise zero-days targeted security and

networking devices — over 60% of enterprise zero-day exploitation. Enterprise software exhibits a consistent structural weakness: networking devices highlight the value attackers place on trusted edge infrastructure that lacks endpoint detection.

Critically, the average time to identify and contain a breach stood at 258 days for identification and 64 days for containment. Every day a zero-day remains undetected, the attacker deepens their access, maps your network, and positions for maximum impact.

VCL's Network Isolation Kill Switch and VCL-Network MousTrap take a fundamentally different approach: **they don't need to recognise the attack. They detect its behaviour.**

How the VCL-Network MousTrap Catches Zero-Days

The VCL-Network MouseTrap is an advanced honeypot — a decoy server that impersonates legitimate critical assets: servers, protection relays, RTUs, payment gateways, SCADA nodes.

When a zero-day exploit propagates through a network, it probes and maps whatever it finds. The moment it probes the VCL-Network MouseTrap, it has revealed itself — without the defender needing to know anything about the exploit's signature or method.

The VCL-Network MouseTrap instantly generates audio-visual alarms, SNMP traps, out-of-band security alerts, and Network Management System alarms. Crucially, its RS-232/RS-485 output is directly wired to VCL's Network Isolation Kill Switch — triggering an automated isolation the moment intrusion is confirmed, with zero human delay.

A zero-day cannot hide its lateral movement from a decoy it doesn't know exists.

How the VCL Network Isolation Kill Switch (VCL-2702/5052/5054) contains Zero-Days

Once the VCL-Network MouseTrap fires, the VCL Network Isolation Kill Switch acts at the hardware level — physically severing the LAN from the WAN, or isolating specific servers and data storage assets, in milliseconds.

This is not a software command that a sophisticated zero-day could intercept or disable. It is a physical disconnection, enforced by hardware, independent of the operating system, management plane, or any software layer the attacker may have already compromised.

This distinction is decisive. Nation-state actors have been documented deploying custom tools to manipulate built-in integrity checker mechanisms and evade detection — precisely the kind of attack that renders software-defined responses unreliable. A hardware-enforced physical cut cannot be subverted by malware already present in the network.

Critically, the VCL Network Isolation Kill Switch is fail-safe: if it loses power or suffers a control card failure, any port already placed in isolation mode remains isolated. **The attacker cannot recover connectivity by disrupting the device itself.**

Why OT and Critical Infrastructure Face Disproportionate Risk

Power utilities, water treatment plants, substations, defence installations, banking infrastructure, and data centres operate on networks where a zero-day breach is not merely a data security incident — it is a threat to physical safety, national security, and economic continuity.

Malicious State-backed campaigns have focused specifically on industrial and OT environments, and nearly half of attacker groups involved in 2025 campaigns were state-sponsored or hacktivist in nature. These are not opportunistic criminals; they are adversaries with the patience, capability, and intent to cause lasting operational damage.

OT environments compound the problem: many protection relays, RTUs, and SCADA systems cannot run endpoint agents, cannot be patched rapidly, and cannot tolerate the latency introduced by software-based security inspection. The only viable defence is one that operates independently of the endpoint — exactly what VCL's hardware architecture delivers.

The Combined Architecture — Why It Matters

Threat Stage	VCL-MouseTrap Response	VCL Kill Switch Response
Zero-day probes network	Decoy lures and logs attacker	Standing by
Intrusion confirmed	Fires alarm + triggers Kill Switch via serial	Physically isolates LAN/WAN and critical digital assets
Attacker attempts lateral spread	Non-volatile forensic log captures IP fingerprint	Network segments remain physically severed
Incident response	Full access log for digital forensics	Isolated mode maintained until manual release

Compliance and Regulatory Alignment

Regulators have responded to the escalating threat by mandating rapid detection and network segmentation capabilities in critical sectors. VCL's architecture directly supports compliance with:

- **International:** IEC 62443 (Industrial Automation and Control Systems security) and IEC 61850 (substation communication security), both of which call for network segmentation and anomaly detection in OT environments.
- **India:** NCIIPC guidelines, CERT-In Directions (April 2022), CEA Cyber Security Regulations (2024, enforceable from April 2027), and NCRF 2024 — all of which mandate OT network segregation, event logging, and incident response capability.
- **UK:** NCSC CAF 4.0 and the Cyber Security and Resilience Bill 2025, which requires critical infrastructure operators to demonstrate active intrusion detection and isolation capability.

VCL's hardware-based approach satisfies these mandates through physical means — immune to the software-level tampering that defeats purely digital compliance tools.

The Base Line

Traditional security asks: *"Do I recognise this threat?"*
VCL's architecture asks: *"Has anything probed what it shouldn't?"* — and then acts physically, not digitally.

In 2025, nearly 30% of exploited vulnerabilities were weaponised on the same day their CVE was published — or before. Time-to-exploitation patterns remain consistent and sustained. In this environment, the window between a zero-day's first probe and its payload delivery can be hours, not days. Automated, hardware-enforced isolation is no longer a premium option — it is a baseline requirement.

This is why the VCL Network Isolation Kill Switch and VCL-Network MouseTrap together provide meaningful, demonstrable zero-day mitigation where software-only solutions cannot.

About Valiant Communications: Valiant Communications (VCL) designs and manufactures advanced IT/OT communication, synchronization, protection, transmission, network-attached storage (NAS), Storage Area Network (SAN) data storage, and cybersecurity equipment and solutions tailored for critical infrastructure and utility / SCADA applications. With successful installations in 110+ countries, VCL technologies serve power utilities, railways, oil & gas, airports, defence, SCADA systems and mission-critical operations and infrastructure across the globe.