Neehar Pathare
MD, CEO & CIO
63SATS Cybertech

63SATS positions itself as "Your Own Cyber Security Force." How does this philosophy translate into real-world protection?

At 63SATS, the philosophy of being "Your Own Cyber Security Force" is built on a simple truth: modern organisations do not just need consultants—they need a force that protects them continuously, across every layer of their digital landscape. Unlike traditional firms that only deliver assessments, 63SATS brings together offensive security, defensive engineering, digital risk monitoring, and advanced security solutions into one integrated capability, allowing us to operate as an extension of our clients' internal teams.

Our work begins with deep, adversary-focused assessments. When we conduct Red Team operations, External Threat Assessments, Application and Mobile Security testing, WIFI reviews, Cloud Security Audits, and governance assessments, we analyse not just individual vulnerabilities but how real-world attackers would chain those weaknesses across identity, endpoint, application, and cloud layers. This gives enterprises, governments, and regulated entities a realistic understanding of their exposure—not just a list of issues.

How is 63SATS enhancing its ability to predict, prevent, and neutralize advanced cyber threats?

We have built an intelligence-first defence model that blends offensive expertise, deep visibility, and engineered resilience.

Our Red Team engagements simulate real adversary campaigns mapped to MITRE ATT&CK, enabling us to uncover attack paths across applications, WiFi networks, cloud workloads, OT environments, and identity systems. This approach moves beyond surface-level VAPT; it mirrors how ransomware groups, infostealer operators, and state-sponsored actors actually infiltrate hybrid infrastructures.

We complement this with our External Threat Assessment and Digital Risk Monitoring programs, where we continuously track leaked credentials, exposed assets, domain impersonation attempts, and dark-web chatter relevant to our clients. By analysing data from cybercrime forums, stealer logs, malware repositories, and global attack telemetry, our teams can forecast potential intrusion vectors with high accuracy.

The result is a holistic security posture where threats are not just detected—they are anticipated and neutralized before they disrupt business operations. Our goal is clear: to ensure every organisation we serve moves from reactive firefighting to strategic cyber readiness.

What strategies is 63SATS using to secure endpoints, mobile devices, and sensitive data flows while ensuring operational continuity?

63SATS addresses this with a layered prevention-first strategy.

Our Anti-Ransomware Assurance combines endpoint protection, behavioral analytics, and threat hunting to identify early stages of ransomware execution—before encryption impacts operations. For mobile-first enterprises, our Mobile Threat Defense and Mobile Application Protection secure devices, apps, permissions, and network behaviour against malware, spyware, and phishing vectors.

To protect high-value or classified data, we deploy Galvanic Separation (Data Diode) systems, ensuring one-way data flow and eliminating the possibility of external tampering or data leakage. Coupled with Encrypted Communication platforms and Secure Instant Messaging, we help organisations protect sensitive conversations, archival data, and mission-critical workloads.

This multi-layered protection ensures that whether data resides on servers, endpoints, mobile devices, or isolated networks, it remains secure, compliant, and tamper-proof. ■