



Srinivas L

Joint MD & Joint CEO
63SATS Cybertech



How is AI changing cyber threats, and how is 63SATS Cybertech adapting its security solutions to address them?

The attacker is no longer human. AI now writes phishing emails in flawless Hindi and Tamil, clones a CFO's voice in minutes, and probes thousands of networks at once. A compromise that once took weeks unfolds in hours. Attacks have become cheaper, faster and personal. Our answer is to fight machine speed with machine speed. We have rebuilt our security operations around AI that detects, investigates and contains threats on its own, with analysts supervising rather than typing. We have set up a dedicated AI defence research unit to study how attackers use these models before those tactics reach Indian businesses. And as companies deploy AI agents of their own, we are building the controls to secure them. You cannot defend against an AI-driven attack with a human-only response.

Which cybersecurity needs and market opportunities will shape 63SATS Cybertech's growth over the next five years?

Three forces will shape the next five years. First, regulation. The Digital Personal Data Protection law, along with guidance from CERT-In, RBI

and SEBI, is turning cybersecurity from a discretionary spend into a board obligation. We see that as a welcome catalyst, not a burden. Second, the mid-market. India's growth companies are digitising faster than they can secure themselves, and they need outcomes, not tools. Managed defence for this segment is our largest opportunity. Third, sovereignty. Government and critical infrastructure increasingly want defence built and controlled in India, and we are positioned squarely there. Underneath all three sits our shift from services to our own intellectual property. India should not just consume cybersecurity. It should build it and export it. ■

How does 63SATS Cybertech turn emerging cyber threats into security solutions for businesses of different sizes?

Cyber threats do not respect company size. A forty-person exporter and a national bank face the same attackers, often the same malware. What differs is the budget and the people available to fight back. So we built one defence system and made it fit three markets. For large enterprises, we run security operations round the clock, with our own people watching, hunting and responding. For government and critical infrastructure, we build sovereign-grade defence that stays under Indian control. For consumers and small businesses, we compressed that same capability into something simple enough for anyone to use. Every threat we see on a bank's network teaches the system that protects a kirana store. We do not write reports. We build and run the defence.