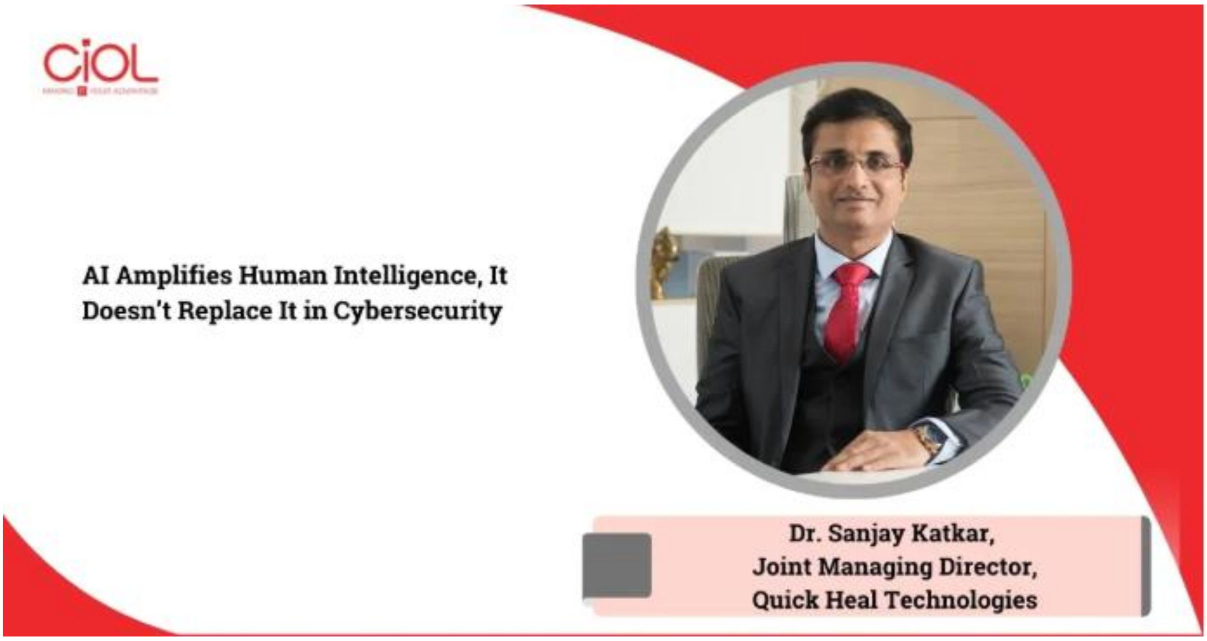
Inside Quick Heal’s Journey: Building India’s First Antivirus to a Global Brand

With a vision rooted in resilience and innovation, Quick Heal has transformed from a local antivirus startup into a global cybersecurity brand trusted by millions.


CiOL
AI Amplifies Human Intelligence, It Doesn’t Replace It in Cybersecurity
Dr. Sanjay Katkar,
Joint Managing Director,
Quick Heal Technologies

Every great company has a defining origin story. Quick Heal’s journey began in Pune, when brothers Kailash and Sanjay Katkar started developing antivirus solutions to tackle the rising wave of computer viruses. What began as an experiment grew into India’s first homegrown antivirus and, eventually, a listed company with global recognition. Sanjay Katkar, Joint Managing Director, Quick Heal, has lived every stage of that journey - innovator, entrepreneur, industry evangelist, and thought leader.

Today, Quick Heal operates on a global stage, competing with international security giants while addressing India’s unique threat landscape.In this conversation with CIOL, Sanjay opens up about the struggles of building a tech business in India, why CXOs must rethink their approach to cyber risk, and how the next generation can turn challenges into opportunities. His entrepreneurship journey with Quick Heal reflects how vision and perseverance can turn a homegrown idea into a global cybersecurity success. Excerpts.

India's digital economy is expanding rapidly, but so are cyber threats. What do you see as the most critical gaps in India's cybersecurity preparedness today, and how can the industry address them at scale?

While India aims to become a $5 trillion economy by 2027, only 7% of our organizations have reached a state of maturity from their cybersecurity readiness perspective. This massive preparedness gap stems from three key challenges we've seen enterprises grappling with since Quick Heal Technologies Limited's early days.

First, the skills deficit remains our Achilles' heel. India needs over 8 lakh cybersecurity professionals, yet our educational system produces graduates with theoretical knowledge that's no match for practical, real-life threats.

Second, we're seeing fragmented security implementations across organizations. Many companies deploy point solutions without understanding the interconnected nature of modern threats. This creates blind spots that sophisticated attackers exploit. The recent surge in supply chain attacks and AI-powered malware demands integrated security approaches, not piecemeal defenses.

Third, there's a dangerous disconnect between boardroom priorities and ground-level security reality. Only 21% of executives allocate cyber budgets to their organization's top risks. This misalignment leaves critical vulnerabilities unaddressed while resources get scattered across less impactful initiatives.

The solution requires coordinated action across multiple fronts. Educational institutions must integrate real-world threat scenarios into curricula—something that our Quick Heal Foundation and Quick Heal Academy actively promote through various programs. The industry needs to embrace apprenticeship models that combine theoretical knowledge with practical experience that reflect the ground reality in terms of what actually works in the cyber world. Most importantly, we need regulatory frameworks that incentivize proactive security rather than reactive compliance.

As an early innovator in indigenous cybersecurity solutions, how do you see the "Make in India" movement shaping the future of cyber defence, not just for India, but as a global export?

The "Make in India" momentum is creating something we've never seen before: indigenous solutions designed for India's unique threat landscape that turn out to be globally relevant. Our experience with threats has taught us that Indian-developed solutions often handle edge cases and resource constraints better than foreign alternatives built for different environments.
What excites me most is seeing the ecosystem mature. When we started, venture capital for security was virtually non-existent. Today, startups can command valuations worth hundreds of crores of dollars from global players. This shows that Indian cybersecurity innovation has reached global standards.

I see India placed in a good position to not only cater to the cybersecurity market at home, but equally relevant to overseas countries as well. Our potent technologies and solutions identify and protect against the various shapes and forms of evolving malware, and the same technologies and solutions are very much applicable to the global audience.

With AI and automation driving the next wave of security products, how does Quick Heal balance machine intelligence with human expertise, especially as threats become more sophisticated and targeted?

This balance is perhaps the most critical challenge we face today. AI isn't replacing human expertise. Rather, it's amplifying it—but only when implemented thoughtfully. Our approach at Quick Heal Technologies reflects lessons learned from 30 years of threat evolution.

Machine intelligence excels at pattern recognition and processing vast datasets. Our AI engines at Seqrite Labs, India’s largest malware analysis facility, analyzed 369 million malware detections across 8.4 million endpoints in 2024, identifying threat patterns no human analyst could spot manually. We have thoroughly integrated AI across threat detection, behavioral analysis, and automated response systems, particularly in our Seqrite enterprise offerings.

But human expertise remains irreplaceable for contextual decision-making and understanding attacker psychology. When we see new attack vectors, human analysts provide the strategic thinking that machines cannot replicate. They understand business context, assess risk tolerance, and make judgment calls about acceptable security trade-offs.

The key insight is treating AI as a force multiplier, not a replacement. Our security solutions and threat research teams use AI tools to accelerate malware analysis and vulnerability research, but human creativity drives the strategic thinking behind new defensive approaches. This balance becomes even more critical as attackers themselves leverage AI to craft more convincing phishing campaigns and adaptive malware.

The world is seeing a surge in enterprise ransomware, supply chain attacks, and sophisticated phishing. Which emerging threat vectors worry you most for Indian businesses in 2025 and beyond, and how should they respond?

There are three, and they're all interconnected in ways that traditional security approaches struggle to address.

First, AI-powered social engineering represents a paradigm shift. We're seeing deepfake voice calls targeting CFOs, AI-generated spear-phishing campaigns that reference real business contexts, and sophisticated business email compromise attacks that adapt in real time based on victim responses. India's rapid digital adoption means many organizations lack the security awareness to recognize these advanced deception techniques.

Second, supply chain attacks targeting India's growing technology ecosystem pose systemic risks. The XZ-Utils compromise showed how attackers can embed malicious code in trusted open-source components used across thousands of applications. Given India's role in global software development and the interconnected nature of our technology supply chains, a successful attack could cascade across multiple sectors simultaneously.

Third, cloud misconfigurations combined with insider threats create unprecedented attack surfaces. As Indian businesses accelerate cloud adoption, they stand at risk of exposing sensitive data through improperly configured services while struggling to monitor privileged user activities across hybrid infrastructures.

The response requires a major shift in security thinking. Organizations need to implement Zero Trust architectures that verify every transaction rather than trusting network perimeters. They must invest in continuous security awareness training that addresses AI-powered deception techniques. Most importantly, they need integrated threat intelligence that can correlate indicators across their entire technology stack. At Seqrite, we're actively addressing these challenges through our advanced solutions such as Seqrite XDR, Seqrite Threat Intel, and Seqrite Intelligent Assistant.

You've led Quick Heal from a startup to a listed, global company. What leadership lessons or personal philosophies have guided you through technology disruption and scaling the business?

The most important lesson I've learned is that technology changes, but fundamental principles remain constant. When Kailash and I started Quick Heal Technologies in 1995, we focused on solving real problems for real people. That obsession with customer value has guided every major decision since.

During our early years, when multinational competitors had massive marketing budgets and established channel partnerships, we survived by being genuinely better at understanding Indian user needs. Global antivirus solutions often couldn't handle the pirated software, outdated operating systems, and resource-constrained hardware that characterized the Indian market. By designing for these constraints, we created solutions that worked better for our customers than expensive international alternatives.

As the cybersecurity talent gap grows, what advice would you give to young Indian engineers and entrepreneurs who want to build a career or startup in this critical sector?

The cybersecurity talent shortage, in my opinion, is the greatest opportunity that has occurred in three decades. India urgently needs more cybersecurity professionals, and traditional educational approaches are failing to bridge the massive demand-and-supply gap. This creates unprecedented openings for young talent willing to take unconventional paths.

My advice is: embrace practical learning over theoretical knowledge. When I was developing antivirus solutions in my college days, I learned more from analyzing actual malware samples than from any textbook. Today's threats are exponentially more sophisticated, but the principle remains the same—hands-on experience with real security challenges teaches you things no classroom can replicate.

For aspiring entrepreneurs, I recommend focusing on solving specific problems rather than building generic security products. The most successful cybersecurity ventures identify underserved market segments or novel attack vectors and develop targeted solutions.

Finally, today's CXOs—especially CISOs and CIOs—often find themselves caught between the devil and the deep blue sea when it comes to taming cyber threats. What are three actionable strategies you would recommend for building a truly proactive digital defence ecosystem?

The pressure on CISOs and CIOs has intensified by leaps and bounds. They're expected to enable digital transformation while preventing sophisticated attacks, often with limited budgets and unrealistic expectations from boards who don't understand cybersecurity complexities. Based on our experience working with thousands of enterprises, three strategies can transform this impossible position into a manageable risk.

First, implement risk-based security investments aligned with business priorities. Most organizations scatter cybersecurity budgets across multiple point solutions without understanding which assets matter most to business operations. CISOs need to conduct comprehensive business impact assessments that identify critical systems, data flows, and processes, then allocate security investments proportionally.

Second, embrace automation for routine security operations while reserving human expertise for strategic decision-making. The talent shortage means security teams cannot manually handle the volume of alerts modern environments generate. AI-powered SIEM platforms, automated threat response systems, and behavioral analytics can handle tier-one security operations, freeing skilled professionals for threat hunting, incident response strategy, and security architecture decisions.

Third, establish integrated threat intelligence that provides unified visibility across the entire technology stack. Modern attacks span endpoints, networks, cloud environments, and supply chains. Security teams using disconnected tools cannot correlate indicators or understand attack progression. Platforms like our Seqrite XDR solution provide the holistic view necessary for detecting advanced persistent threats and coordinated attacks that traditional perimeter-focused approaches miss completely.

Cybersecurity needs to be treated as a business enabler rather than a cost center. When security teams can showcase measurable business value through risk reduction, operational efficiency, and competitive advantage, they gain the executive support necessary for building truly proactive defense ecosystems.