



# Made in India

## POWERING NATIONAL SECURITY

Circulated with The Economic Times, Delhi NCR, Mumbai, Bengaluru, Ahmedabad, Kolkata, Chennai, Pune, Hyderabad & Nagpur

Wednesday, 13 August, 2025

An Advertorial Promotional Feature  
An Optimal Media Solutions Initiative, A division of Times Internet Limited

## National Security in the Intelligence Age: Sify's Blueprint

As part of our Independence Day special on powering India's national security, we speak with Sharad Agarwal, CEO of Sify Infinit Spaces, a wholly owned subsidiary of Sify Technologies. He shares insights on Sify 4.0, AI-ready infrastructure, and building intelligent, sovereign digital systems for a secure, resilient future. Excerpts.

**Sify has evolved from an early private ISP in India into an enterprise ICT powerhouse. How do you define "Sify 4.0" in an age where robust digital infrastructure is critical to national security?**

Sify's journey from 1.0 to 4.0 mirrors the evolution of the digital world itself—from the simple act of connecting people to enabling an intelligence-driven future that underpins national security.

We began on 12 December 1995 as India's first private ISP. In those early days, Sify 1.0 was about one thing—connectivity. The mission was clear: connect people. The idea of doing something transformative with that connection wasn't yet in the conversation.

Sify 2.0 marked the era of data consumption and sharing. Connectivity now enabled businesses and individuals to move information from one point to another. But data volumes were still modest; the focus was largely on computerisation, not on unlocking data's deeper potential.

Then came Sify 3.0, when we entered the data processing and analytics phase. This was when raw data began to be transformed into knowledge. By analysing patterns and processing information, we could make better decisions—technology started serving strategy.

Today, with Sify 4.0, we have stepped decisively into the intelligence age. This is the era where data doesn't just inform decisions—it predicts them. We can model outcomes, anticipate threats, and respond proactively. This predictive capability is at the heart of modern national security, where speed, accuracy, and foresight are critical.

Our role has evolved from providing basic internet connections to building and managing integrated digital infrastructure—spanning data centres, connectivity, cloud, cybersecurity, and now AI-driven intelligence systems. In the early days, "digital infrastructure" wasn't even a term; today, it is the backbone of secure economies and resilient nations.

For India, this transformation matters deeply. A robust, intelligent digital infrastructure safeguards critical sectors—finance, defence, healthcare, governance—from emerging threats. As the digital frontier becomes the

new battleground, Sify 4.0 is not just about business growth—it's about national resilience.

Our vision now is to ensure that India's digital infrastructure is not only built for scale but also for security, agility, and intelligence. We've moved from the information age to the intelligence age—a journey that began with connecting people and now empowers the nation to protect its future.

**With GenAI, LLMs, and real-time analytics driving an unprecedented rise in data and compute needs, how are you ensuring that your data centers are not just AI-ready, but also AI-secure?**

At Sify, we ensure our data centers are both AI-ready and physically secure—whether hosting enterprise infrastructure or hyperscalers. Physical safeguards are paramount, while AI and cybersecurity measures



**Sharad Agarwal**  
CEO of Sify Infinit Spaces

evolve in step with emerging threats. Security is a continual catch-up game, and we work with multiple partners to strengthen defenses. In our data center business, the primary focus remains uncompromising physical security, and enabling safe, high-performance AI operations. We continue to invest in capacity across all our AI-ready data centers which are purpose-built to support this emerging ecosystem in the data center industry.

**As India emerges as a trusted global data hub, how is Sify reinforcing sovereign digital infrastructure while serving customers clients? Does a Make in India, Secure the World strategy define your approach to balancing domestic security priorities with global ambitions?**

As India positions itself as a trusted global data hub, our focus at Sify is on building sovereign digital infrastruc-



ture that is both self-reliant and globally competitive. The reality is that enterprises relying solely on global hyperscalers are inherently exposed to certain risks. That's why like-minded organisations in India are working to develop Indian infrastructure, Indian cloud platforms, and AI agents tailored to our unique needs.

Self-reliance begins with physical infrastructure. Our goal is clear—all components, from engineering to mechanical systems, should be made in India.

Equally important is enabling the growth of Indian cloud service providers. By opening our data centres to initiatives like Sarvam and the India AI Mission, we provide the robust, secure infrastructure they need to scale. This, in turn, fuels the development of India-specific Large Language Models (LLMs) and agentic AI applications.

**Beyond expanding capacity, how are you embedding AI/ML to autonomously optimize energy use, manage workloads, and preempt failures—while strengthening operational resilience against potential disruptions?**

A data center is one of the most complex infrastructures you can operate—within a single campus, power consumption can reach 200 MW, supported by a vast network of engineering systems and control mechanisms. Any failure in these components can disrupt not just our operations, but also those of our customers. This makes it critical to stay ahead of failures through early risk identification and mitigation.

Predictive maintenance has long been part of our approach, but AI and ML now allow us to take a leap for-

ward. By analysing vast streams of operational data, we can design the next-generation data center—one that is self-optimizing, self-correcting, and more resilient.

Our vision is to deploy AI agents that handle routine operational activities autonomously, from managing workloads to monitoring energy use and responding to anomalies in real time. These agents will not only improve efficiency but also free up human teams to focus on higher-value problem solving.

We're currently in the phase of collecting detailed operational data and mapping out high-impact use cases. The goal is clear: build AI-enabled data centers that predict, prevent, and adapt—ensuring uninterrupted service and strengthening resilience against any potential disruption.

**Given the link between energy resilience and national security, how are you integrating renewable energy, green certifications, etc., to ensure both environmental responsibility and infrastructure reliability?**

For us, the most immediate opportunity in driving both energy resilience and environmental responsibility is renewable energy. Energy consumption is the largest footprint a data center leaves behind, so we're taking decisive steps to change that. We've already signed agreements for approximately 300 MW of solar and wind power, and in the next few years, we aim to source 60% of our total energy needs from renewables—eventually moving towards 100%.

The next focus area is efficiency in design and operations. We are committed to minimising both energy and water wastage. On water, we've made a

conscious decision to avoid evaporative cooling and are using non-water-based cooling solutions. On energy efficiency, while Indian data centers operate at an average PUE of 1.5, we're working aggressively to bring this number down as low as possible.

The third priority is addressing Scope 3 emissions—the indirect environmental impact from equipment like generators and chillers. We are looking for more environmentally friendly options in these areas. We now have a dedicated ESG team that is driving our objectives and long-term strategy, and with strong confidence in our Scope 1 and Scope 2 progress, we are pushing for a greener, more resilient, sustainable and future-ready data center ecosystem.

**With 5G, IoT, and mission-critical applications demanding ultra-low latency, how is the company deploying distributed edge infrastructure to serve both commercial needs and national security use cases?**

We are actively expanding our distributed edge infrastructure, with our first edge data center in Lucknow set to launch soon, followed by several more in tier-2 cities. These facilities, typically in the 4–14 MW capacity range, will create a robust local backbone, offering caching, processing, and storage capabilities closer to the point of consumption.

In the immediate term, this proximity benefits use cases like OTT streaming and online gaming, where local caching significantly improves network efficiency and user experience by reducing latency. Over time, these same capabilities will be critical for supporting advanced AI workloads, IoT deployments, and other laten-

cy-sensitive applications as these technologies mature.

We also anticipate that next-generation hyperscalers will increasingly look beyond metro hubs, and our tier-2 data centers will be well-positioned to support that growth.

Importantly, distributed edge infrastructure isn't just about commercial opportunity—it plays a role in national resilience. For state governments, these edge facilities can serve as secure, AI-enabled local hubs to roll out large-scale digital initiatives without investing heavily in their own infrastructure. Whether it's for e-governance, smart city projects, or public safety applications, the ability to process and store data locally enhances both efficiency and security.

In essence, our edge strategy delivers the low-latency, high-performance foundation needed for the next wave of digital transformation—serving commercial innovation and national security priorities alike.

**How are you enabling secure interoperability between on-premise environments and hyperscalers?**

Secure interoperability begins with understanding how hyperscalers connect. They operate core data centers or availability zones and extend connectivity through transit centers or edge plugs that link their cloud to the wider world. Sify is uniquely positioned because we host not only the cores of these hyperscalers but also their plugs—enabling Direct Connect or Cloud Connect capabilities.

This allows us to offer customers dedicated, cross-connect links between hyperscaler clouds and their on-premise or private cloud environments. The result is ultra-low latency—often reduced from milliseconds to microseconds—while ensuring a fully secure, private connection.

**With the digital economy and technology ecosystem rapidly maturing, what will be your next major area of focus and innovation?**

As the digital economy matures, our focus is on building AI-ready infrastructure. We are investing in AI-enabled liquid cooling technologies, with all our data centers certified by NVIDIA. This isn't just on paper; we've deployed a live lab to study real-world power consumption and cooling efficiency.

While AI adoption in India remains in early stages, we see opportunities in applying AI for operational efficiency and enhancing sustainability. We are also closely monitoring quantum computing, which could revolutionize energy consumption models in the future.

Additionally, our Founder, Chairman & Managing Director, Raju Vegesna—originally a chip designer—has a long-standing vision to create a Made-in-India chip. This ambition aligns with our broader strategy of driving innovation from the ground up, ensuring India not only consumes but also creates core technologies.

**For more queries; email to [shaaz.hasan@timesofindia.com](mailto:shaaz.hasan@timesofindia.com)**

DISCLAIMER – THE VIEWS/CONTENTS EXPRESSED/PRESENTED HEREIN, WITHIN THIS ADVERTORIAL, PROMOTIONAL FEATURE, ARE THE SOLE AND EXCLUSIVE RESPONSIBILITY OF INDIVIDUAL CLIENTS/ THEIR AUTHORIZED REPRESENTATIVES, TO WHICH EFFECT, PUBLICATION HOUSE/ ITS REPRESENTATIVES ARE NOT RESPONSIBLE/LIABLE WHATSOEVER