FMBusinessDaily

Survey reveals IT directors turn to decentralised networks as cyber threats surge

4 months ago

Leading global enterprises face mounting risks as cyber threats escalate, prompting an urgent shift towards Decentralised Physical Infrastructure Networks (DePIN) to safeguard critical infrastructure, according to alarming new findings from Post-Quantum Security pioneers Naoris Protocol.

DePIN: A Critical Component of Cybersecurity Strategy

A ground-breaking global survey of senior IT directors across major corporations—with annual turnovers exceeding $300 million across the US, UK, EU, and APAC—reveals that an overwhelming 73% now classify DePIN as “extremely important” to their cybersecurity strategy. An additional 25% view it as significantly important, highlighting an industry at a critical inflection point.

The survey highlights deep concerns among IT leaders regarding cybersecurity weaknesses and preparedness, prompting rapid investment in DePIN—a blockchain-powered technology that decentralises physical infrastructure like cloud, network nodes, data storage, and edge devices.

Centralised cybersecurity solutions create single points of failure, exposing vulnerable devices to attacks and breaches from multiple adversaries. Centralised cloud services further concentrate risk, while weak endpoint detection leaves systems vulnerable. DePIN mitigates these risks by transforming devices into secure validator nodes that continuously validate each other, enabling a zero-trust, always-validated data architecture. According to the Messari State of DePIN 2024 report, DePIN projects have exploded, with more than more than 13 million devices running every day as market value exceeds US$50 billion.

DePIN’s Resilience Against AI-Powered Cyber Threats

DePIN technology is particularly noted for its resilience against sophisticated cyber-attacks, system failures, and the alarming rise of AI-powered hacking tools.

With approximately 2,369 active DePIN projects worldwide today, respondents anticipate explosive growth, with nearly 36% expecting the figure to exceed 4,000 within just one year. Additionally, about 31% foresee their organisation’s DePIN projects increasing by over 50% within two years, underscoring heightened urgency and investment.

Security & Trust: The Driving Force Behind DePIN Adoption

IT directors emphasised DePIN’s security and trust attributes as the primary attraction, surpassing other noted benefits such as operational efficiency and scalability.

● Network resilience emerged as the top priority, cited by 70% of IT directors as crucial to their current cybersecurity strategy.

● 60% highlighted DePIN’s robust security architecture, which decentralises critical system components, thereby reducing vulnerabilities associated with centralised infrastructures.

● Data management efficiency also ranks highly, cited by 39% of respondents, reflecting DePIN’s potential to transform compute and storage solutions.

● Scalability, essential for meeting the exploding demand of IoT ecosystems, is identified as a key advantage by 31%, with an overwhelming 92% of IT leaders acknowledging DePIN’s potential to significantly enhance cybersecurity scalability for connected devices.

Blockchain and AI-Driven Security Enhancements

The survey highlights specific blockchain and AI-driven security enhancements most valued by IT leaders:

● 34% named continuous real-time validation—a hallmark of blockchain technology—as the most promising security development.

● 20% emphasised eliminating single points of failure as a critical advantage.

● 42% stressed the importance of AI integration for dynamic, real-time threat detection, a key driver for securing both Web2 and Web3 digital environments.

David Carvalho, CEO and Founder of Naoris Protocol, warned: “The cybersecurity landscape is reaching a critical tipping point. IT directors at major global firms clearly recognise the threats posed by increasingly sophisticated, AI-driven cyberattacks and are urgently adopting DePIN technologies to mitigate these risks.

We are witnessing a seismic shift as enterprises decentralise infrastructure, dramatically enhancing resilience, security, and operational efficiency.”

This stark outlook underscores the urgency with which IT leaders are acting to address vulnerabilities exposed by an increasingly hostile digital threat landscape, emphasising that cybersecurity now firmly

dominates corporate agendas globally.