Securing quick service restaurant assets in the quantum era



A quantum-secure global network for the next generation of connected quick service restaurants.

Prepared for public release.

29.09.2026

Nisient

Contents

01 **Executive summary**
02 **The infrastructure challenge of global restaurant operations**
04 **The evolving cyber and quantum threat landscape**
07 **The Nisient IoTransit network architecture**
09 **Financial impact potential**
10 **About Nisient**
11 **Nisient's IoTransit network overview**
12 **Conclusion**
13 **References**

Nisient Pty Ltd

Level 1, 55 Collins St
Melbourne VIC 3000
Australia
ABN 40616962899

enquiries@nisient.com
+61 7 5227 9613
nisient.com

Executive summary

Quick Service restaurants today operate one of the world's most extensive and technologically sophisticated distributed networks. Some chains operate over 44,000 restaurants globally, serving approximately 68 million customers daily. Up to 93% of those restaurants franchised in 2021[1]. Each location functions as a digital node within an international system, with this complex network of digital assets including integrated kitchen appliances, point-of-sale systems, digital ordering technologies, supply chain platforms, and increasingly advanced operational analytics related to both food preparation and safety.

Using McDonald's as a case study, it continues to advance its core mission to create positive experiences by investing in digital transformation and operational modernisation as part of its "Accelerating the Arches" growth strategy. Other quick service restaurants are building a customer-centric sales and marketing framework by optimising mobile platforms, integrating delivery services, and improving drive-thru efficiency through digital asset management and connected infrastructure.

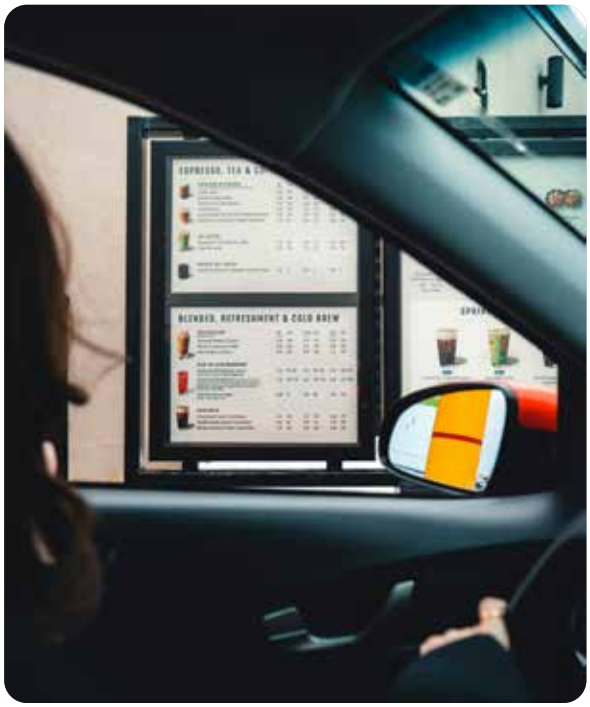
These initiatives are enabled by secure, reliable digital asset control and remote operations. Undertakings like this rely on robust, dependable connectivity that securely links millions of dispersed digital assets and facilitates not only seamless operations but also predictive maintenance to ensure consistent service standards across thousands of independent franchise locations.



The infrastructure challenge of global restaurant operations

Every quick service restaurant operates as a technologically complex environment. Behind the customer-facing experience lies a sophisticated operational system comprising numerous interconnected digital assets and devices. Kitchen appliances, refrigeration systems, environmental sensors, point-of-sale terminals, digital menu boards, and order-processing systems must operate seamlessly together to maintain service speed and food safety compliance.

Scaled across more than 40,000 locations globally, each with 12 to 20 interconnected kitchen devices, the result is a substantial network of operational technology assets. Each site functions as part of a broader distributed system that requires uninterrupted uptime while providing franchise operators with reliable operational tools, creating several significant challenges.



Continuous availability

Restaurants function continuously, often with extended hours or 24-hour service. Any interruption to kitchen equipment or operational systems can immediately impact customer service and revenue. The average cost to dispatch a technician is between $150 and $250 per hour (AUD)[6], with a MachineQ report indicating that 24 per cent of respondents estimate revenue loss of $1,001 to $5,000 per hour[7]. Ensuring uninterrupted operations across numerous establishments necessitates infrastructure capable of withstanding network outages, equipment failures, and regional disruptions, which is a non-negotiable requirement to remain competitive.

Operational consistency across franchise networks

For global quick service restaurants, global brand consistency is paramount in maintaining goodwill. The franchise model permits local entrepreneurs to operate restaurants in accordance with global brand standards. This consistency has been essential to its international success by standardising core food offerings, integrating drive-through facilities, and customising menu displays based on the time of day, weather conditions, current restaurant traffic, and trending menu items. Ensuring operational reliability across a vast and diverse network of up to 44,000 stores requires centralised oversight, including the ability to monitor and manage equipment performance across numerous locations simultaneously.

Expanding cybersecurity exposure

The rapid digital transformation of quick service restaurants to compete against rivals has fundamentally reshaped restaurant operations by connecting previously isolated systems into a unified, data-driven ecosystem. While this connectivity enables significant operational benefits, including real-time analytics and AI-driven automation, to improve customer experiences[8], it also substantially expands every organisation's cybersecurity attack surface. Devices and critical business assets that were once confined to local, closed environments are now integrated with cloud platforms, mobile applications, and enterprise systems, creating multiple entry points that can be exploited if not properly secured.

This challenge is further intensified by the emergence of next-generation artificial intelligence capabilities, such as Anthropic's Claude Mythos, which can autonomously identify and exploit multiple system vulnerabilities at unprecedented speed. The advent of such tools signals a step-change in the threat landscape, where attackers may increasingly leverage AI to orchestrate complex, multi-vector cyberattacks that can bypass traditional defences. For a globally connected enterprise, this elevates the urgency of adopting advanced, adaptive quantum security architectures like Quantum Key Distribution, capable of defending against both current and future AI-driven threats.

Fleet-scale device management

Software updates, configuration changes, diagnostics, and monitoring must be performed across thousands of geographically dispersed restaurants. Doing these tasks manually or through fragmented systems can create operational inefficiencies, splintered DevOps teams, and higher maintenance costs.



As part of corporate strategies in the quick service arena, restaurants are implementing advanced technologies, including edge computing, IoT-enabled kitchens, and AI-powered systems, to improve speed, accuracy, and efficiency across their global restaurant network[9]. Nonetheless, this heightened interconnectivity adds complexity, as each connected device, regardless of type, must be authenticated, monitored, and safeguarded with PQC in real time, regardless of network stability. The extensive scale of global operations, encompassing thousands of restaurants combined with highly distributed franchise models, further complicates maintaining consistent, quantum-resistant security standards across all endpoints, especially when novel algorithms will be necessary to stay ahead of emerging cyber threats.

The evolving cyber and quantum threat landscape

Quick service restaurants face unprecedented cyber threats, with rogue and misconfigured AI placed at the centre of heightened espionage and increasingly sophisticated adversaries. Conventional cryptographic techniques such as RSA and ECC will become vulnerable as commercial quantum computing becomes accessible.

With cyber breaches increasing, attackers will be able to break into back-end systems at a scale we have never seen before. Opportunistic actors have already begun collecting encrypted data to decrypt later and gain a strategic advantage[3]. To mitigate this risk, the U.S. National Institute of Standards and Technology (NIST) has launched a global effort to develop new, more secure encryption methods based on mathematical algorithms resistant to quantum-computer decryption. Although no commercially viable quantum computers exist as of 2026, a combination of public collaboration, AI tools, and faster computer processing could potentially break modern encryption techniques[4].

As we have seen with the rapid uptake of large language models like ChatGPT. Agentic AI (AGI) and quantum computing, currently at the development and laboratory stage, will eventually become accessible to the global community once a pathway to commercialisation is established.

For many software providers, hardware vendors, and operators, implementing Post-Quantum Cryptography (PQC) is a significant challenge, as legacy systems require updates, rigorous testing, and stronger security protocols that ageing hardware can support. A key advantage for Nisient is our control over the data layer at both ends of the communication channel, complemented by capabilities that enable an agile cryptographic approach and allow us to update and replace encryption techniques as needed. This ability is particularly important for protecting long-lived, business-critical digital assets, including connected kitchen devices and operational technology supporting quick service restaurant expansion strategies.

To stay competitive, essential global infrastructure requires a secure-by-design, zero-trust network that withstands current threats and anticipates future risks in the quantum era. The Nisient IoTransit Network fulfils this requirement with a deployment-ready, post-quantum-protected network architecture, guided by a strategic directive to implement Quantum Key Distribution[5].

Whereas PQC uses mathematical algorithms and can be deployed through classical computing infrastructure, quantum key material uses changes in entangled photons, called qubits, to detect interception attempts and alert the classical PQC security layer to auto-rekey. The QKD network also provides ultimate security by ensuring unique security keys, preventing AI from finding inherent patterns in computer-generated random key generators.

The strategic objective is therefore not to rely on a single cyber pathway, but to establish a layered approach to crypto-agile security that can evolve as the threat landscape changes. Without robust cybersecurity controls and cryptographic agility that enables real-time, network-driven key switching, any vulnerability in this interconnected environment could cause service disruptions, data breaches involving customer or payment information, or compromise of operational systems. This risk is particularly critical in a business where uptime, speed, and customer trust are essential to brand reputation and revenue generation.

For quick service restaurants where digital assets are expected to remain operational for many years, this approach reduces dependence on any one cryptographic algorithm and provides a structured migration path as PQC, AI-enabled cybersecurity, and quantum technologies mature.

'EVE' in the following figure (1) is no longer simply a rogue actor, corporate espionage or geopolitical influence but could instead represent misconfigured AI or AI cybersecurity tools designed to detect software vulnerabilities.

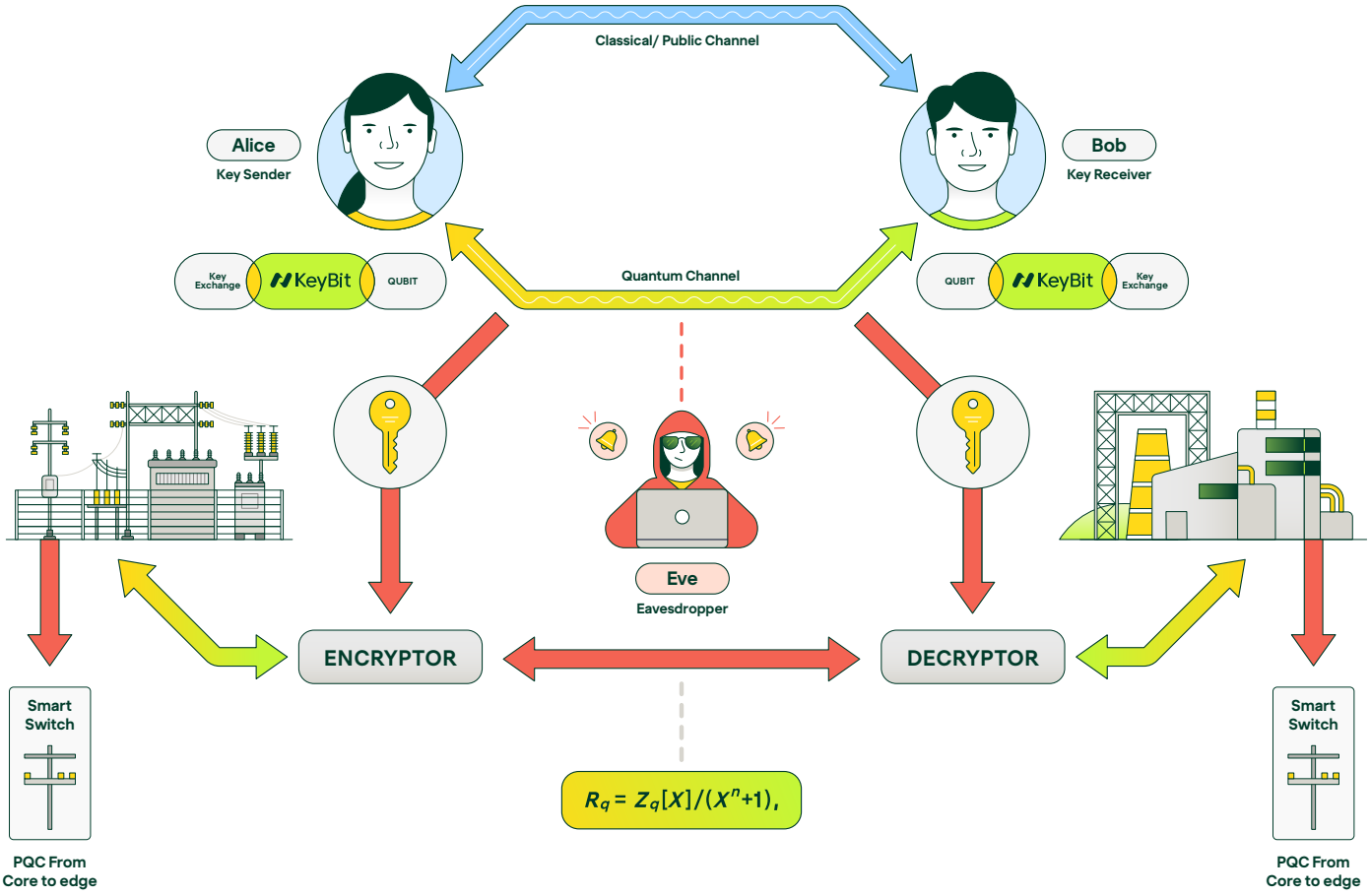


Figure 1

Eve is now considered to be an automated system being 'materially uncontrolled'

The evolving cyber and quantum threat landscape (continued)

Quantum as a risk and an opportunity

Traditional encryption systems widely used today will eventually become vulnerable as quantum decryption capabilities mature. Organisations operating long-lived distributed infrastructure must already be on the journey to transition to quantum-resistant cryptographic systems. Addressing these challenges requires running PQC over a networking architecture designed for global operational environments with unstable, varied, and sometimes low-bandwidth network topologies, rather than conventional high-speed enterprise IT infrastructure.

A quantum security opportunity naturally presents itself when you adopt a cybersecurity strategy that places Quantum Key at the core and bridges it to the PQC security layer, so your network can distinguish network instability from an attempted security breach.

Over time, commercially viable quantum computers will enable hybrid CPU/GPU/QPU data centres, and Nisient have already partnered with a range of global data centres to ensure the highest level of trust and dedicated space to commercialise what will become the gold standard of encryption.

Quantum Key Distribution (QKD) provides theoretically verifiable security, but its practical use is currently constrained by physical infrastructure requirements, distance limitations, cost, and operational complexity. Nisient's strategic objective is to create a bridge between QKD and PQC, enabling customers to access quantum-resilient security now while remaining prepared to adopt QKD capabilities when they become operationally and financially feasible.

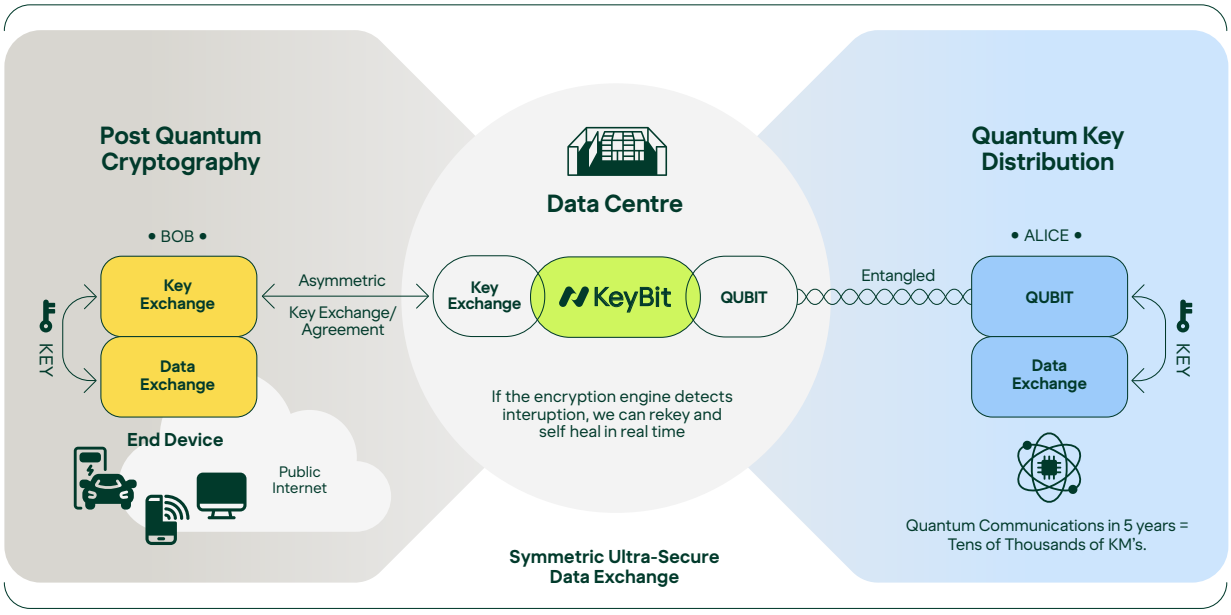


Figure 3

The Nisient IoTransit bridge between QKD and PQC

The Nisient IoTransit network architecture

Massively scalable architecture

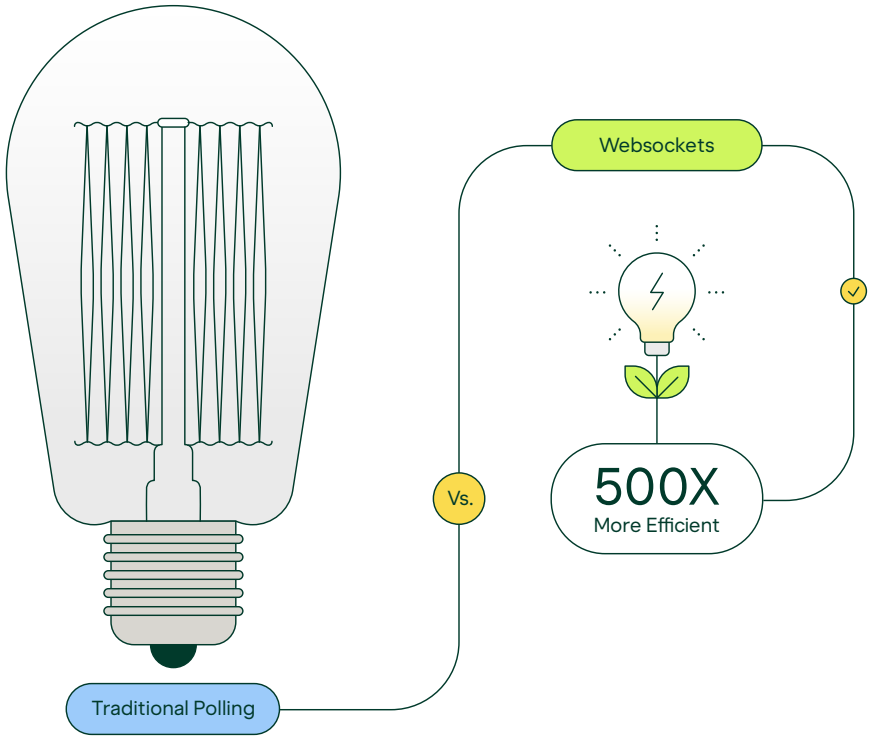
By deploying event-driven WebSocket message processing, Nisient's IoTransit Network is engineered to let various tasks operate and adapt independently, without relying on a single central process. This configuration enables functions such as connecting new devices, collecting data, transmitting commands, controlling individual devices or an entire restaurant, and conducting extensive, countrywide analytics to manage increased demand autonomously. As a result, the platform can handle significant surges in activity in a specific area without performance degradation or operational delays.

Energy saving

WebSockets offer more efficient communication by maintaining a persistent connection between devices and servers (10), enabling instant data exchange without repeatedly opening and closing connections. Unlike traditional REST APIs that require continuous requests to check for updates, WebSockets enable real-time, bidirectional communication with lower latency, reduced network overhead, and improved server efficiency. As a result, they are well-suited for applications that depend on live data, including IoT platforms, messaging systems, real-time analytics, and interactive dashboards.

Figure 2

WebSockets return a 500 times greater energy efficiency over traditional polling networks



The Nisient IoTransit network architecture (continued)

Triple redundancy and geographic distribution

The reliability of PQC-secure data pathways constitutes a fundamental design principle of the Nisient platform. Core services run with triple redundancy across geographically dispersed infrastructure to ensure continuous availability, even during regional outages or infrastructure failures.

This architecture incorporates several layers of fault tolerance, including service redundancy, triple data replication, and global geographic distribution, ensuring business-critical services always have multiple operational pathways. As a result, it delivers a resilient, unified platform that monitors, manages, and maintains operational continuity for mission-critical device fleets worldwide.



Automation-first operational framework

Automation or machine-to-machine learning represents the foundation of the Nisient IoTransit Network, not through insecure third-party AI or AI written code but through 20 years of experience in building software-defined, sensor-controlled networks that prioritise leading security frameworks to facilitate workflows and automated responses to system events.

Financial impact potential

Connected operational platforms have demonstrated measurable economic benefits[11] across the restaurant industry. Predictive maintenance alerts can warn when equipment moves outside standard operating parameters and reduce downtime by enabling early detection of performance anomalies or faults. Remote control and diagnostics reduce technician dispatch costs by allowing many issues to be resolved without on-site visits.

Automated monitoring systems can also mitigate food waste by ensuring that refrigeration equipment maintains appropriate temperature ranges. Intelligent energy management systems connected via IoTransit can optimise power consumption across refrigeration, cooking equipment, and HVAC systems. Furthermore, the system automatically upholds food safety standards by monitoring food temperatures throughout the cooking cycle.



About Nisient

Nisient is a network technology research and development company with over forty years of experience in deploying global telecommunications and software-defined infrastructure.

Its leadership heritage dates back to the mid-1980s when one of the founders contributed to the development of SONET/SDH within international standards bodies such as ANSI T1X1 and CCITT (now ITU-T), helping to establish software-controlled, self-healing architectures that form the foundation of modern carrier-grade networks.

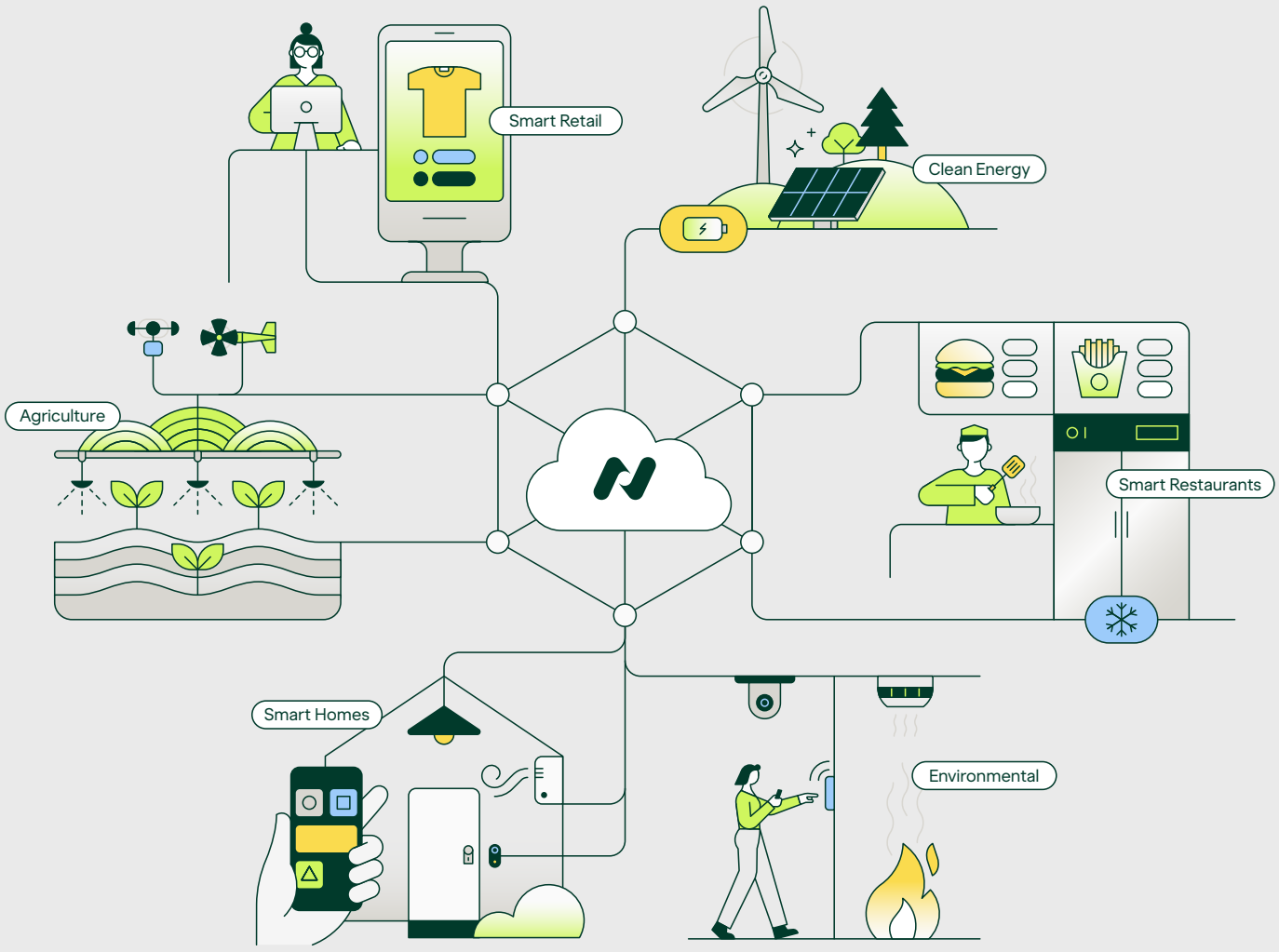
Nisient's IoTransit network offers a significant competitive edge through our software-native approach to resilience, security, and distributed control, bypassing the hardware legacy limitations faced by most supervisory control and data acquisition asset vendors and enabling a globally distributed, quantum-ready network architecture designed for the next generation of digital operations.



Nisient's IoTransit network overview

The Nisient IoTransit Network is a global, real-time, secure, software-defined data network designed to support fleets of digital and operational technology assets across diverse industries. Its architecture enables seamless management, monitoring, control, and communication for quick-service restaurants, point-of-sale systems, IoT deployments, and energy and utility infrastructures, delivering remote secure access through a single pane of glass.

The Nisient IoTransit network represents a significant advancement in how our global customers safeguard, manage, and connect their digital systems within the quick-service restaurant industry. Designed not only for predictive maintenance and kitchen monitoring to ensure compliance with food safety standards, Nisient's extensible, triple-redundant network provides post-quantum cryptography-based security for digital assets across any restaurant function.



Conclusion

The quick service restaurant industry operates one of the most extensive, distributed, and technologically sophisticated networks in the world. As companies embrace a future of uncertain cybersecurity, the resilience and intelligence of underlying infrastructure become increasingly mission-critical.

Nisient is uniquely positioned to support this evolution. As an Australian enterprise delivering secure, large-scale edge-to-remote communications across 53 countries, Nisient's IoTransit network already forms part of a quick-service restaurant operational ecosystem. This creates a powerful advantage when extending secure connectivity to connected kitchen assets, with no additional development investment or complex deployment model.

With triple-redundant, geographically distributed architecture, native post-quantum cryptographic agility, predictive analytics, and remote device management delivered at only cents per device per month in OPEX cost, the Nisient IoTransit network provides a practical, scalable pathway to modernise restaurant operations while preparing for future cyber and quantum threats.

In a business where kitchen appliances, refrigeration, digital menus, point-of-sale systems, and order processing platforms must operate seamlessly to maintain speed, compliance, and customer trust. Predictive maintenance and secure operational visibility are no longer optional; they are strategic necessities.

Nisient enables global operations to transform these connected assets into an intelligent, resilient, and quantum-ready operational network that reduces downtime, lowers maintenance costs, strengthens food safety assurance, and supports continued global growth. The opportunity is clear: leverage infrastructure already in place to unlock a more connected, secure, operationally efficient, and future-ready ecosystem.



References

1 **McDonald's: Number of Restaurants Globally (2005 – 2021)**
https://www.globaldata.com/data-insights/foodservice/mcdonalds-number-of-restaurants-globally/

2 **McDonalds Strategic Direction**
https://corporate.mcdonalds.com/corpmcd/our-company/who-we-are/business-model-and-growth-strategy.html

3 **Harvest Now Decrypt later**
https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

4 **Public decrypt efforts**
https://www.ecdsa.fail/

5 **Quantum Key Distribution**
https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

6 **Average Commercial Equipment fee**
https://www.ckeservice.com.au/rates

7 **Lost Revenue**
https://corporate.comcast.com/press/releases/restaurant-operators-surveyed-report-lost-revenue-equipment-downtime-machineq-report

8 **AI Automation**
https://corporate.mcdonalds.com/corpmcd/our-stories/article/technology.html

9 **Edge Computing and IT Infrastructure for Quick-Serve Restaurants**
https://www.scalecomputing.com/qsr-it-solutions

10 **WebSockets versus polling**
https://www.pubnub.com/blog/websockets-vs-rest-api-understanding-the-difference/

11 **WebSockets versus polling**
https://iot-analytics.com/state-of-enterprise-iot-from-iot-autonomous-connected-operations/

Nisient

Contact

To learn more about our IoTransit Network or begin your transition of entire- site assets and connected kitchen function to quantum-secure global operations:

enquiries@nisient.com

+61 7 5227 9613

nisient.com