

# Retail efficiency journey to Zero Trust Virtual Networking



## Background

The future of retail is heavily influenced by technology, with the growth of smart retail systems and the use of advanced technologies such as AI, IoT, and big data analytics. Technologies are enabling retailers to provide personalised experiences, optimise inventory management, and improve operational efficiency. According to a report by Gartner, the number of connected devices used in retail will reach 5.4 billion by 2025, up from 3.7 billion in 2018. Smart supermarkets use connected IoT devices to collect physical data, relay this information to digital platforms and help grocery store staff make better decisions, from smart shelves to smart grocery carts, cashier less options and underlying infrastructure support. The future of smart retail requires secure, high-performance seamless connectivity.

## Challenge

For the retailer, the first layer of an ecosystem comprises of smart retail IoT devices that include beacons placed strategically throughout the store, POS technology, Video surveillance systems and RFID technology. All are connected to the retailer network, and transmit data back and forth to the data repository, which in turn interface with the analytics platform and the retail business systems. Of course, for the retail enterprise, there are several IT investment implications when creating a safe, secure and effective IoT ecosystem. Areas like device authentication and authorisation, network performance and wireless communications, device and traffic administration, and data analytics and storage are just some of the big ones. With so much data being generated a robust and efficient network infrastructure is critical to support real-time data processing and analysis, low latency communication, and secure data transmission to protect against cyber threats.



**Industry**

Retail



**Challenge**

- Asset visibility, tracking and management
- Simple, easy and secure management of a distributed network
- Network segmentation complexities
- Network access requirement for dumb terminals and the supply chain
- Multi-layer networks, fast switchover, low latency and uninterrupted services
- Bandwidth-intensive applications and services



**Goals**

- Optimise Asset and Energy Management
- Simpler and better networks at lower costs
- Maximise network stability and availability
- Strengthen security on the edge devices and isolation of each data stream
- Pervasive and ubiquitous secure technology at more than just the network layer
- Adopt granular and transparent access controls
- Seamless integration for easy setup, deployment

## Solution

SElink™ provides a zero trust security model combined with Service-level software defined network segmentation, granular privileged access management. Delivering efficiency, security and control to Devices and Networks in a single solution.

## Solution

**SElink™** introduces **Virtualisation, Isolation and Security** for Retail back-office networks and interactions with the **Supply chain and Third Party providers (IT, Equipment, Services)**, ensuring a **logical separation of the network domains**. Each host and network is isolated and segregated from the data link layer, up to and including the application layer. Identification, authentication and authorisation of hosts to access services is based on least-privilege principles, increasing the overall security posture of the environment. SElink™ is more than a data diode or traditional network-based segmentation through subnets. **SElink™ is a Zero Trust service-oriented, secure, virtual networking solution** to replace siloed IT systems and infrastructures for simpler and efficient networks, cost savings and streamlined operations across distributed networks. **SElink™ provides** smart mechanisms for **network stability** and **low bandwidth requirements**, extends **protection to the edge devices**, **segregate services and create private networks**. It replicates heterogenous clients and server behaviours in a seamless way, as in a private LAN. The **SElink™ Gateway** acts as a broker and performs connectivity virtualisation to the endpoints. The advantages are overwhelming. **SElink™** protects both the data channel and the access to the communication channel, which can only be used by authorised processes. This ensures that the server is protected even if the endpoint device is compromised, preventing infection propagation through the network and major service disruptions. **Implementing SElink™, devices no longer need public static IP addresses, resulting in a significant reduction of the attack surface, increased efficiency and substantial savings on operational costs.** Lightweight protocols and zero encryption overhead make band availability and integration of security no longer a limit. Easy integration in any environment, over any protocol, portable, multi-device for a fast deployment of new devices without requiring experts to travel to the site. **SElink™** is ready to use the Post-Quantum algorithms shortlisted by NIST. Crypto agility allows **SElink™** to migrate to new symmetrical algorithms in a centralised way without any effort. A centralised deployment and management security system guarantees control across a large-scale network.

## Benefits

1. **Unstoppable connectivity** through anti-shaping, network stability and non-evident headers techniques
2. **Low-bandwidth strategies and smart mechanisms** to improve QoS and availability of service
3. **Virtual one-way dynamic micro-segmentation links** at service level to different sites simultaneously
4. **Private networking**, no need for costly dedicated connectivity contracts
5. **Unified Management Platform** for security automation, greater network visibility and control
6. **Zero Trust Network Access and Assumed Breach model** strategies
7. **Enhanced system longevity and resilience** to quantum attacks and **Seamless encryption updates, redesign-free** through Crypto Agility

