Case Study

Transforming Vending Competitiveness with Zero Trust

Background

The need for readily available items has increased following consumers' busy lifestyles, and urbanisation. Due to this and to digital payments choices, the demand for vending machines, particularly in offices, commercial spaces, and public areas, has accelerated. With so many touch points and channels available for consumers, vending operators are pressured to create a frictionless end-to-end experience: from a seamless user journey to fast payment, customised messaging and agile supply chain. Technological innovations (face and voice recognition, interactive display systems and big data integration) and the advent of IoT, have contributed to respond to consumer demand, increase operational efficiency and straightforward vending machine management. Wireless solutions facilitate transactions anywhere. To support their growth in a fast-evolving digital world, companies have to manage system complexity.

Challenge

Vending machines, as cyber-physical systems, rely on machine-to-machine communication, enabled by technological innovations and wireless connectivity. Telemetry and online cashless payments drive the interconnection of vending machines. Hence vending machines makes the devices susceptible to various challenges and risks including counterfeit money, stock shortages, maintenance field trips, increased costs, limited infrastructure, high data transfer costs, technological constraints, geographical challenges and regulatory issues. Vending machines often operate in areas with conflicting or costly data transfer capacities, posing challenges for real-time communication, remote monitoring, and data transfer. Furthermore, vending machines integrate sensors and connect to local networks for real-time data, yet this connectivity exposes networks to potential online threats. Hacking is a growing concern in cashless payments. Therefore, new architectural and security measures are essential to address system complexity across all levels.

Industry

Vending Systems

Challenges

- Low and less reliable data transfer capability
- Establish and maintain consistent connectivity
- Expensive data transfer capacity
- Reliable connectivity
- Ability of VMs to communicate effectively
- Vulnerable wireless communication channels
- Remote maintenance
- Vending machine efficiency
- Network and Device vulnerabilities

Goals

- Granular Access Controls for Remote Maintenance
- Efficient Asset Management
- Simpler networks at lower costs
- Enhanced service speed
- Consistent and affordable data connectivity
- Stronger security on the Vending Machines
- Isolation of each data stream to the datacenter
- Increased network stability and availability
- Seamless integration for easy setup, deployment

Solution

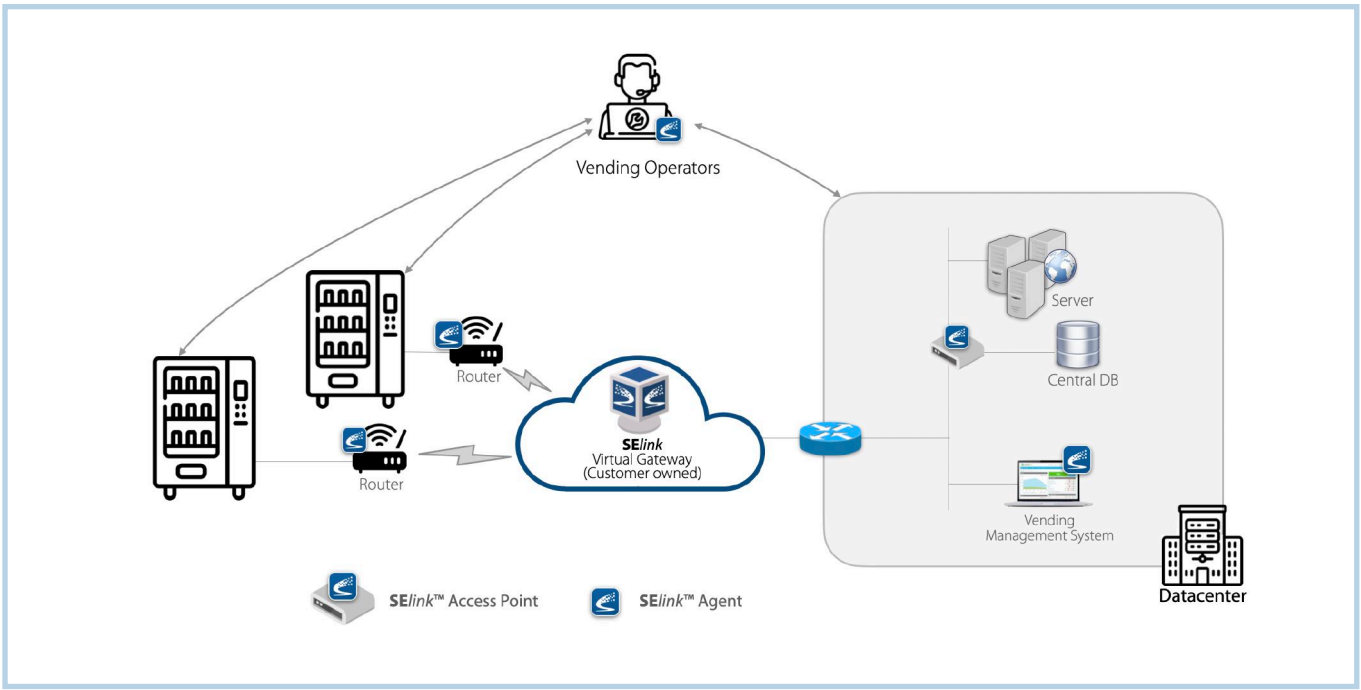
SE*link*™ provides a zero trust security model combined withs service-level software defined network segmentation, granular privileged access management. Delivering efficiency, security and control to Devices and Networks in a single solution.

Solution

SE*link*™ solves connectivity, networking and security challenges of Vending Solutions enhancing the ability of vending partners to seamlessly and securely operate cross various channels. **Introducing Virtualisation, Isolation and Security, SElink ensures a logical separation of the network domains at different levels -** the network, the devices and the interactions with the Supply chain and Third Party providers (IT, Equipment, Issuers, Services). 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. **SE*link*™ 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. **SE*link*™ 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 SE*link*™ Gateway acts as a broker and performs connectivity virtualisation to the endpoints. The advantages are overwhelming. SE*link*™ 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 SE*link*™, 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. SE*link*™ is ready to use the Post-Quantum algorithms shortlisted by NIST. Crypto agility allows SE*link*™ 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. **Improved QoS and service availability** through low-bandwidth strategies and smart mechanisms
3. **Virtual one-way dynamic micro-segmentation links** at service level to different sites simultaneously
4. **No more costly dedicated connectivity** contracts with Private Virtual Networking
5. **Security automation, greater network visibility and control** delivered by a Unified Management Platform
6. **Empowering 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



Blu5 Group
info@blu5group.com
www.blu5group.com