SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Increasing Data Integrity and Resilience in Retail Businesses

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved as a means for practitioners to choose a trustworthy risk mitigation provider with confidence when there is a myriad of options in the marketplace. Proven Solution Innovation Practice Case Studies help to evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This Solution Innovation Case Study offers a proven process approach for mitigating risk(s) that could result in injury or impairment of people, assets, critical processes, products and/or brand reputation. This proof point examines representative risk issues, mitigations and result outcomes as validated by the SEC and end-user.

The following case study demonstrates a unique data communication and security enhancement for a fast-casual restaurant chain with operations in the United States and Canada. The project objective involved enhancement to the security, throughput, and reliability of data connections for point of sale (POS) and customer focused data communication. SecurePCN™ worked with the parent company and a major franchisee to evaluate a new solution and set a path for widespread adoption.

Context and Background:

Howley Bread Group is a franchisee with forty (40) Panera Bread bakery-cafe fast casual restaurants. The project involved a Proof of Value (PoV) demonstration of the SecurePCN™ cellular data communication solution at two cafe locations, franchisor corporate office, and franchisor datacenter to prove the viability and value of SecurePCN™ prior to corporate-wide approval.

The franchisor corporate IT manages all IT activity for franchisees, including help desk functions. They also mandate the use of a Cisco architecture with MPLS as the primary connection augmented with a blend of T1, Cable or Internet VPN as a secondary redundant circuit for branch office communications. In-store data systems serve three primary purposes: Point of Sale data communication, in-store data network, and customer WIFI. Most franchise locations have a mixture of MPLS, T1, and broadband connectivity. Franchisees have the ability to utilize any corporate approved primary and redundant communication sources based on local availability and service cost.

Risk Issues and Mitigation Opportunities:

The Howley Bread Group was looking for a primary circuit for their Point of Sale (POS) data connections that

- Meet the service level agreements (SLAs) of a T1 line
- Reduce operating expense (currently $250-$482 per month)
- Exceed the existing bandwidth connectivity of legacy T1 connections (1.54 Mbps)

The franchisor desired to test cellular as a primary form of cafe connectivity to their datacenter. Prior to discussion with SecurePCN™ the franchisor had investigated a custom-developed cellular communication system for cafe locations.

POS data transfer in a secure and reliable manner was of highest priority. This communication is the financial lifeblood of a cafe and subject to Payment Card Industry Data Security Standard (PCI DSS) conformance.

Solution Requirements:

- Howley Bread Group
  - Reliability up to the expectation of a T1
  - Bandwidth exceeding existing solution
  - Data transfer latency exceeding existing solution
  - Lower cost than current solution
- Franchisor Corporate IT
  - Measurable improvement in latency, bandwidth, and uptime as depicted through network telemetry
  - Support inclusion of “DevOps” downloads during off hours, which isn’t viable with existing T1 architecture
  - Operate within the existing Cisco-based Dynamic Multipoint VPN environment
- Route all POS data from cafes to the franchisor datacenters.
- Payment Card Industry Data Security Standard (PCI DSS) compliance. This relies on secure communications infrastructure, so any alternate data communication path must adhere to PCI DSS.

Delivered:

- Established a reliable and secure data transit solution from each cafe to the franchisor Datacenter for business-critical POS data.
  - Installed a communications platform at two cafe locations, franchisor datacenter, and franchisor corporate IT location that is encrypted, segmented and monitored; thereby reducing and potentially eliminating the vast majority of communications threat surfaces.

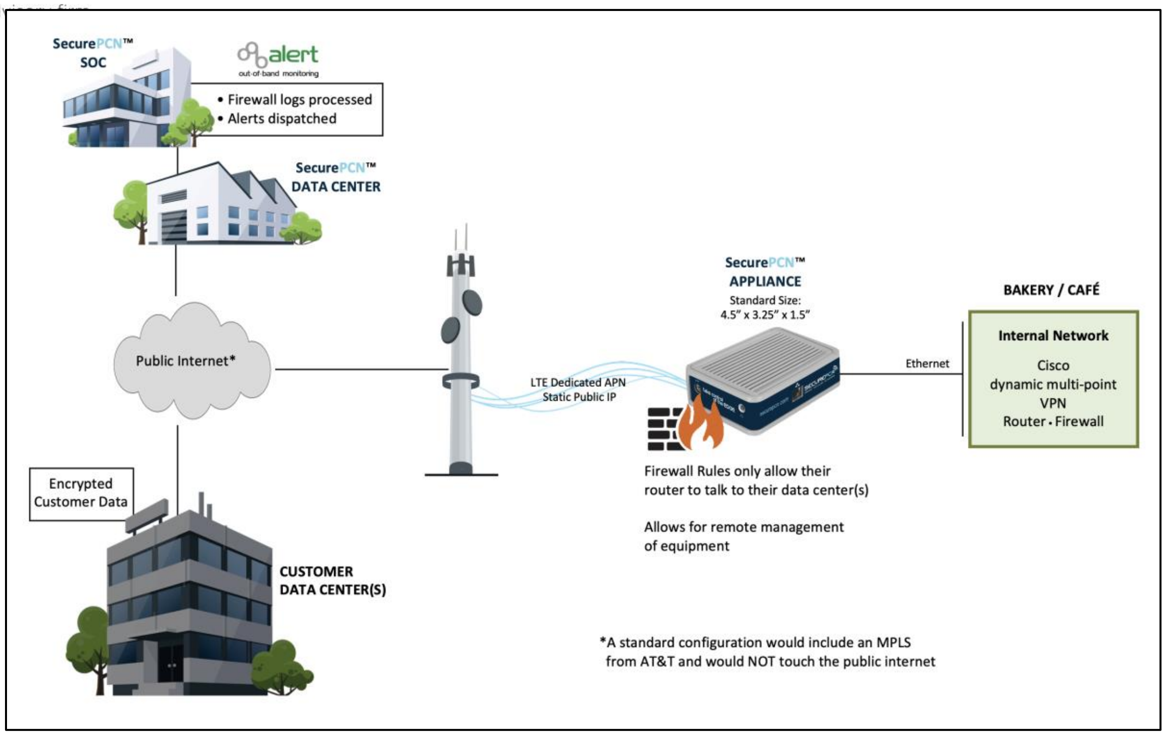

Figure 1 – SecurePCN™ deployment for Howley Bread Group

- Data communication achieved using a prioritized, reliable and efficient Machine to Machine (M2M) cellular network.
  - Unlimited monthly data, unthrottled, and with no overage charges.
- SecurePCN™ adapted the standard 4G LTE security appliance solution to integrate with the Cisco infrastructure. The SecurePCN™ appliance was installed between the customer's Cisco architecture and the Internet with the SecurePCN™ edge firewall limiting traffic to individual "known" IP addresses.
- Maintained Point to Point (P2PE) with AES 256 encryption of all data.
  - SecurePCN™ P2PE AES256 encryption was deferred for this application to utilize the franchisor-managed encryption included in their pre-established PCI DSS program.
- Established a direct datacenter connection to franchisor business management systems in a manner approved for application to all cafe locations and corporate facilities. The SecurePCN™ datacenter connection to franchisor was direct to a secure data network supporting all company operations.
- Implemented a Data Firewall with Deny by Default Rules. Created an edge firewall that only allows IP addresses and ports prescribed for the franchisor datacenter traffic while denying all other non-prescribed traffic.
  - No one can add, remove or relocate a device without customer authorization.
  - No unauthorized phone home capabilities for any edge-connected device.
  - No unauthorized or unintended streaming of data.
- Established continual Out of Band (OoB) monitoring to assure only authorized communication occurs, without touching or monitoring customer's encrypted data.
  - SecurePCN™ monitors bandwidth utilization and latency as well appliance status (power on/off, POS connection, temperature, etc.). Alerts regarding operations anomalies are directed to the franchisor corporate IT and Howley Bread Group.

  - Alerts delivered to customer of detected data transmission or attempted penetration anomalies.
- Established Zero Trust Architecture (ZTA) compliant implementation meeting ZTA tenants as defined in NIST 800-207 guidelines.
- Installed SecurePCN™ appliances that are future-enabled for 5G.

Outcome and Benefits of Service Including ROI:

Business Benefits

- During the multi-month system test, POS data along with other restaurant operations data was transferred from cafes to franchisor. POS data was prioritized as the most critical data to Howley and the franchisor.
- Minimum of 44% monthly reduction in internet service expense per franchise location and savings of $57,600 per year across 40 cafes.
- As a result of SecurePCN™ evaluation success, the Howley Bread Group has initiated all 40 locations.
- SecurePCN™ was vetted by the franchisor corporate IT and approval is expected for rollout to the remaining franchisees as well as franchisor cafe locations.
- Realized customer retention and marketing value improvements that were unexpected. The increased bandwidth allows the franchisor to push out marketing content in real time that was not possible or previously envisioned as realistic due to prior connection limitations.
- Confidence of online, kiosk, and in-store sales received and processed moved from 7 to 9.9.
- Insider risk during T1 connectivity outage is virtually eliminated.
- Transaction throughput and kiosk internet speed for administration and training fully realized but not yet measured due to COVID-19.

Technical Benefits

- SecurePCN™ serves as a firewall at the edge, blocking all but the known IP address, serves as a means of transport of the data (cellular), and provides OoB integrity monitoring without touching encrypted customer data.
- 100% uptime and zero data packet loss during the 3 months the SecurePCN™ machine to machine private cellular network was under evaluation.
- 30x improvement in data transfer speeds realized for Howley Bread Group in comparison to the legacy T1 circuits (50 Mbps vs 1.5 Mbps B).
- Rapid deployment, no lag time for cable installation or T1 service configuration.
- Additional remote management capabilities for router/firewall.
- Established a solution applicable to use for primary and redundant data communication.
- Data going out to managed internet using franchisor-defined encryption with managed firewall (SecurePCN™).
- PCI DSS compliance
  - Continuously monitored security control and compensating controls found in PCI DSS versions 2.0 / 3.6, 3.6.1, 3.6.2, 3.6.3 satisfies the compensating controls necessary to protect PCI DSS data transactions. SecurePCN™ does not hold data, it is part of the ecosystem that transmits securely and monitors this transaction.
  - ZTA conformance supports new PCI DSS v4.0 requirements (currently in final review).

- Howley Bread Group and the franchisor corporate IT praised SecurePCN™'s ability and willingness to understand their infrastructure and adapt to their needs. Sincere appreciation expressed regarding SecurePCN's flexibility and willingness to implement the level of solution that met their needs and risk tolerance.
- Approval to work with their franchisor corporate systems support partner, Retail Technology Group, in providing on-site service and installation support.

SIP Case Study Authentication Process
This process was overseen by a Council Faculty member with 20+ years of experience in developing and leading people and asset protection programs as trusted security advisor for global and multinational organizations. End-user authenticated May 2021**.**

Note: *The Security Executive Council's Solution Innovation case study represent a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

A General Comparison of Competition

	SecurePCN™ (LTE) Standard Offering	Cellular (LTE)	T1 with IPSec Tunnel
Cost	**$$** • Modem/Appliance purchase • Fixed monthly rate • No long-term contract • No cable installation costs	**$$** • Modem/Appliance purchase • Cellular plan required • Bandwidth overage charges and/or data throttling • No cable installation costs	**$$$$** • Modem/Appliance purchase • Fixed monthly rate • Long-term contract required • Cable installation
Connection Type	Cellular – Commercial Grade	Cellular – Consumer Grade	Typically fiber
Throughput	Up to 50 Mbps up Up to 300 Mbps down	Up to 50 Mbps up Up to 300 Mbps down	1.5 Mbps up 1.5 Mbps down
Security	Zero Trust Architecture (ZTA) framework	None	Typically Secure
Encryption	Point to Point (P2P) AES 256	None	AES 128 / AES 256
Data Segmentation	• Data never traverses the public internet • No routable IP addresses	Public IP address	None
Monitoring	• Out of Band (OOB) • Deny by Default Rules • Customers alerted to detected anomalies	None	None
Management	• Service Level Agreement • Configuration management • Device & patch management	None	Self-administration
Deployment Timeline	Immediately deployable and fully operational in minutes	Immediately deployable and fully operational in minutes	Weeks to Months
Data Priority	Prioritized, reliable and efficient Machine to Machine (M2M) cellular network	Standard consumer cellular data priority	Prioritized dedicated line
Expandability & Upgrade Path	Upgradeable to 5G	Upgradeable to 5G	No clear upgrade path without technology change or installing additional capacity

Note: SecurePCN™ LTE plan deviations available upon customer request, as was the case with Howley Bread Group.

See other case studies and learn more about the SIP Program here:
https://www.securityexecutivecouncil.com/about/solution_innovations.html