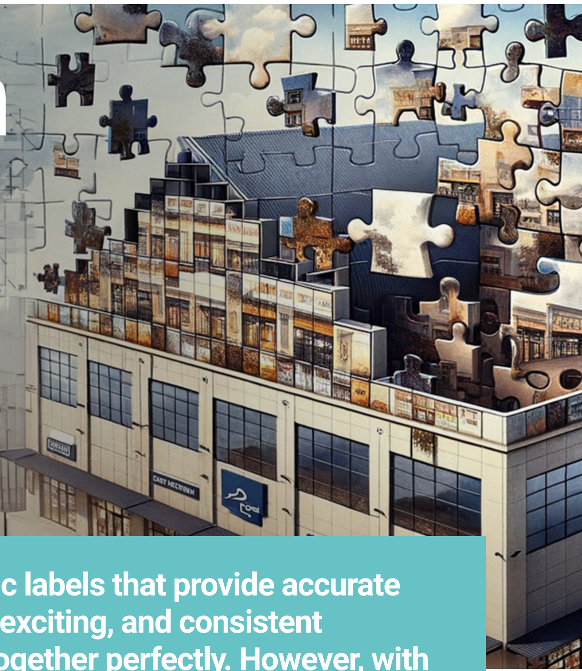
Retail

C-Store

Solve the IoT Protection Puzzle in Retail and C-Store Environments



Retailers and C-Stores were early adopters in the Internet of Things (IoT) revolution, using technologies for monitoring, automation, and process efficiency.

More recently, IoT has helped modernize store shelves via electronic labels that provide accurate pricing to consumers. The goal of all these efforts is to create new, exciting, and consistent customer experiences. When done right, all the pieces seem to fit together perfectly. However, with the increased risk and expansion of the digital attack surface brought on by IoT, it may seem like you are putting together a puzzle with no clear edges.

1 The Cipher

My IoT devices have impenetrable native security. No one can break the code protecting them.

2 The Analysis

The global IoT market for retailers was valued at $28.1 billion in 2021 and is projected to reach $177.9 billion by 2031.[1] This projected growth will connect more devices to retail and C-Store networks, exposing more openings for attackers to exploit.

4 The Fool-Proof Encryption Key

Retailers and C-Stores across America trust SageNet to thwart ransomware and other threats against their data, networks, and IoT devices. Powered by Fortinet security solutions, SageCONNECT™ delivers the safe, high-performance networks required to operate IoT devices, enhancing customer experiences and employee productivity. Detect and respond to anomalies before they become problems with the complete visibility and predictive analytics of SageIoT™. Robust device user management and access control secure IoT devices and maintain top performance.

3 Cracking the Code

Even though IoT is not a new concept, the truth is there is still a long way to go when it comes to standardization of security protocols and controls in the industry. IoT devices often have insufficient authentication controls, providing an access path for ransomware attacks.[2] As ransomware becomes commoditized, making it easier to build and deploy, what once was a fragmented threat actor community has now evolved into organized "cyber-crime-as-a-service." This means retailers must be on guard against the threats posed by improperly secured IoT devices and the networks that they run on.

SageNet's solutions can help you crack the code to ironclad IoT protection and complete visibility, whether you're tracking assets and battery performance or using an RF scanner to streamline pick, pack, and ship fulfillment workflows.

[1] Allied Market Research, IoT in Retail Market Global Opportunity Analysis and Industry Forecast, 2021-2031, August 2022.

[2] Fortinet, What is IoT Security? Challenges and Requirements, 2023.

To learn more about how SageNet provides ransomware protection for your retail operations and C-Stores, from store one to store 1,000 and beyond, read our eBooks–**Demystifying Ransomware for Retailers** and **Demystifying Ransomware for C-Stores**.