
Sagenet
FORTINET
Demystifying Ransomware for C-Stores
Harness the Power of Data Protection


# Ward off the Dark Arts

As a convenience store (C-Store) owner, you likely rely on digital resources that collect and store data and have access to your customers' personally identifiable information (PII). Therefore, it's no surprise that you're a favorite target for malicious actors and one of their preferred dark arts attack vectors, ransomware.

**69%** **In fact, 69% of retail organizations were hit by ransomware in 2023.[1]**

**$2,458,481** **From a monetary perspective, retailers struck by ransomware are likely to pay a fortune, as the global mean ransom payment by retailers in 2023 was $2,458,481.[2]**

Like hexes, ransomware attacks can result in profoundly destructive and lingering consequences for C-Stores. The attack can result in reputational damage, loss of revenue from interrupted and suboptimal operations, potentially expensive compliance violations, detrimental strain upon relationships with vendors, suppliers, and partners, and even employee layoffs.

**37%** **It's reported that 37% of organizations were forced to eliminate jobs following a ransomware attack.[3]**

# Why C-Stores Are at Risk of Ransomware

## There are a myriad of reasons why C-Stores are susceptible to ransomware attacks, including:

1. C-Stores collect and transfer scores of PII and financial information, making them a treasure trove for malicious extraction and extortion.

**In 2022, a Pennsylvania-based convenience store chain was ordered to pay $8 million to settle a multi-state data breach that compromised 34 million payment cards used to buy food, gas, and other items. Stolen data included customers' card numbers, expiration dates, and cardholder names from transactions that took place between April 18 and Dec. 12, 2019.[4]**

2. A compromised digital ecosystem can provide hackers access to launch further attacks across an organization's network and potentially, even third-party partner systems.

3. C-Stores with on-site fuel and expanded food service offerings face unique security challenges compared to traditional retailers. The additional systems needed for fuel management, food delivery, inventory tracking, and more create a broader attack surface for hackers to exploit.

4. The emergence and proliferation of IoT devices, in-store applications, and digital signage throughout C-Stores create a larger attack surface.

5. Many C-Stores rely upon complex supply chains and just-in-time deliveries, which opens an ample array of auxiliary targets for attackers.

6. C-Stores are attractive targets for cyber criminals due to the sensitive information they handle within the forecourt and inside the store. C-Store POS systems handle vast amounts of customer data.

**In January 2023, researchers discovered an open dataset at an American C-Store chain with over 7,000 locations. The company's internal Azure blob storage was exposed to the public. It contained sensitive information, such as POS terminal transaction logs and tax, employee, and inventory data.[5]**

# Anatomy of a C-Store Ransomware Attack

1

## Payload

A C-Store employee opens a malicious link or email attachment, or is hit by a drive-by download from a compromised website.

2

## Execution

Malicious code executes and contacts a command-and-control server for instructions.

3

## Lateral Movement

The malware moves to steal credentials, escalate privileges, and establish persistence throughout the C-Store's network.

4

## Search

The attackers identify valuable files to encrypt (e.g., customer PII, shipping logistics).

5

## Encryption/Exfiltration

Attackers encrypt the C-Store's valuable files and may also keep a copy of the data.

6

## Demand

Payment demands are made by the attacker in order to provide the decryption key or prevent the release of stolen data.

# Protecting Your Data from Illicit Incantations


**To stymie the harmful consequences of ransomware, C-Stores can craft a protective shield to prevent attacks. Below are the steps C-Stores can follow to protect against ransomware:**

1) Establish and enforce robust security and protection policies
2) Build and maintain a consistent and secure network across all locations (including affiliated suppliers)
3) Fortify access control and management
4) Deploy an event visibility and monitoring system and perform constant analysis
5) Design and implement continuous cybersecurity education and training programs for staff

> *With SageNet we have a dedicated account team, with whom we're on a first name basis. We consider them an extension of our own team. For our 24-hour locations, knowing that our network is backed by SageNet's three 24/7 NOCs provides an extra level of peace of mind.*

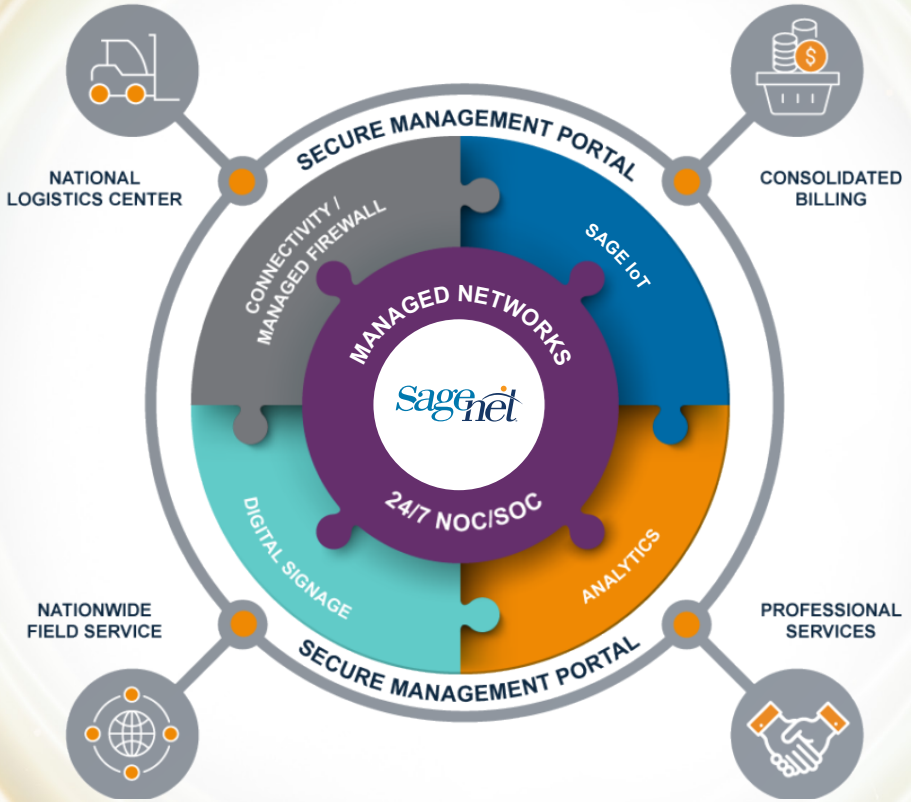
**GARY MCKEE** • Co-Owner • Pak-A-Sak

# SageNet: Demystify and Defeat Ransomware

To correctly and economically erect ransomware protection shields at scale, C-Stores need a seasoned network and security managed services provider. With more than 30 years of experience supporting some of America's leading retailers, SageNet has the technology, expertise, and support to build and secure modern networks, cloaking C-Stores in powerful ransomware protection.

From design to operations, SageNet delivers unparalleled managed networking services to C-Stores for store one to store 1,000 and beyond, protecting the entire supply chain and distribution network. SageNet's team of certified network engineers, digital experience leaders, and cybersecurity experts adeptly safeguards C-Stores' business and customer data from ransomware.

SageNet SageSECURE offers C-Stores a PCI-compliant, comprehensive managed services approach that follows a real-world proven way to connect, manage, and protect process. The SageSECURE platform delivers rapidly deployable, effective, and affordable connectivity, security, and digital signage solutions engineered specifically to protect the multi-site C-Store from ransomware and empower the launching of next-gen stores, applications, and services.



# SageNet and Fortinet: Power to Thwart Ransomware

SageNet builds its digital ransomware protection shields with the most comprehensive and effective security solutions on the market. SageNet's managed network services are bolstered by a long-standing, extensive partnership with industry leader Fortinet. Producing the world's most deployed network security solutions, Fortinet delivers AI-based security, performance, and actionable threat intelligence to thousands of customers around the globe, including leading C-Stores.

Wielding the power of Fortinet to thwart ransomware, SageNet keeps C-Store data in safe hands, as every SageNet-optimized network is backed by three US-based 24/7 NOCs, and a state-of-the-art, nationwide service and support organization. By choosing SageNet, C-Stores gain peace of mind that comes from having a single point of contact for everything from implementation and management to security, billing, and support.

# Set a Safe Environment with SageCONNECT™

SageCONNECT by SageNet enables the safe and high-performance networks that C-Stores need to win their customers' mind and wallet share. Using Fortinet FortiGate Next Generation Firewalls (NGFW) to thwart ransomware and other cyber threats to increasingly complex modern networks, many of the industry's leading C-Stores count on SageCONNECT for reliable, secure, and affordable connectivity.

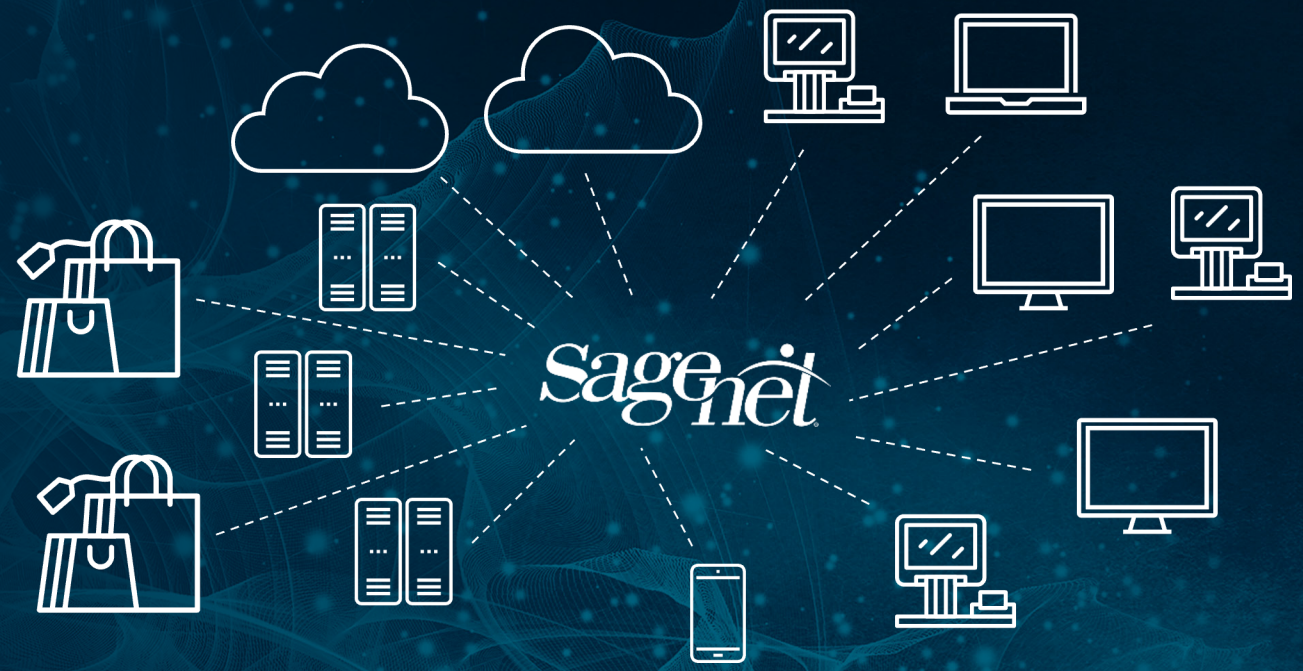
SageCONNECT ensures continuous connectivity that produces exceptional customer experiences and revenue generation. SageNet Wi-Fi enables C-Stores to display unique branding for customer engagement, and auto-back-up services such as 5G coverage ensures locations can continue selling when primary connectivity fails. Plus, SageNet satellite services provide emergency communications and disaster recovery to enable business continuity.

sageCONNECT™

# The Ultimate Ransomware Defense for C-Stores

To cast the widest range for an invisible, yet powerful ransomware protection barrier, C-Stores can adeptly prioritize and route their networking traffic with SD-WAN architecture. SageCONNECT is SageNet's Fortinet-based SD-WAN solution that delivers the network flexibility, efficiency, availability, and security that multi-site C-Stores require, along with 24/7/365 monitoring and support.

By leveraging the built-in SD-WAN capabilities provided by FortiGate NGFWs, SageCONNECT combines robust, high-availability networking with enterprise-class security to stop cyber threats. By offering automated path intelligence, tunnel bandwidth aggregation, and best-of-breed NGFW and unified threat management (UTM), SageCONNECT enables C-Stores to scale their operations with the confidence that their data, applications, and critical resources are well protected from ransomware.



sageSECURE™

## Enhance the Potency with SageSECURE™

SageNet's security team helps C-Stores increase visibility, detection, and response; achieve PCI 4.0 compliance to ensure continuous operations, protect critical data, and conduct employee training for ransomware prevention.

sageIoT™

## Ensure a Receptive Audience with SageIoT™

Leverage predictive analytics to better understand the C-Store audience with an IoT visibility platform that monitors activities and identifies issues, so SageNet can respond to optimize network performance with precision.

sageVIEW™

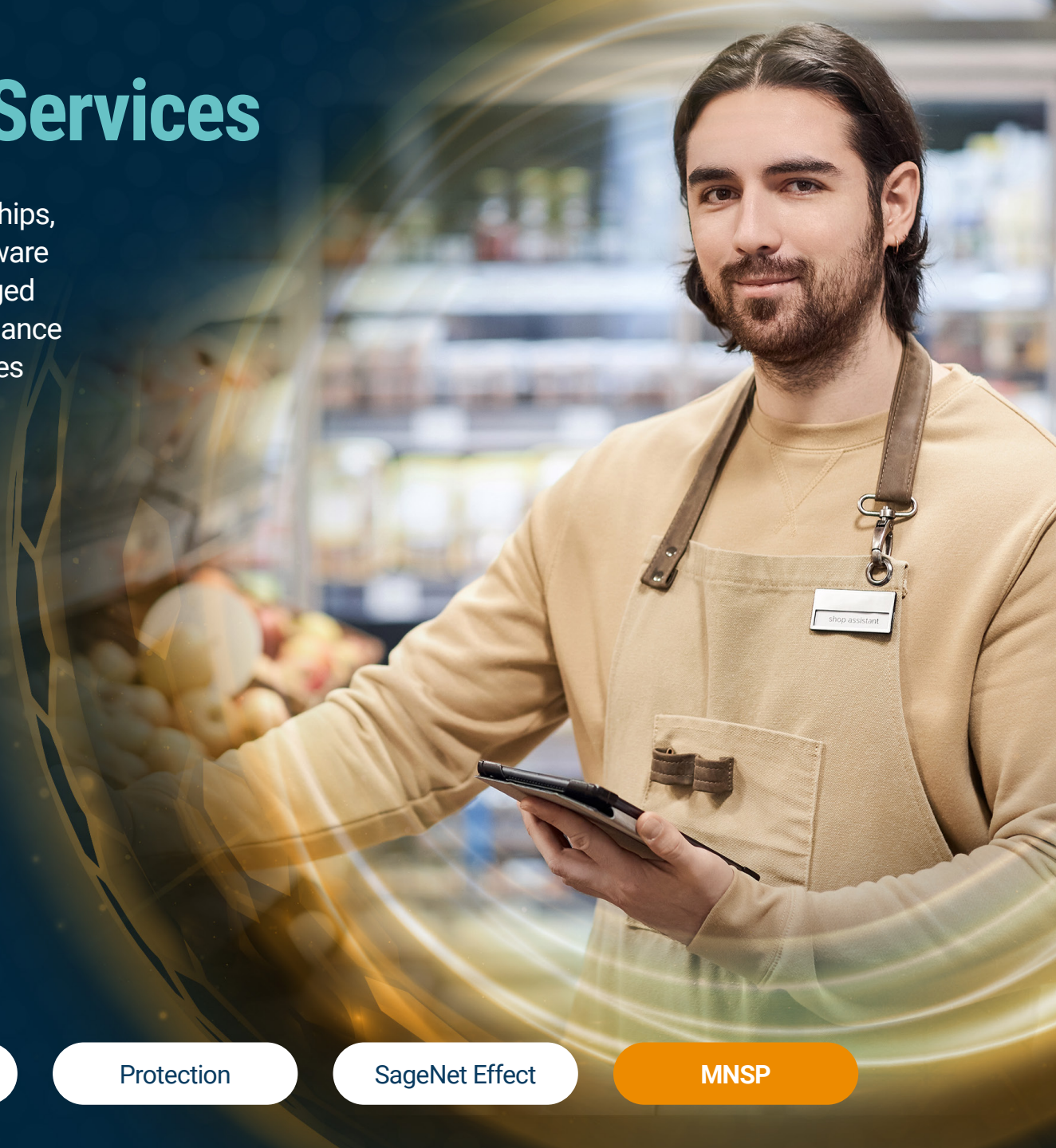
## Impact the Entire Crowd with SageVIEW™

Display safe and secure digital signage-as-a-service (DSaaS) to increase revenue, influence purchase decisions, and improve operational performance and efficiencies. Plus, SageNet Experience Labs will help design the most effective content for engagement and scale.

# SageNet Managed Network Services

Entrust SageNet's industry-leading managed services, extensive partnerships, and networking and cybersecurity expertise to craft the ultimate ransomware protection shield for your C-Store operation. With SageNet as your managed network services provider, you can improve operational performance, enhance customer experiences, and grow revenue, all while keeping your employees and customers safe from ransomware and other cyber threats.

## Contact SageNet today to counteract the ransomware hex or email us for more information.




**SOURCES:**

1) Sophos, The State of Ransomware in Retail 2023, July 2023.
2) Ibid.
3) Cybereason, Ransomware: The True Cost to Business 2022, June 2022.
4) Winsight Grocery Business, C-Store Chain Wawa to Pay $8M in Data Breach Settlement, July 2022.
5) Cybernews, Circle K US spills partial credit card details, among other sensitive data, February 2023.