IMAGINE THE IMPACT:
POS Ransomware = Devastating Business Loss

Netsurion™
Secure and Resilient Networks

EventTracker
Actionable Security Intelligence

"We are not far away from a major breach of a POS system that has nothing to do with stealing credit card data, but instead is intended to hold the business' ability to conduct transactions hostage for a large ransom. Stealing credit card data takes months, whereas ransomware takes minutes. It will not be long before cybercriminals utilize ransomware that freezes all of a business' POS systems, and the ransom will not be for the release of data, it will be for the ability to get back in business. Imagine the lost revenue for a major retailer if they needed to shut down all of their stores for a few days, or even a few hours, especially over the busy holiday season. It would be worth millions to have those systems unfrozen. The impact would be devastating. Just recently it was reported that a web hosting-company paid over one million dollars to get their data back…a million-dollar-plus ransomware demand from a retailer is not too far away."

– Kevin Watson, CEO, Netsurion

Point-of-sale (POS) malware continues to make headlines and inflict damage on brand reputation and profit margins alike. Cybercriminals can widely impact most or even all locations by exploiting the POS system itself. It's not much of a leap to go from POS malware stealing credit card data to POS ransomware holding a business hostage. The difference: Typical credit card malware must successfully persist on the target's network for months while it syphons off credit card data. A ransomware attack needs only minutes to execute its plan.

What would the victimized retailer be willing to pay to unlock their POS systems? If a brand was bleeding millions per day in actual revenue and potentially more in resulting data breach fines, brand reputation, and loss of customer loyalty, one could easily foresee the company being willing to pay a ransom of $2 million, which may be less than what they'd lose if they successfully restored operations on their own in just two or three days.

The solution is to go beyond bare-bones regulatory compliance-based security and begin implementing real security measures that predict, prevent, detect, and respond to advanced threats. This whitepaper delves into this topic more deeply, with solutions that vary depending on whether you are at the brand-level or a multi-location franchise business owner.

IMAGINE THE IMPACT:
A company is hit with ransomware every 40 seconds. (Kaspersky)

POS Ransomware...What This Could Mean

The motivation of most cyberattacks has been to steal credit card data that can be sold on the black market. Researchers estimate that U.S.-based credit card data can be sold by hackers for $5-$30 per card, depending on the data. Why so little? It's basically supply-and-demand fundamentals. As data breaches become more prevalent, the market for stolen credit cards gets flooded... there's too much supply, therefore it drives the price down. Also, stolen credit card data has a short shelf-life because of fraud detection and the consumer's ability to cancel the account.

Ransomware is the cybersecurity phenomenon that has been dominating headlines. It is a form of malware that encrypts data and demands a ransom payment, typically in Bitcoin cryptocurrency, to restore the victim's data and render their systems useful again. The next big cyberattack to terrorize the globe is not too far off. Remember the pandemonium that swept the globe as "WannaCry" ransomware propagated and infected more than 230,000 computers in over 150 countries within a day? Only to be followed shortly thereafter by "Petya" or "NotPetya", which infected computers in over 64 countries. In both attacks, victims included healthcare, telecom, and logistics companies. Both global attacks were based on a multi-vector ransomware variant known as "ransomworms". These variants are just as adept at spreading themselves to other unprotected systems as they are in locking up the host computer's files. Based on preliminary analysis, the Petya / NotPetya attack was particularly concerning because it acted as ransomware, locking up files, and stole the host user's credentials, thereby creating data breach and ransomware rolled into one.

It wasn't that long ago that a major retailer lost almost $20 million between fines, fees, lawsuits when they were breached during the 2013 holiday season. This impacted an estimated 40 million customers' credit cards plus another 70 million customers' personal data. Imagine the impact if a similar scope infection of nationwide POS systems occurred, only this time it was ransomware freezing an organization's ability to conduct business. The 2013 breach involved a major retailer that earned approximately $70 billion in revenue in 2016. Assuming half of its revenue was from online sales, it would still be left with approximately $35 billion in POS system-based sales, **or a loss of potentially $100 million per day.** Assuming the stores are open for 15 hours each day, **that's over $6 million per hour.** The question is, would they pay to have their POS systems turned back on, or would they be willing to have all their stores shut down for a few days while they reimaged every POS terminal? Keep in mind, this is simply lost business per day, we haven't scratched the surface of reputation damage, fees, lawsuits, and more. Imagine the real cost to any merchant or business.

It's a matter of time. The pay-out for stolen credit cards has dropped significantly and criminals are always looking for the biggest payout with the shortest amount of effort. If a next-level malware/ransomware breach occurs, freezing the POS devices themselves, it would offer immediate monetization for the bad guys, as the ransomware only has to persist for a minute, versus months for malware.

IMAGINE THE IMPACT:
1 in 5 businesses that paid the ransom never got their files back. (Kaspersky)

POS Systems Security

A POS system is the "center of the universe" for any business. It feeds sales information into revenue and accounting management systems, and often handles inventory control, purchasing, receiving, and

transferring of products to and from other locations. Other typical functions of a POS system are sales information, customer returns, reporting purposes, sales trends as well as cost, profit, and price analysis.

Customer information may be stored in a POS system for receivables management, marketing purposes, and specific buying analysis. Many retail POS systems include an accounting interface that feeds sales and cost-of-goods information to independent accounting applications. Given the importance of POS systems to retail operations, and the success hackers have had compromising them, the subject deserves special attention.

IMAGINE THE IMPACT:
72% of infected businesses lost access to data for 2 days or more. (Intermedia)

The Current State of the Consumer

Consumers need to feel confident in the brand, whether its global, national, or local. The best marketing is reputation and word-of-mouth. A wide variety of industries have fallen victim to data breaches in recent years, and retail and hospitality is no exception. According to the 2016 KPMG Consumer Loss Barometer report, 81 percent of consumers would feel uncomfortable shopping at a large retailer where their personal information has been compromised due to a hack, even if the security flaws were addressed soon thereafter. Of those that would return, only 48 percent said they'd come back immediately, and 68 percent said lack of a solid plan to prevent future attacks would deter them from shopping there ever again.

That loss of trust due to a breach at one or some of its stores adds up to real dollars in terms of lost revenue. For example, it is estimated that a large retailer lost $372 million in revenue in fiscal 2014 due to a loss in shopper confidence after about 56 million credit-card accounts and 53 million addresses were exposed in an April 2014 cyberattack.[1]

This loss of consumer trust not only impacts large brands—small "mom and pop" shops and franchisees with one to hundreds of stores are equally impacted. The difference is the scale of money and consumer impact, but these small businesses are not equipped to bounce back like the big guys. Frequently small- to mid-size businesses (SMBs) will be forced out of business after just one breach.

The Current State of a Franchisor or Corporation with Multiple Locations

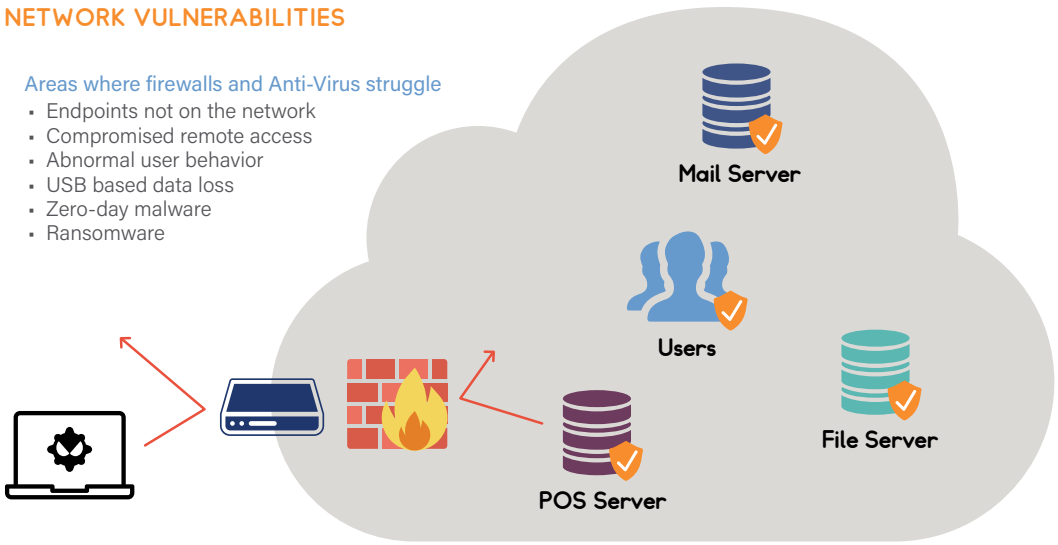
In their efforts to prevent data breaches, franchisors and brands face unique security challenges. First, like any enterprise, they must protect inside the corporate perimeter of their IT infrastructure and networks. The greater problem, however, is trying to deploy the same elevated level of cybersecurity measures at dispersed locations outside of that corporate perimeter. Typically, this includes a mix of corporate-owned stores, as well as independent franchise locations, which are not easily controlled, make their own decisions on security investments, and are more challenging to protect.

No matter what size of the business, it's rare to find a truly robust and large InfoSec team prepared to handle every endpoint security threat. The hard reality is that distributed, or frequently referred to as "edge"

[1]According to a 2016 Data Breach Impact Estimation report by the SANS Institute.

locations, are usually far too small to have the kind of dedicated cybersecurity expertise and teams that are available at the corporate level. The result is that these independently owned stores and franchise locations are often the weak link, a fact that is not lost on cybercriminals.

For most retailers, network security currently consists of a firewall and anti-virus ("AV") installed on each workstation and server, as depicted in the image below. Unfortunately, as cybercriminals have become more sophisticated in their attacks, these defense measures alone are not enough to protect the network. Specifically, firewalls and anti-virus software are vulnerable to compromised third-party remote access tools, zero-day malware, and abnormal user behavior, all of which have been seen before in major retail breaches. Further, since most ransomware is a form of a zero-day malware, firewalls and anti-virus software cannot prevent most ransomware attacks. To prevent these types of vulnerabilities, additional protection is required.



Staying Ahead of Threats

In the battle against cyberthreats, the best offense is a good defense. Cybercriminals give signals and leave tracks at every step as they progress through the retail hack chain. Capitalizing on this, there are techniques and technologies that can detect, block, and remediate hackers at every step. Foremost among these are:

- *Managed Next-Generation Firewall:* A network security system that provides a barrier between the trusted local area network and untrusted networks such as the internet. A firewall must be configured with rules that control incoming and outgoing network traffic, and ensure the entire infrastructure is protected. Most importantly, it must be managed 24/7 to be truly effective.

- *Security Information and Event Management (SIEM):* A software application, either in the cloud or on premises, that system gathers, correlates, and analyzes all data on the network in real time. A complex and powerful security tool, SIEM makes it possible to look at all the security information from a single point-of-view, filter out the noise (false positives), and spot trends and anomalies such as those typical of a cyberattack. Plus, present alerts for action.

- *Managed Detection and Response (MDR):* Applications that are designed to detect the activity of malware inside a network at the endpoint or workstation level. Endpoint-based threat detection helps to protect against advanced threats, especially previously unidentified malware and suspicious network

traffic. Unlike a firewall, that scans incoming and outgoing traffic, it focuses on malicious activity within the network or on a particular workstation to identify possible breaches in progress. Unlike anti-virus, MDR systems also contain a response component, allowing them to take some direct remediation steps to alleviate the threat.

- *Security Operations Center (SOC):* A centralized unit staffed by security analysts that deals with security issues on an organizational and technical level. Operating 24/7, the SOC provides the expertise and resources needed to continuously monitor, evaluate, and respond to all security alerts coming from the IT infrastructure.
- *User and Entity Behavior Analysis (UEBA):* UEBA is a type of machine learning model that uses advanced analysis, aggregates data from logs and reports, and looks at packet, flow, file and other types of information, as well as certain kinds of threat data to figure out whether certain kinds of activity and behavior are likely to constitute a cyberattack.

It is likely, that many previously breached organizations used these technologies to some degree. So why were they still breached? There are many possible explanations.

- *Vulnerable systems.* Most large-scale breaches occur through exploitation of a known vulnerability in an endpoint's operating system or a particular software application. Keeping all operating systems patched with the most recent versions would have mitigated many breaches. Unfortunately, not all legacy applications work with every newly released patch. This means that many IT teams are constantly testing new patching against all business-critical applications to ensure that a patch will not have an adverse effect. This necessary delay means that some systems will go months or even years with known vulnerabilities unpatched.
- *Improper configuration.* Firewalls, for example, are almost always deployed, even in home PCs and networks; however, firewalls are extremely complex to set up and use effectively. This is particularly true in the complex and highly distributed network environments. An improperly configured firewall, or gaps in its coverage, will leave networks and systems vulnerable to hackers.
- *Lack of expertise.* Properly implementing network and firewall security requires specialized expertise—and SIEM technology is even harder to use. In fact, industry analysts consider SIEM the most likely IT security tool to become "shelfware"—purchased, but not effectively deployed or used. Many organizations lack the expertise needed to properly use these tools, especially in remote locations.
- *Remote locations not protected.* One of the biggest reasons these breaches occur is that while these IT security technologies are used inside the corporate perimeter, they are not deployed or properly managed in remote or franchise locations.
- *Failure to control outgoing data.* Breaches can only be successful if the stolen data can be extracted or exfiltrated. Often firewall implementations focus exclusively on preventing malware from getting into the network, which is of course a primary function. But firewalls can also work in reverse, managing the outbound flow of data leaving the organization's network. Many implementations ignore the very effective practice of preventing data from going out of the organization to unknown destinations.
- *Lack of network segmentation.* POS systems and transaction processing networks are the center of the universe for retailers. Yet often these systems are not segmented or isolated on their own network from other systems in a store's location. Mixing POS traffic with general internet and business traffic makes it easier for hackers to get access to these critical systems.

- *Insufficient or ineffective endpoint threat detection and response.* Post-breach analysis shows the average breach is active for 265 days before detection. In many cases, the lack of breach detection allows hackers to collect sensitive data for a prolonged period of time.
- *Too much noise and too few resources.* In many cases, post-breach analysis shows there were indicators or alerts that an attack was underway, but these signals were missed. One reason is often that there are too few resources, but this problem is compounded by the lack of effective filtering of alerts. Security analysts are often overwhelmed by the volume of security alerts being generated, so the real threats are hidden by all the noise from false positives.
- *No SOC and very small InfoSec teams.* Many organizations, and especially remote locations, lack a 24/7 security operations center staffed by trained security analysts who continuously monitor alerts coming from IT security tools, and have the expertise to evaluate and identify serious threats and act urgently.

For remote locations, and franchise businesses, network security is a particular challenge. The threats in these environments are just as high as inside the perimeters of large enterprises, but the budgets and technical resources are a fraction the size.

IMAGINE THE IMPACT:
Global ransomware damages are predicted to exceed $5 billion in 2017. (Cybersecurity Ventures)

Imagine the Impact: Stop Threats in Real Time

An ounce of prevention is worth a pound of cure. Except in business, where an ounce of prevention can be worth several million dollars. The force of that logic has compelled enterprises and SMBs across industries, from retail and hospitality, to healthcare and finance, to invest significantly in cybersecurity. But as events have shown, those investments are not always effective. The secret is to invest strategically.

Drawing on years of experience and accomplishment in preventing data breaches across thousands of locations, Netsurion and EventTracker recommend these best practices as simple, reliable solutions to the large problem of implementing a holistic and effective retail cybersecurity strategy.

- Use a managed security services provider, backed up with 24/7 monitoring and an SOC, to add expertise and resources to your IT security teams.
- Standardize security measures across the corporate perimeter and ALL edge locations, and implement the same security measures you use inside your corporate perimeter.
- Segment network traffic and implement a managed firewall to protect both inbound and outbound traffic.
- Add a managed SIEM for your remote locations to provide early warning of cyberattacks. Inside your perimeter, consider a co-managed SIEM to provide the necessary expertise and resources to make the technology effective.

- Invest in managed detection and response (MDR) to monitor internal network traffic and shorten the active window of a breach and limit the damage. This can be done for a small incremental investment and provide tremendous peace of mind.
- Lock down your POS systems by segmenting these systems and limiting traffic to only known addresses.
- Consider Brand Guard security, a comprehensive program of managed services and technology implementation uniquely designed for multi-location brands and their franchisees.

Netsurion is a leading expert in managed network security, including enterprise-class firewalls, with a focus on protecting multi-location and franchise businesses from data breaches at affordable prices. Its latest innovations, powered by EventTracker, are SIEM-at-the-Edge, endpoint monitoring and file integrity monitoring (FIM), all designed to provide advanced security benefits to "edge" locations that normally would not have the means to leverage such a solution.

EventTracker, a subsidiary of Netsurion, provides advanced security solutions that protect enterprises from data breaches and insider fraud, and streamline regulatory compliance. EventTracker's platform comprises SIEM, vulnerability scanning, intrusion detection, behavior analytics, HoneyNet deception network and other defense-in-depth capabilities within a single management platform. The company complements its state-of-the-art technology with 24/7 managed services from its intelligence-driven security operations center (SOC), ensuring its customers achieve desired outcomes: safer networks, better endpoint security, earlier detection of intrusion, and relevant and specific threat intelligence.

Combined, Netsurion and EventTracker address every one of the pain points that have historically left retailers vulnerable to data breaches. In addition, Netsurion and EventTracker have countermeasures for every step of the hacker attack chain.

See Where You Stand: Get Your Free Assessment

Find out your risk level and revenue impact potential with our free online assessment tool: Netsurion.com/pos-ransomware or EventTracker.com/pos-ransomware. Get a custom risk report, along with tailored recommendations.

For more information about Netsurion's services, visit netsurion.com/contact-us

For more information about EventTracker's services, visit EventTracker.com/contact

Netsurion™
Secure and Resilient Networks

EventTracker
Actionable Security Intelligence