reliant

CONTENTS

Securing the Retail IoT

By Mark Weiner, *Co-Founder and Chief Operating Officer*

Often retailers implement expensive security controls without taking the time to understand what assets they are protecting or devising a strategy beforehand. These companies often exhaust their limited budgets deploying security devices with no control objective in mind.

As retail systems shift toward IP-connected Internet of Things (IoT) devices and the use of containers to process associated data, an entirely new security paradigm must now be considered. Given this, what exactly is it that we are trying to protect in the newly formed landscape of the retail IoT?

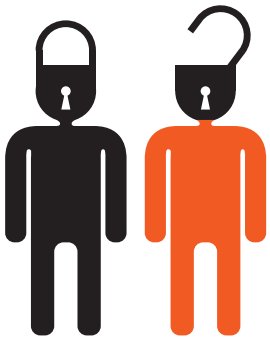
InfoSec academics tend to focus on the "CIA Triad" with CIA referring to "Confidentiality, Integrity, and Availability." In reality, the vast majority of security practitioners have focused only on Confidentiality, meaning that the defenses they design are focused on keeping privileged data private. The IoT changes things.

The most cited example of an IoT system compromise is Stuxnet[1], a malicious computer worm, first uncovered in 2010. Stuxnet targeted SCADA (Supervisory Control And Data Acquisition) systems and partially crippling Iran's nuclear program by damaging industrial centrifuge systems engaged in the enrichment of uranium. Stuxnet targeted Windows-based controllers designed to monitor and manage centrifuge systems, impacting the Integrity of the control process and ultimately the availability of the "dumb" centrifuge devices themselves.

While no one may know what future attacks on the retail IoT will look like, the Stuxnet episode provides a valuable clue. In protecting the retail IoT, Availability and Integrity will be as important as Confidentiality, which is a crucial component under PCI DSS (Payment Card Industry Data Security Standard) requirements.

This white paper examines features of the new retail IoT landscape and suggests control objectives that may be valuable to InfoSec practitioners in constructing defenses against malicious threats. We recommend edge computing not only as a mechanism for building the retail IoT but also as a means of protecting it.

[1] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html



61

percent of respondents had experienced an IoT-related security incident.

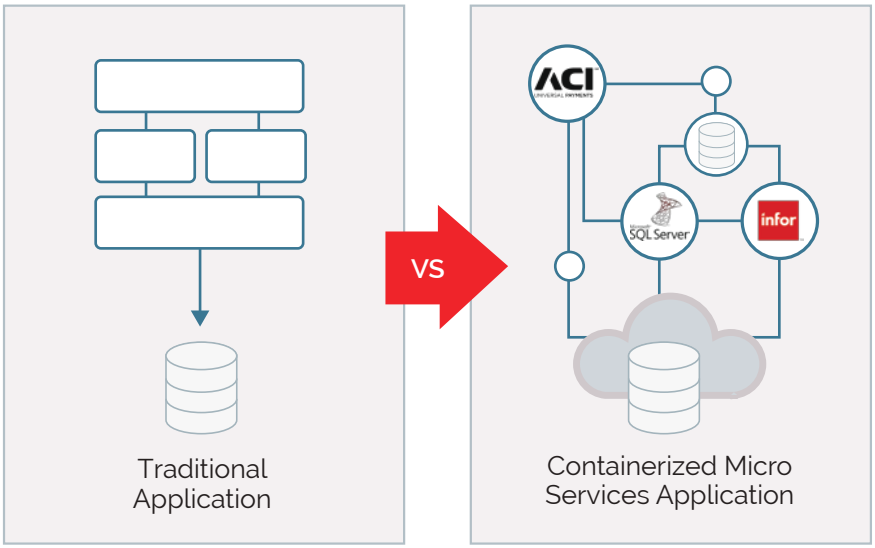
Retail IoT - Complexity as a Security Risk

According to a recent study[2] by Trustwave, they found that 61 percent of respondents had experienced an IoT-related security incident. With retail's push toward automation, personalization and digital shopping experiences, the number of IoT devices will continue to grow. Today's stores depend on these devices as new technologies and applications are brought online. Managing and securing all these systems will be a complex task and protecting all of the corporate data will become increasingly difficult.

Containers and AI:

Two groundbreaking technologies will reside at the foundation of the retail IoT: Containerization and Artificial Intelligence (AI).

Delivery of applications is increasingly done in containers. These are discrete units of application logic provisioned only with the minimum required components (libraries, configuration files, application binaries) necessary to perform their function within the application. Containers are lightweight, efficiently packaged, and offer a seamless way to manage and control a variety of micro-services. What makes containers unique from a security standpoint is their dynamic nature. Application updates are delivered in the form of new containers while old containers are destroyed in the process. The security program must adapt to the dynamic nature of ever-changing applications as well as the containers where they reside.



AI will be heavily utilized in retail automation including machine vision and machine learning applications. While the technology is just coming out of its infancy, it is increasingly clear that security professionals need to be aware of this trend and find new methods of securing autonomous systems. They'll need to build controls for systems that are capable of learning and making decisions based on data gathered from their environment. Unlike traditional

[2] Report: Internet of Things Cybersecurity Readiness, Trustwave & Osterman Research, 2018

Traditional botnets consist of large groups of malware-infected computers that are centrally controlled by a malicious actor to orchestrate distributed-denial-of-service (DDOS) attacks or flood email servers with spam messages.

IT applications, the behavior of such systems cannot be fully predicted, raising some uncomfortable questions. How do you protect devices and systems whose behavior can be unpredictable?

The impact of these technologies in the retail stack is not well understood. However, its vulnerabilities must at least be considered if necessary defenses are to be built.

Retail IoT Threats:

We can expect attacks on the retail IoT to be focused on disruption of the complex processes above in a manner that impacts the Availability and Integrity of the retail systems. For example, Stuxnet succeeded by targeting devices organized under SCADA controllers by making unauthorized changes to data parameters controlling device thresholds. This caused the operation of centrifuges to be well outside of their specified range and led to their failure.

Alternatively, retail IoT devices themselves can provide the source of an attack in the form of an IoT botnet. Traditional botnets consist of large groups of malware-infected computers that are centrally controlled by a malicious actor to orchestrate distributed-denial-of-service (DDOS) attacks or flood email servers with spam messages. As software designers and enterprises have improved their security, attackers have focused on the more weakly defended IoT devices to compromise and orchestrate IoT botnets. In 2016, the Mirai botnet consisting in large part of IP-connected cameras attacked gaming servers and later, the DNS infrastructure. This resulted in global internet outages and the prosecution of the Rutgers University students who created it[3].

The prior two examples offer a glimpse of what could come. Consider some other examples of simple attacks focused on disrupting the retail IoT and their aftermath:

- An IoT botnet consisting of devices on the retail LAN attack their store controller causing network disruptions.
- Addition of rogue IOT devices to networks - rogue sensor capturing customer information operates in ways that are either illegal, distasteful or both.
- Disrupting communication amongst IoT devices and their controllers - payment devices that can no longer communicate with the PoS and the bank.
- Changing IoT device configurations to make them function in undesirable ways - a restaurant temperature sensor whose calibration is reset such that it undercooks food.
- Alteration of an artificially intelligent system or device such that its learning function is impaired - an intelligent system may decide that customers are not to be helped and acts to dissuade purchasing in a store.
- Impacting the automation of such systems so that they do not function as desired - a kiosk or smart display designed for hyper-personalization that sends personally identifiable customer data back to the attacker.

[3] "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet," CSO Magazine, Josh Fruhlinge, March 9, 2018.

The central doctrine of InfoSec is "Defense In Depth" meaning that those controls are deployed in layers such that if a single control fails for any reason, others will be in place to offer needed protection.

As we have learned through past security breaches, malicious actors have the time and creativity to dream up new attacks to exploit any new wave of technology. We should assume that the emerging retail IoT will be no different.

Retail IoT Control Objectives:

Now that we understand the issues posed by unprotected retail IoT devices, we can enumerate a better list of the types of controls required to provide a layered defense. The central doctrine of InfoSec is "Defense In Depth"[4] meaning that those controls are deployed in layers such that if a single control fails for any reason, others will be in place to offer needed protection. In the emerging retail IoT, the control objectives will change, but the need for InfoSec professionals to ensure that the defensive measures align with the control objectives in a layered fashion will not.

Audit trails

At first glance, it might seem strange that the primary controls discussed are not preventative in nature. After all, audit trials only provide useful information after an issue has already occurred.

In very complex and mission-critical systems, logs are the raw material of recurrence prevention. Without them, unimaginable resources can be wasted in attempts to understand and recreate issues in a controlled environment. When critical systems fail, investigators will go to enormous lengths to retrieve logs. In airplane accidents, for example, investigators have been known to send submersibles miles deep in the ocean based merely on the possibility that the logs can be obtained.

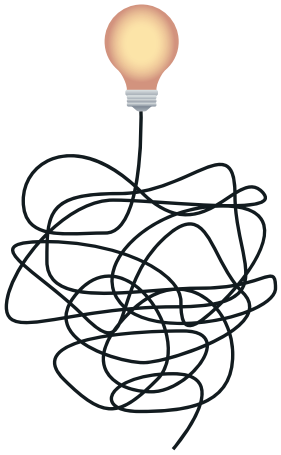
In the retail IoT, stores will cease to function under malicious or accidental technology failures. The ability and on-going review of logs across a variety of systems and devices provide the only cost-effective solution for prevention of future issues.

That is, of course, if you have devices that are capable of providing logs. Most devices, even relatively complex ones like payment terminals, currently do not have a means of providing logs. Similarly, logging standards for intelligent systems have yet to be fully defined which makes analysis, at best, a proprietary exercise. Finally, logs must be irrefutable. What that means is that they are collected at the edge and retained in the event upstream log servers cannot be contacted. For the retail IoT to be secure, the addition of a new generation of devices capable of generating time-synchronized logs must be addressed..

Network Security

In stores, network security is focused on the protection of Wide Area Networks (WAN) which is usually taken to mean implementation of firewalls and Virtual Private Networks (VPN). While these technologies will undoubtedly be critical for years to come, network security for the Retail IoT must also incorporate protections for devices and systems on the local area network. In a retail store with thousands of intelligent devices and applications delivered through ever-changing containers, controlling assets on the network and monitoring their traffic flows will become much more critical.

[4] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team, September 2016, US Department of Homeland Security



How do you go about managing all of this complexity in a way that adheres to security policies and is auditable?

Today, we have an independent category of device that provides Network Access Control (NAC). NAC typically recognizes devices by their unique MAC addresses and provides a mechanism to admit or reject them from the network. With containers, this becomes more complicated, because such systems often have virtual MAC addresses that can be changed like any other configuration parameters.

For a retail store with thousands of IoT devices, the problem of managing admission to the IoT network at scale becomes a data management problem. As new devices are admitted and containers are changed, an intelligent subsystem at the edge will be required to securely manage entry and exit of devices and systems.

System Policies

So how do you go about managing all of this complexity in a way that adheres to security policies and is auditable? First, we need to look at the size of the problem. Imagine a store's local area network with hundreds or thousands of containers or IoT devices. Many of these systems perform similar functions while others do not, meaning that management policies even within the walls of the store will differ depending on system function and OS type. This includes not only the applications, but parameters related to the container, OS, and networking configurations. It turns into a big problem very quickly. For a large retail operator with one thousand or more locations, you can take the magnitude of the problem and increase it by a factor of 1000.

While this is a very new problem encountered by only a few entities to date, we can look at similar examples to form some preliminary conclusions regarding how the problem might

The problem with patching IoT systems is that patches are frequently not available.

be solved. A comparable situation that we can turn to is the management of desktop computers in a secure enterprise like a bank or government agency. The various desktop systems encountered in such environments perform different functions and have different tolerances for risk. Some systems involved in administration may receive open internet access while those processing sensitive data may not. Group policies which enforce such standards are typically employed to support this level of standardization.

In the retail IoT, however, the problem is more multi-dimensional due to the need for mass standardization policies across systems and stores. Given the number of components, policies must be managed on a full-stack basis as they are applied across the network, system and application stack. As an example, firewall policies may need to be set at the system- or container- level and application configuration files must be managed as rigidly as OS components.

While solutions for network-level IoT security are new and evolving, the answer may lie in organizing systems and containers such that these components can be placed in a hierarchy where policies can be applied across physical and logical organizations.

Patching and Hardening

The problem with patching IoT systems is that patches are frequently not available. Device manufacturers are not generally focused on patches or hardening because their focus is in selling new devices[5] and not maintaining existing units in the field. Put differently, it is to their advantage that IoT devices be viewed as disposable. In the event a device is vulnerable, their strategy is that a customer should buy a new one.

In the rare cases when patches or hardening options are available, primitive or non-existent user interfaces often inhibit large-scale configuration or patch management. One enterprise recently discussed its efforts to patch 1.5 million IP-connected devices[5]. This effort took more than a year and led to a variety of unexpected problems including network congestion and developing tools capable of managing at scale.

If reliability requirements are to be met, retail IoT will need to address these issues of patch availability, hardened configuration and management at scale.

Access Control

Access control, incorporating Authorization, Authentication, and Auditing (AAA)[6] is an old standby for security professionals. Most would tell you that this area of security is extremely well understood and commonly implemented in most enterprise IT environment. The retail IoT adds several new dimensions of complexity to the challenge of meeting AAA goals.

[5] New Cybersecurity Report Warns CIOs -- 'If You're Breached Or Hacked, It's Your Own Fault', Forbes, Zak Doffman, May 2, 2019.

[6] https://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting

Authentication requests will rise as a result of adaptive behavior and may not follow a predictable pattern. Any failure of requests due to network connectivity will likely lead to system failures in the store.

First, and probably most notably, is that IoT devices can operate autonomously and may display behaviors akin to a "personality." The processes for authorization and authentication may be behaviorally based and have different methods. For example, authentication requests may happen at irregular times based on parameters of machine learning and evolving needs to access IoT services. Adding to this challenge is the fact that many current IoT devices and applications are known to be riddled with default credentials used for all types of application or system level access.[7] Furthermore, there is a current trend for such devices to use RESTful APIs when communicating with other systems or devices on the retail IoT. This means that not only the devices themselves but the messages they send to communicate with other connected systems must also be authenticated. All of this adds to the complexity. Remember, there can be hundreds or thousands of such devices on the retail IoT LAN, all building to potentially large volumes of authentication requests.

This poses a big challenge. Fortunately, traditional security offers ways to solve it. Authentication for an autonomous device is probably best implemented via certificates which combines the processes of AAA into a single cryptographic file. For this to work, certificates must be pushed down to IoT devices and systems and require a Public Key Infrastructure (PKI) to operate. Certificates must be created, securely deployed and destroyed upon expiration and this process needs to include the constant addition and retirement of devices and containers. That means that you'll need an AAA and certificate management infrastructure capable of managing potentially thousands of certificates and millions of authentication requests per day. Authentication requests will rise as a result of adaptive behavior and may not follow a predictable pattern. Any failure of requests due to network connectivity will likely lead to system failures in the store. While the retail world has not yet encountered this problem at scale, with the growth of IoT devices, it is only a matter of time before it needs to be addressed.

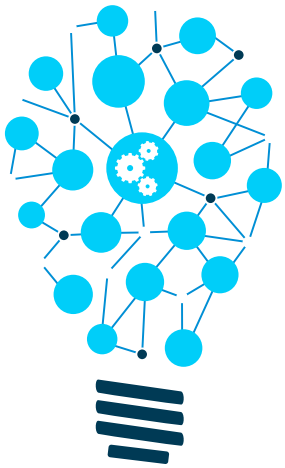
Physical Asset Management

The retail IoT will depend on devices operating in tandem with containerized systems to enable tightly controlled retail processes. Establishment of device inventories so that they can be secured and maintained in good working condition by location will be critical to the overall maintenance of the system.

Today, payment PIN pad inventories are managed in estate management applications by serial number, lane, and store. The good news is that these applications can generally support the management of the retail IoT device inventories as well. The bad news is that this does little to address the issue of device tampering which can happen either with criminal intent or through an act of vandalism. Physical device inspections with the purpose of uncovering damage or tampering will need to occur regularly. In parallel, store designers will need to enhance physical security features to limit non-staff access to IoT devices in the store. As in automated factories and enterprise data centers, rigid physical inspections of devices will likely become a new norm in retail.

[7] New IoT security rules: Stop using default passwords and allow software updates, Zdnet, Danny Palmer, March 7, 2018

[7]Enabling Microservices with Containers & Orchestration – Docker, Mesos, and Kubernetes Explained" (https://www.mongodb.com/containers-and-orchestration-explained).



Machine learning is used to establish a set of expected system-wide behaviors and send an alert when such expected behaviors are not observed in real time.

Behavioral Monitoring

With the retail landscape shifting rapidly to hyper-personalization & automation, a malfunction by one of the retail IoT components can cause business operations to cease. This is a new type of security risk directly tied to Availability and Integrity. For example, all physical components of a robotic inventory restocking system may appear to be functioning without issue. If the overall system ceases to operate properly, however the business is just as impacted as if there were an easily identified component failure.

To address this risk, a new type of system-wide monitoring is required. This level of oversight will be built on event correlation and heuristics.

Per the discussion regarding audit trails, log messages provide the raw material for event correlation. In our robotic inventory management system example, a log entry showing an application level decision to restock a shelf correlated with a lack of response to robotically add inventory after one hour would create an alert to check the system. As the complexity of the retail IoT increases, such event correlations could become very complex ultimately encompassing analysis of multiple events and timing thresholds in a series of nested & conditional formulas.

Heuristics effectively involves machine learning to establish a set of expected system-wide behaviors and send an alert when such expected behaviors are not observed in real time. In our robotic inventory management, example above, a heuristic solution might "learn" that inventory needs to be replenished after a camera observes ten customers stopping by a shelf without selecting an item. In security, heuristics have been used extensively in anti-malware solutions. For the retail IoT, we anticipate dedicated applications running in containers receiving real-time inputs and reviewing log files to provide this function.

Security Testing

When viewed in the context of categories, testing controls in retail IoT should not differ much from other IP-connected systems. Procedures for network scans, integrity checks, and penetration tests are not expected to change. The scale of testing is what changes. Testing of security controls tends to be bandwidth intensive. For example, vulnerability scans run across a WAN will often need many hours to test just a few Windows POS systems in a store. Imagine the challenge of running such tests against thousands of IP-connected devices. In such scenarios, scans would need to run for days. This is simply not possible without impacting business operations.

Consequently, systems that conduct security testing will themselves need to be containerized and pushed to the edge. Test results (for example, Vulnerability Scan Results) also must be packaged and sent back up to the cloud. Once in the cloud, analysis using automated tools will parse through volumes of test data to get past false positives and other anomalies.

Finally, security testing in the retail IoT will require orchestration of tests across store locations as "jobs," and these will provide feedback on the success or failure of device tests. As a simple example, if we reserve an overnight window for network scans, that window is likely different for eastern US vs. western US stores. Similarly, if scans fail for any reason, operators need to be informed that these tests were not completed so they can schedule windows for retesting. Note that orchestration will be necessary across control groups including data leakage testing, penetration testing, and IoT system integrity checks.

Conclusion: A New Approach is Required

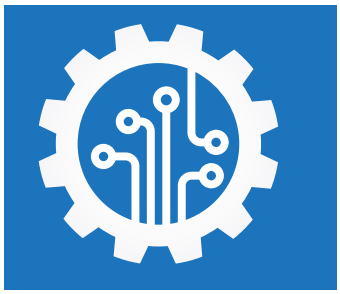
In the new technology-laden retail environment, failures of security carry not only liability but could result in stores being simply unable to conduct business at all. While it is still early in the retail IoT technology lifecycle, current approaches to implementing security controls may not be adequate to address the scale or complexities posed by the retail IoT.

While Reliant believes the doctrine of Defense-in-Depth will continue, the control objectives implemented will shift from Confidentiality to Integrity and Availability. This shift, combined with the scale of the retail IoT environment, requires a new approach to security. This approach must incorporate requirements to:

1. Organize massive inventories of IoT devices and containers across store locations
2. Automate the operation of controls and the analysis of security data
3. Adapt controls to address unique elements that will arise across store environments

[8] https://www.zdnet.com/article/devsecops-what-it-is-and-how-it-can-help-you-innovate-in-cybersecurity/

[9] DevSecOps: How to Deliver Security at DevOps Speed, eWeek, Sean Michael Kerner, March 08, 2019



Controls will need to be built into systems, containers, and devices.

Risks associated with the retail IoT are born out of its complexity and the sheer volume of systems and devices that that must be supported. Some new controls will be required in the retail environment to address this including Behavioral Monitoring and Physical Asset Management. Controls such as engines for Audit Trails, Security Testing, and Access Controls will have significantly expanded roles and will likely need to run as containers on edge devices. Finally, others like Network Security and management of System Policies will need to be reimagined entirely. In defending the retail IoT, security practitioners will need to organize devices, systems, and controls into groups so that security policies can be created and enforced.

Furthermore, the scale of the retail IoT will require more than improved organization of systems into groups where policies can be enabled. Controls will need to be built into systems, containers, and devices. These controls, by extension, will be automated in both their execution and in the collection of data demonstrating their effectiveness. In cloud-based systems, an entirely new field called "DevSecOps,"[8] was recently born. Under DevSecOps, "part of the product deliverable is provisioning secure development environments for developers that are already integrated with single sign-on, hardened operating systems, proper network controls, and enterprise security policies." [9] While not a prescriptive approach, DevSecOps leverages many of the same concepts previously discussed including containerization, automation, and orchestration. The concepts of DevSecOps will play an essential role in creating an agile control environment for retail IoT.

Finally, a new approach to the well-used and proven methodology of defense in depth should be considered. The doctrine of defense in depth has been interpreted as constructing fixed fortifications around critical IT assets in much the way that medieval kings built castles to protect themselves. Just as castles had a system of physical barriers, traditional approaches to protection of IT assets call for a broad set of preventative controls such as firewalls, access controls and logging to protect critical assets. Given the complexity and variance of system behaviors that will be encountered, a more agile approach to defense in depth is required. This approach requires an agile infrastructure that will allow retailers to rapidly place the right controls in the right place, all based the nature of the assets to be defended and the magnitude of the threat. For example, computationally expensive controls like Data Loss Prevention may be placed in a set of stores for a period of time and removed after testing requirements have been met.

[8] https://www.zdnet.com/article/devsecops-what-it-is-and-how-it-can-help-you-innovate-in-cybersecurity/

[9] DevSecOps: How to Deliver Security at DevOps Speed, eWeek, Sean Michael Kerner, March 08, 2019

Reliant Edge Platform and Securing Retail IoT:

Based on the control requirements above, securing the retail IoT will be an exercise in policy management, orchestration, automation, and containerization within retail environments. These components are supported extensively with Reliant Edge Platform including:

Audit Trails & Behavioral Monitoring

Logging infrastructure including LAN-based storage and secure log transport to a centralized search engine is an integral part of Reliant Platform. Messages of all types, ranging from simple authentication requests to vulnerability scan results are transported and indexed for searchability and correlation.

Embedded Network Security Controls

Reliant Platform supports network security features such as a flexible firewall, proxy, and VPNs. These controls are centrally configured and managed through Reliant Platform Manager to control security on the retail LAN.

Automated enforcement of System Policies

Reliant Platform provides a feature set for hierarchical policy management of systems, devices, and containers by location or system type. This flexible approach allows for management of system policies at web scale.

Patching and Hardening

Package management, including automated distribution of packages to Reliant's in-store appliances and the ability to orchestrate deployment of patches and configuration updates is also part of the platform. The deployment of container and IoT updates is greatly simplified under Reliant Platform Manager, our cloud-based management interface. Orchestration tools enable additional flexibility for more complex deployment tasks.

Access Controls

Role-Based Access Controls are implemented across the platform and include strong passwords supplemented by multi-factor authentication. This infrastructure is also centralized for improved access management.

Inventory Management

Reliant Platform maintains extensive features to manage device inventories according to levels of hierarchies which allows flexible extraction and storage of device metadata, as well as secure package management for patch updates.

Security Testing including extrusion detection and network-based vulnerability scanning

Infrastructure for security testing is built in. This includes a container-based network vulnerability scanning engine and mechanisms for network access control and data extrusion detection. Orchestration of these controls is supported to enable flexible testing of individual stores or groups.

Reliant is an edge computing company providing retail and hospitality operators with a single platform technology solution that bridges the gap between the store and the cloud.

About Reliant:

Reliant is an edge computing company providing retail and hospitality operators with a single platform technology solution that bridges the gap between the store and the cloud. By converging new and legacy systems into an integrated, scalable system through virtualization, centralized management, and comprehensive application monitoring, Reliant offers retail and hospitality chains a simpler and more effective way to deploy and manage applications, networks, and security controls at the store or restaurant.

Years of experience and customer engagement on the front lines of retail automation has given Reliant a unique lens for discussing the accumulated set of frameworks, best practices, and technologies that comprise today's complex world of retail infrastructure and automation. Over the past decade, the company has steadily aligned and integrated its patented cloud platform with core technologies and best practices that comprise the world of infrastructure management, DevOps, and application automation.

Author Information

Mark Weiner (CISSP, QIR, QSA) has worked with several retailers, payment processors and card brands in support of their PCI compliance need and has been a featured speaker at National Retail Federation and PCI Standards Council events. Mark has over 20 years of experience in Information Technology including a variety of executive roles in sales, professional services, product development and operations. He was an early pioneer in driving practical, cost-effective implementations of security policy and compliance requirements. An engineer by trade, Mark has BS and MS degrees in electrical engineering. Mark also earned an MBA from Columbia University's Graduate School of Business.