NOZOMI NETWORKS

SOLUTION BRIEF

Cybersecurity is Increasingly Important to Retail Strategy

The retail industry knows that IoT vulnerability management is beyond transaction and inventory system security, because trust is inextricably linked to brand equity

Retail is a B2C relationship where customers and business owners recognize that trust is a critical element of engagement. The inextricable link between trust and brand equity means that value can be rapidly eviscerated if trust is lost. Therefore, it follows that protecting the entire customer relationship from engagement, transaction, and fulfillment through to the retail setting is of the utmost importance.

"Our corporate IT department had zero visibility into devices that were connected to our network not even considering devices connected either intermittently or one time only. Nozomi Networks helped up to see what we had no idea we were missing."

Chief Operating Office, A Global Retailer in Home Related Supplies ›

“Recognizing the impact that a major cybersecurity event could have on our reputation, we cannot afford to continue operating as though an event were unlikely to happen to us. It just wasn’t feasible to continue that way.”

Executive, Risk Management ›

IoT has widespread deployment in retail organizations. One of the most recognizable systems is the Point Of Sale (POS) network for payment processing. It is an essential tool in the retail environment. POS systems have changed over time and include many variations including self-service kiosks and alternate payment method systems such as contactless payment.

In addition, other programs intended to create customer stickiness (such as customer rewards programs, warranty tracking and access to instant credit approval networks) expand risk profile and the opportunity for bad actors to insert themselves.

To protect overall customer experience and programs, security needs to be top of mind in the context of current day threats. Customer-centric applications and tools which protect both the business and the consumer should be in the purview of the security office of the retail owner, be it an SMB or multi-regional corporation.

It is as important to build customer loyalty and nurture the relationship as it is to protect the trust that surrounds the engagement from beginning to end. Cybersecurity is the new facet that impacts customer experience.

The Retailer's IoT Security Challenges

Retailers are not immune to security challenges faced by many industries today. In fact, the cost to a retailer affected by a cyberattack can be just as significant and lost lasting as the impact on any manufacturing or energy company. The most frequently noticed systems in the retail environment include those which process and store customer transactions. These include:

Point of sale and various processing platforms from credit cards to alternative payment services

Customer contact databases store shipping addresses, store location information and major purchase data

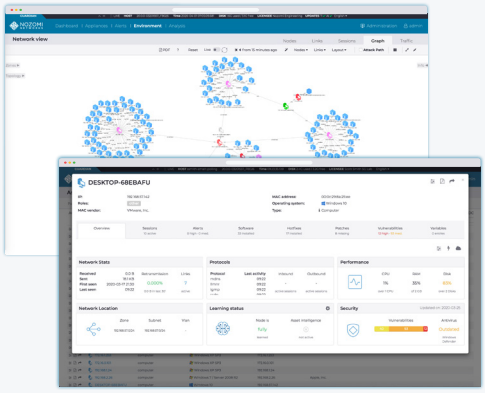
Customer loyalty programs where information is stored in an online customer database

Transaction-centric databases may store customer contact information to be collected for shipment, warranty and recall information

Often, the mode of an experienced cyber hacker is not to enter through the front door. Attackers will seek any avenue from which they can exploit information required to leverage an attack. The back-office and adjacent systems represent opportunities for an experienced hacker seeking to elicit a chaotic and unprepared response. Entry may be gained through:

- Transportation networks
- Closed circuit TV (CCTV)
- Building Automation Systems (BAS)
- Physical intrusion detection systems
- Heating, ventilation and air conditioning (HVAC)
- Fire alarm protection systems

With the proliferation of intermodal transportation and in-building tracking networks connected to online tracking applications, the cyber attack surface surrounding the retail environment is much larger than it has ever been in the past.



Site Discovery in the Retail Industry

When connecting to a new site, the Nozomi Networks **Guardian** observes, captures, and analyzes traffic to compile a profile of network activity. Typical site survey findings in retail environments reveal a mix of anticipated and unexpected connections:

- Security cameras, CCTV
- HVAC with WiFi enabled controls
- Refrigeration / cold chain monitoring
- POS devices
- Rogue device connections
- Personal shopping network equipment
- Smart inventory or shelving equipment

Once captured, Nozomi Networks solutions process the device findings to augment equipment details with information from **Asset Intelligence**.

This data can then be further enriched with the latest threat intelligence. The **Threat Intelligence** subscription serves both to highlight configuration weaknesses and to identify risky equipment that could jeopardize network security.

How Does Nozomi Networks Enable Retailers to Secure Customer Trust?

Nozomi Networks delivers cybersecurity and analytics for IoT-based processes. With a zero-trust approach to network visibility and security for industrial digitization, we provide real-time integration of security and asset intelligence that is purpose-built for enabling reliable operations.

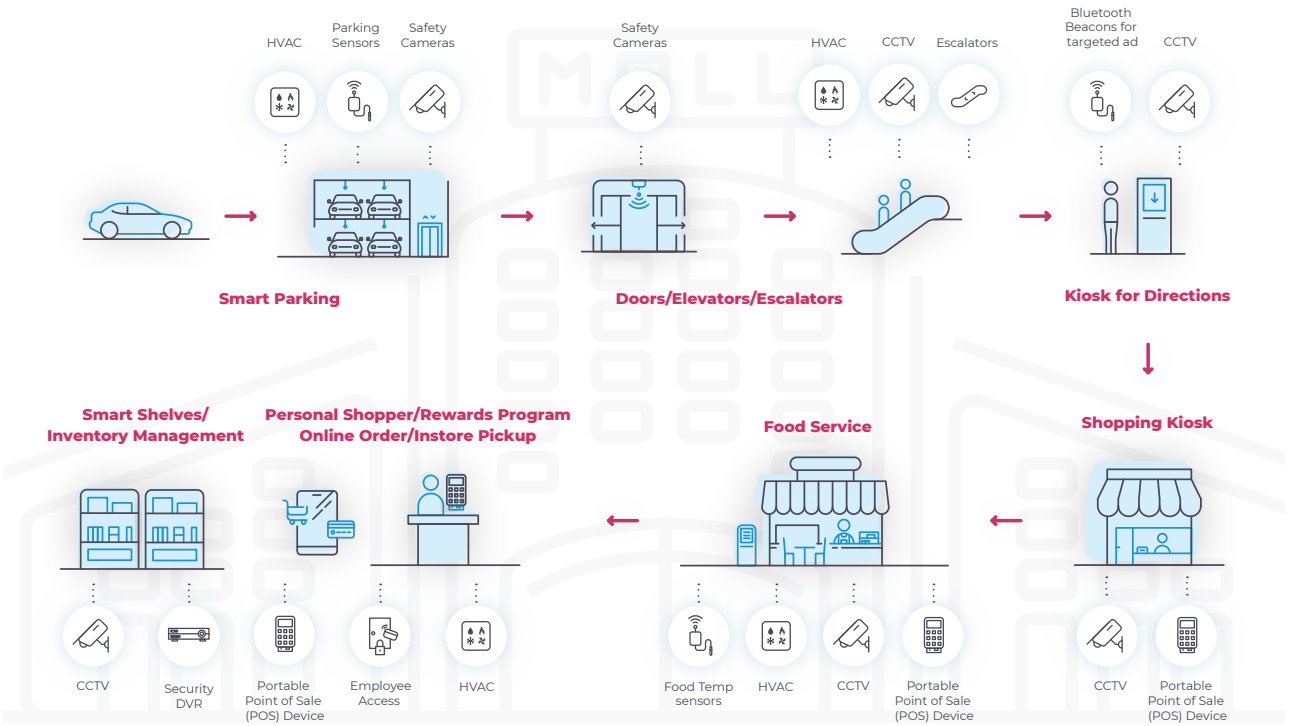
The Nozomi Networks solution detects and secures critical customer data in a landscape of the growing number of devices, increasing amount of data, and rapidly evolving network vulnerabilities and threats to infrastructure across the retailer environment of networked organizations.

With the Nozomi Networks solutions, you can:

- Automate the analysis of IoT devices and network traffic
- Maintain visibility of all network assets
- Capture device behaviors from the warehouse to the retail site
- Profile behaviors of connected devices
- Leverage data and process knowledge to anticipate process issues
- Predict maintenance requirements and diagnose problems
- Quickly identify potential threats

The Nozomi Networks solution bridges the full life cycle of IoT vulnerability management, threat detection, diagnosis, and remediation to ensure you are addressing risks in real-time. Our platforms connect onsite systems to globally available and secure dashboards so that corporate governance has as much insight into the overall state of cybersecurity as each retail site.

Working with Nozomi Networks, customers experience the deepest insight into the widest range of IoT devices and processes to deliver actionable intelligence when and where you need it.



The retail environment has multiple connected networks including those on and offsite to the retail location. With the right solutions and processes, you can protect against any of the many types of cyber threats.

The Nozomi Networks Solution in Detail

The Nozomi Networks solution provides a variety of features that can be readily integrated into current onsite processes. The net effect of raising a security profile, across regions and globally, effectively secures the blanket of customer protection. The efficacy of the solution can be readily demonstrated, and it is best exemplified by a sensor network from which to oversee all traffic.

An enduring process capable of detecting threats and providing response ability to retail management is the best means of closing the cybersecurity gaps present in most retail locations and enterprises.

The Nozomi Networks solution enables retail organizations to:

Anticipate

Detect potential issues in your IoT networks by analyzing device inventory and vulnerabilities, changes in process variables, or network traffic. Address issues before they can be exploited or disrupt operations.

Diagnose

Understand where threats may be coming from, or when maintenance may be required. Quickly identify root cause issues, and direct where remediation efforts where needed.

Respond

Manage response with guided playbooks that can coordinate and track specific remediation efforts based on the problem type. Get help in prioritizing risk reduction efforts through process adopted use of asset intelligence and operational awareness.

The critical onsite component of a secure cybersecurity solution for retailers

Guardian™ - Containerized sensors for standard and ruggedized installations.

Smart Polling™ - A Guardian-based application that delivers active asset status updates, vulnerability assessments, and security monitoring.

Subscription and SaaS services connect to Guardian to enrich and protect the information that is part of a retailer's cybersecure network

Vantage™ - A SaaS-based centralized management console to aggregate all collected data from a local, regional, or global network of sites.

Asset and Threat Intelligence™ - Subscription services to deliver timely manufacturer device information, and the latest cybersecurity intelligence to identify threats and vulnerabilities identified from across industries.

Anomaly Detection - An application or service which establishes a baseline of network behaviors to quickly recognize unusual and atypical device. connections and communications

Products and Services

SAAS

Vantage

Vantage accelerates security response with unmatched threat detection and visibility across your OT, IoT and IT networks. Its scalable SaaS platform enables you to protect any number of assets, anywhere. You can respond faster and more effectively to cyber threats, ensuring operational resilience.

Requires Guardian sensors.

EDGE OR PUBLIC CLOUD

Guardian

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single application. Guardian shares data with both Vantage and the CMC.

SUBSCRIPTION

Asset Intelligence

The Asset Intelligence service delivers regular profile updates for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-respond (MTTR).

SUBSCRIPTION

Threat Intelligence

The Threat Intelligence service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of emerging threats and new vulnerabilities, and reduce your mean-time-to-detect (MTTD).

GUARDIAN ADD-ON

Smart Polling

Smart Polling adds discreet active polling to Guardian's passive asset discovery, enhancing your asset tracking, vulnerability assessment and security monitoring.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

SB-RETAIL-8.5x11-001

nozominetworks.com