opentext™

Improving security with dynamic zero trust in Retail

Adopting modern defenses to keep pace with growing threats

> **"Two out of three retailers report being attacked by ransomware in 2022."**
>
> Sophos, The State of Ransomware in Retail. (2022)

The retail industry is changing at a rapid rate. Supply chain disruptions, technology innovations, and a need to engage with customers have all led to significant business model changes. The retail store has morphed and evolved into an entire set of omnichannel experiences.

Retail organizations must now connect customers with data from their suppliers. Employees must now be allowed to access a broad range of information resources to resolve customer issues. Increasingly, companies are leveraging partners and managed service suppliers to fill in gaps in their capability to deliver end-to-end omnichannel customer experiences.

In this environment, security becomes much more challenging. Organizations can no longer hide behind a hardened perimeter, but instead need to consider approaches that support appropriate information sharing across multiple platforms while ensuring robust security.

Rising cyber risk

Preventing ransomware, malware, fraud, and theft is increasingly important, as cyber threats facing the Retail industry grow in number and sophistication. Traditional perimeter-based security measures are no longer sufficient, as retail businesses often have numerous endpoints, both in physical stores and online, making them vulnerable to a wide range of attacks.

This paper discusses how, by taking a holistic approach to cybersecurity and leveraging a zero trust model, retailers can bolster defenses and more effectively address internal and external risks.

A zero trust model works on the assumption that no entity, inside or outside the organization, should be trusted by default. It enforces strict access controls and continuous authentication for users, devices, and applications. That way, even if a threat actor gains initial access, they still must be authenticated and authorized for each specific action or resource. This provides extra defense against unauthorized access and lateral network movement.

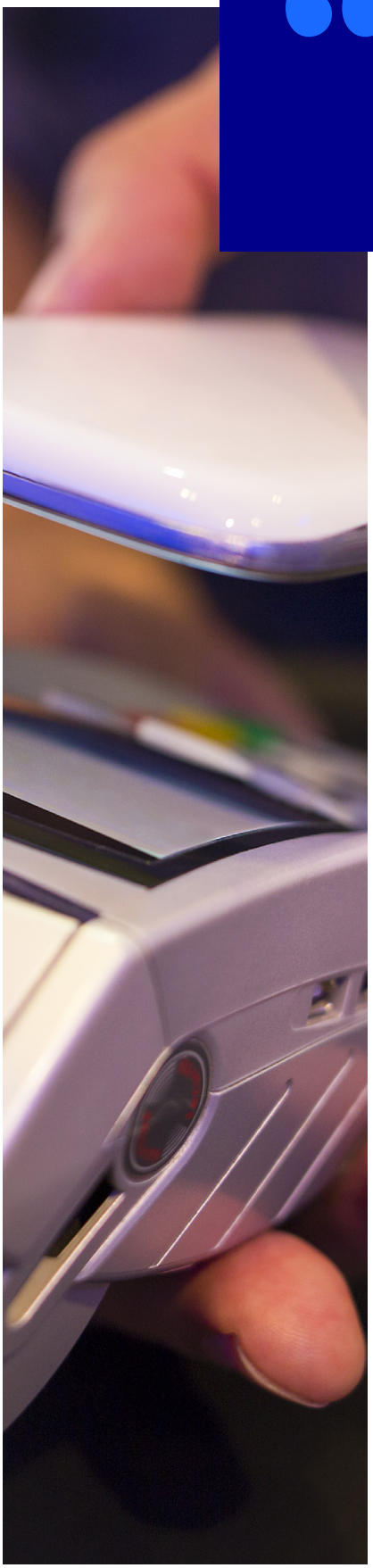
Increasing regulatory obligations

As more customer data is collected, stored, and processed by Retail companies, the need for strong data protection and compliance with regulations like GDPR and CCPA is paramount. By segmenting sensitive data, a zero trust approach can ensure that only authorized personnel can access it while monitoring and logging all data interactions. Retail companies can better safeguard customer data, protect the brand and maintain trust, boosting customer loyalty and stakeholder confidence.

The move to zero trust

Most retail organizations still use firewalls as a first line of defense, however changes in where services are located, who controls them, and how they are used are challenging that paradigm. The move to cloud-based services has created a move toward IT practices that create layers of security protection for sensitive and regulated data, but the need to safeguard is only growing.

Zero trust's initial focus was to apply tighter controls for each network segment and resource endpoints—equivalent to putting a security guard at every office door, hallway, and elevator. It has since evolved beyond these origins, moving up the stack to the services and applications layer. Today, IT can use zero trust methodologies to control responses to access of their protected resources directly.



> **"Zero Trust is an important strategy for implementing security required to enable commerce, which has an overall effect of boosting trust between businesses and their customers."**
>
> IDC, Future Enterprise Resiliency and Spending Survey. (2021)

Many retailers are surprised to learn that a zero trust environment isn't more complicated or costly than what most organizations already have. Often savings and simplicity are achieved by consolidating multiple disconnected technologies and leaving behind expensive legacy technologies to move to a simpler solution with significantly lower overhead.

Embracing a holistic security approach

Traditional security sees devices and applications within the network perimeter as trusted, as they are behind the protection of perimeter defenses. However, that approach does not work well in the cloud, where there is no perimeter to defend.

Zero trust assumes that every device and account could be malicious, regardless of whether it is located inside or outside the network perimeter. All devices, accounts, applications, and connections are subject to robust authentication checks and comprehensive security monitoring.

Fundamental to zero trust is the principle of least privilege. Give anyone who uses the network (employees, partners, contractors, etc.) access only to the tools they need to do their work—nothing more, nothing less. This provides the strongest possible defense, ensuring all identities are validated, and that access is managed dynamically. It centralizes policy management and automates enforcement, closing security gaps and making compliance and auditing much easier.

By embracing a zero trust architecture, retailers can gain the following security advantages:

- **Protection for hybrid and cloud-first environments**
  Zero trust goes beyond the network perimeter, with policies determining what identities can and can't do in every environment.
- **Privileged access management**
  Extra protection for accounts with access to the "keys of the kingdom," which are major targets for cyber thieves.
- **Protection from insider threats**
  With insider threats becoming more frequent and costly, more than half of which are caused by negligence,[1] zero trust approaches need to be dynamic and mature.
- **Reduce third-party vulnerabilities**
  A framework to minimize third-party risk across all network access.
- **Continuous identify verification**
  Ensure access isn't possible unless explicitly granted, and any access granted is continually monitored, reducing risk and increasing visibility.

1 Ponemon Institute, Cost of Insider Threats Global Report. (2022)

- **Understand identities**
  Zero trust recognizes patterns and distinguishes real threats from noise, resulting in faster detection and fewer false alarms.
- **Complete visibility and control**
  View and manage the organization's risk profile through a single pane of glass, tweaking policies for any group, with changes automatically synchronized and enforced.

Maximizing the user and customer experience

A zero trust architecture (ZTA) can significantly improve the customer experience in retail by enhancing security, increasing trust, and streamlining operations. Customers can trust their sensitive information is being handled with the utmost care and retailers can facilitate more personalized experiences, leveraging data to recognize customers, remember preferences, and provide tailored recommendations and offers.

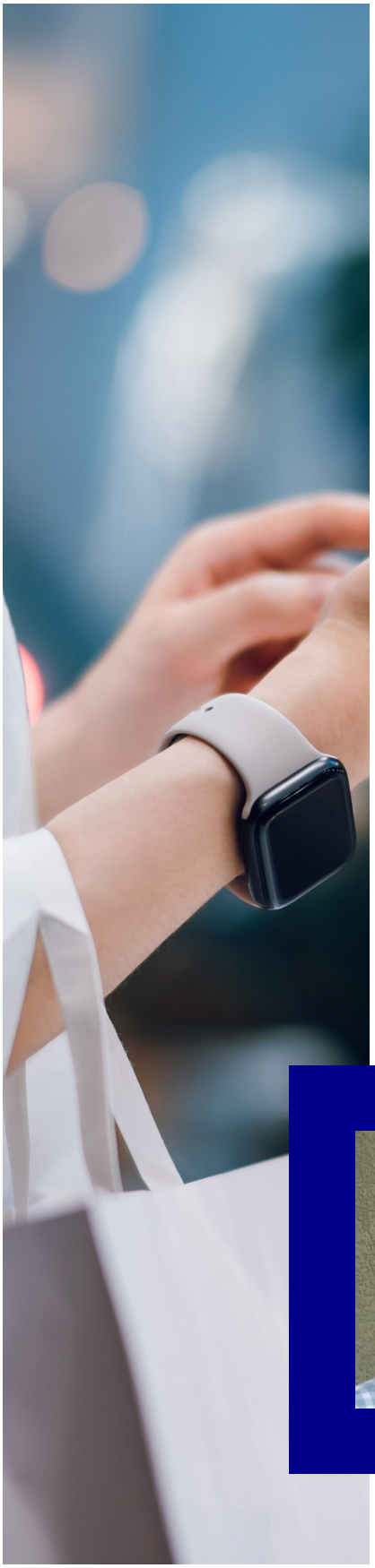
Zero trust helps maximize the user experience while minimizing retailers' security exposures by enabling:

- Support for various authentication methods with the flexibility to choose biometric, voice, or geolocation options.
- New applications and systems to be recognized and analyzed to help determine risk scenarios and levels.
- Controls, such as risk-based authentication and re-authentication requirements, to show that the system is looking out for the best interests of the consumer.
- Self-service password resets to drive efficiency with users and help desk.
- Visibility and oversight to allow for immediate control or prompt response to threat scenarios.

Why OpenText

As security becomes more challenging and cyber threats multiply in the age of the cloud, companies are employing carefully crafted security policies to protect themselves. However, the truth is that no policy can properly protect an organization unless it is well managed and consistently enforced. Traditional security approaches fall short in today's environment of distributed users and devices, on-premises and cloud-based apps, and multiple physical and virtual servers.

OpenText can help you build a robust zero trust framework that ensures identities are validated and access is managed dynamically. Through centralizing policy management and automating enforcement, you can close security gaps and make compliance and auditing much easier.



Proposed next steps

Together, we can outline a vision and identify opportunities to address your organization's zero trust security goals. Below are suggested next steps.

- **Initial introductory meeting**
  Bring together your OpenText Global Account Director or Senior Account Representative with your organization's CISO, COO, CTO or decision maker on cyber security investments.
- **Joint roadmap exchange**
  Hold a day-long information exchange between operational leaders (Directors and above) and OpenText to gather insight into your security challenges, threats, operations, and cloud architecture.
- **Engage the OpenText Business Value Consulting team**
  Have them assess your current state of security and define a vision and roadmap to optimize your move to zero trust.

Wade Dennis
GAD
wdennis@opentext.com
832-564-5322