

# Security in the Phy-gital Retail World



## SECURING THE PHY-GITAL INTERSECTION BETWEEN THE PHYSICAL AND THE DIGITAL

Today's retail world is no longer about purely physical or digital. What started as brick and mortar evolved to "click and mortar", and further to multi-channel retail. Now, we are moving to an omnichannel model, which emphasizes a uniform experience across channels, relies on deep customer insights to ensure contextual relevance, and enables engaging customers across multiple channels through their digital journey. This is the phy-gital world. The whole landscape is greatly expanded, with new channels, new technologies and many changes in people and processes:

## EXPANSION OF SECURITY CONSIDERATIONS IN OMNI-CHANNEL RETAIL

 <p><b>TRADITIONAL ONLINE RETAIL</b></p>	<ul style="list-style-type: none"> <li>■ Web</li> <li>■ Mobile</li> </ul>	CHANNELS	<ul style="list-style-type: none"> <li>■ + Partners and API</li> <li>■ + Mobile POS</li> </ul>	 <p><b>OMNI-CHANNEL RETAIL</b></p>
	<ul style="list-style-type: none"> <li>■ Web, Mobile apps</li> <li>■ On premise</li> </ul>	APPS	<ul style="list-style-type: none"> <li>■ On premise + on cloud + SaaS</li> <li>■ Non-traditional stacks</li> </ul>	
	<ul style="list-style-type: none"> <li>■ PII</li> <li>■ PCI</li> </ul>	DATA	<ul style="list-style-type: none"> <li>■ + Price lists</li> <li>■ + Supply chain networks</li> <li>■ + Enterprise strategies</li> </ul>	
	<ul style="list-style-type: none"> <li>■ Data center</li> <li>■ Network</li> </ul>	INFRA	<ul style="list-style-type: none"> <li>■ + Store infrastructure</li> <li>■ + Partner infrastructure</li> </ul>	
	<ul style="list-style-type: none"> <li>■ Own team</li> <li>■ In-house processes</li> </ul>	PEOPLE PROCESSES	<ul style="list-style-type: none"> <li>■ + Extended teams w/ partners</li> <li>■ + Geographical separation of data &amp; processes</li> </ul>	

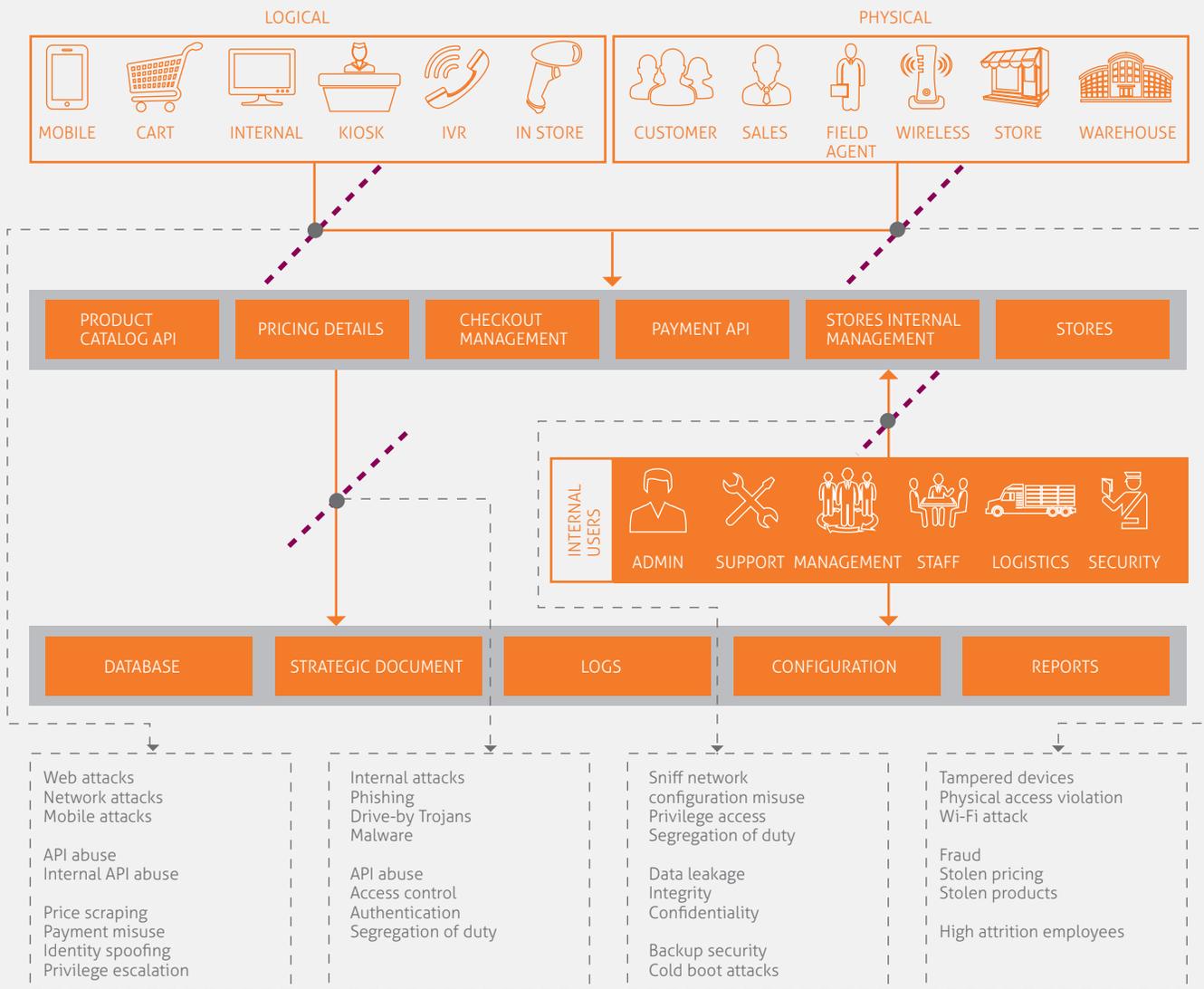
The way this landscape is architected is also quite different. It consists of:

- Systems of engagement which include physical and digital channels
- Partner and third party systems
- An API layer that acts as the boundary between the above and the core systems
- Multiple access paths - external and internal applications accessing the API and core systems, and internal applications directly accessing core systems

## EXPANDING SECURITY CONSIDERATIONS IN THE PHY-GITAL WORLD

Security threats and concerns have also evolved alongside the new landscape. First, it was all about physical security: protect the store and its merchandise. Then it expanded to online security. Now, the dimensions of security are even more complex. The overall ecosystem is no longer in the realm of one entity, but is spread across several partners. It's no longer deployed only on organization-controlled data centers, but also in cloud environments.

With increasing competition, the definition of sensitive data has changed from just PII and card holder data, to include numerous customer details. The pace of evolution is now varied: systems of record are stable, while systems of engagement evolve rapidly. With this rapid evolution comes the need to contain any security lapses that rapid development brings. The new attack surface looks like:



To protect this burgeoning environment, we must employ defense-in-depth and data-based security for all layers and components. While traditional security measures such as preventing Open Web Application Security Project (OWASP) vulnerabilities in applications, network attacks such as Denial of Service (DOS), malware, man in the middle and securing data at rest and in motion continue to be essential, the additional implications of this expanded landscape are described below:

## ATTACKS AT THE EDGE: PHYSICAL TOUCHPOINTS

### Compromised Devices and Networks

This class of attack vectors uses tampered devices,

Trojans or malware, or compromised networks to sniff and hijack data or inject malicious payloads, and targets consumer devices, in-store POS systems and Wi-Fi hotspots,

and inadequately secured partner infrastructure.

It is critical to support these multiple payment modes while ensuring non-fraudulent transactions.

### Malicious Intent and High Attrition

In this class of attacks, there is malicious intent by consumers, employees, partner workforce, or hackers, to commit fraud or theft. A variety of vectors may be employed, ranging from phishing to stealing data from systems. Malicious intent, when combined with high attrition employee roles, compounds the problem since these roles can move to competitors along with sensitive data.

## ATTACKS AT THE EDGE: ONLINE TOUCHPOINTS

### Web and Network Attacks

These threats include those of OWASP vulnerabilities, malwares, 3rd party vulnerabilities, DOS, etc., targeted at browsers and the network.

### Mobile Attacks

In addition to securing what mobile apps access on the server side, it is equally important to secure sensitive data on mobile devices. Attacks range from rooting the device, HTML5 cross-domain attacks to extract sensitive information, to MITM (Man in the Middle) attacks.

### Attacks on Kiosks

Kiosks have now expanded beyond traditional on-premise operations, to being exposed or to call external APIs to perform advanced tasks. The attack surface for kiosks has thus increased, with more Internet or web service connectivity, and could be prone to attacks like drive-by downloads and Trojans.

### Attacks on the POS

Traditional POS systems on controlled hardware are now being replaced by Mobile POS solutions, mobile wallets,

mobile apps, and numerous payment modes on consumer or third party devices. It is critical to support these multiple payment modes while ensuring non-fraudulent transactions.

### Attacks on API

Since the API layer is exposed to external applications, it is subject to multiple attacks such as verb abuse, Denial of Service, script-, XML-, and SQL-injection, cross-site request forgery, local file inclusion, parameter and identity attacks, authentication bypass, and session and token abuse. The API layer must be secured similarly for client, partner, and external applications.

### Attacks on Data

Whether it is internal or external, all attacks or fraud are on data. In addition to securing PII and PCI data, various forms of competitive data must now be secured against inadvertent disclosure to entities that may misuse it. Examples of such competitive data are price lists, supply chain networks, and confidential enterprise strategy documents. Data must also be secured in partner systems and on field devices. The typical attacks on data involve dumpster diving, cloud service attacks, phishing and malware, and internal attacks.

## TRUST CHAIN ATTACKS: ATTACKS ON PARTNERS

Our partners and vendors are now closer than we think, and an impact in our vendor or partners' network would impact our business and data. Examples of attacks on partner / vendor networks are cold boot attacks, network sniffing, phishing, drive-by downloads, privilege access, data leakage or misuse, dumpster diving, and compromises of confidentiality.

### Deployment and Infrastructure Considerations

Applications are now being deployed in hybrid models leveraging cloud infrastructure and SaaS applications to augment on-premise systems. It is thus essential to address aspects related to securing data in the cloud, during transfers to the cloud, and ensuring parity of identity across boundaries. These considerations need to extend to partner and store infrastructure.

### People and Process Considerations

The focus used to be on securing in-house processes and access of data to the organization's workforce. Now, this needs to extend to how data can be secured across extended teams, including those of partners and centralized entities, and how data distribution is constrained, for example by geography.

Insider attacks form a high percentage of threat vectors

### Insider Attacks

Insider attacks form a high percentage of threat vectors. Insider threats are either due to malicious users, due to compromised identity or devices, or simply due to negligence. The contribution of compromised or negligent users to threats has increased due to BYOD, open networks, and social engineering.

## APPROACHES TO SECURITY

Given the number of new threat vectors and the increased attack surface, the key principles to achieving security should be:

**Defense in Depth:** No layer trusts the layer above, and builds in security to deal with possible compromise in that layer.

**Evidence based Audit:** All external entities – partners, vendors, consumers – must prove that they are not compromised, and the landscape has checks in place to validate this trust.

**Untrusted Insiders:** Since many attacks are insider attacks, access to internal entities must also be based on authentication and authorization, with established segregation of duties, including to protect against malicious administrators.

These approaches to security are explored below:

### Securing Channels

Any apps built by partners are isolated from core systems of record. Next, partner access and security is managed and limited, and systems are secured against “rogue” partners. Then, API usage is protected against non-partner access. All across, keys are protected against compromise using HSM (Hardware Security Module) for storage, and key rotation policies.

Secure data in the cloud and on premises through access control and encryption

### Securing Application and Deployment

First, secure data in the cloud and on premises through access control and encryption. Then, secure data transfers between premises and cloud at protocol and message /payload level, and by checking integrity using Hash-based Message Authentication Code (HMAC). Finally, unify identity management through directory replication or federated identity.

### Securing Data

Use rights management for electronic documents and electronic interchanges. Then, secure sensitive data within partner ecosystems and control data transfer to and storage on field staff devices. Finally, constrain data on a need to know basis.

### Securing Infrastructure

First, secure store POS systems through anti-virus, and also secure in-store connectivity such as Wi-Fi hotspots, and mobile POS applications. Then, secure infrastructure in partner premises (or impose minimum criteria and audits). Ensure that the same rigor is applied across all infrastructure, be it private, partner owned, or cloud-based.

### Securing Mobile and Cloud

Impose a reference architecture on mobile applications that includes security of on-device data, identity, and authentication. Next, have a strict adherence to a cryptography standard for securing data and transport, and to secure the identity and PII of customers. Finally, protect data on cloud through encryption and transport security, ensure that data isolation is provided for, and that keys are stored securely (for example, using HSMs).

### Securing People and Processes

Put in place processes to secure data across extended teams and diversified remote workforces, including those of partners, using mechanisms such as rights management, content expiry, and multi-factor authentication. Put in checks and balances for data security for geographical distribution or for use by centralized or global teams.

### Incident Response

First, ensure that processes are in place to rapidly assess the nature of compromise due to the incident, and to propagate any mitigation steps to adjacent systems. Next, ensure that a root cause analysis is carried out as soon as possible to identify the underlying threat vectors and to put mitigation steps to prevent future attacks. Finally, update the threat model to include this and similar vector classes.

## SUSTAINING SECURITY HYGIENE

While implementing this new approach to security, take a conscious effort to ensure that security is defined in the Assess, Build and Sustain formula as depicted below:



Assess

- Create the threat model
- Assess the threat levels
- Assess current vulnerabilities



Build

- Based on threat model and current state, implement security measures
- Evaluate vulnerabilities through audits



Sustain

- Establish governance and processes for periodic audits and reassessments
- Establish timelines for periodic review of threat model

## SUMMARY

The digital world brings new challenges in supporting business growth while ensuring that associated security risks are controlled. As business continues to evolve in the Phy-gital world, new attack surfaces will arise and we'll need to create new ways to build and secure systems, and to educate users across the entire value chain. However, if security is not a consideration from the beginning, then, instead of letting business grow confidently, it will impede business agility. Security must hence be a core aspect across applications, data, infrastructure, people, and processes, and be driven through a robust threat model to ensure manageability of security risks.

Mindtree and our security specialist partner, Aujas, can deliver services to assess your security landscape and set up a security center of excellence (COE) with you. For the landscape assessment, we offer services such as:



### Data Flow Analysis

As certain how data flows across systems and processes, and identify vulnerabilities therein



### Data Security Analysis

Assess the data security architecture for identified critical areas, and identify vulnerabilities and recommendations for securing data at rest and in motion



### API Security Architecture Definition

Define the strategy for API security



### Red Team Assessment

Assess on-ground processes including physical security and processes



### Digital Security Readiness Assessment

Verify and validate the readiness for digital security

#### The Security COE would be responsible for:

- Defining and enforcing security guidelines across the group
- Enterprise Security Architecture
- Carrying out periodic audits and assessments
- Establishing forward-looking business and technology change impact assessment
- Recommending ongoing security architecture evolution
- Threat Intelligence
- Cloud Security and Migration Risk

We will be happy to work with you to identify these areas of collaboration.

## ABOUT MINDTREE

Mindtree [NSE: MINDTREE] delivers digital transformation and technology services from ideation to execution, enabling Global 2000 clients to outperform the competition. "Born digital," Mindtree takes an agile, collaborative approach to creating customized solutions across the digital value chain. At the same time, our deep expertise in infrastructure and applications management helps optimize your IT into a strategic asset. Whether you need to differentiate your company, reinvent business functions or accelerate revenue growth, we can get you there. Visit [www.mindtree.com](http://www.mindtree.com) to learn more.

## ABOUT AUJAS

Aujas is a Global Information Risk Management (IRM) services company. We help clients mitigate risk and enhance information value and today partner with over 370 clients in 23 countries. Aujas' service portfolio includes Risk Advisory, Identity & Access Management, Threat Management, Data Protection, Secure Development Life-cycle, Privacy Services and Mobile & Cloud security. Aujas has been ranked the fastest growing information risk management services company in India for last 4 years

