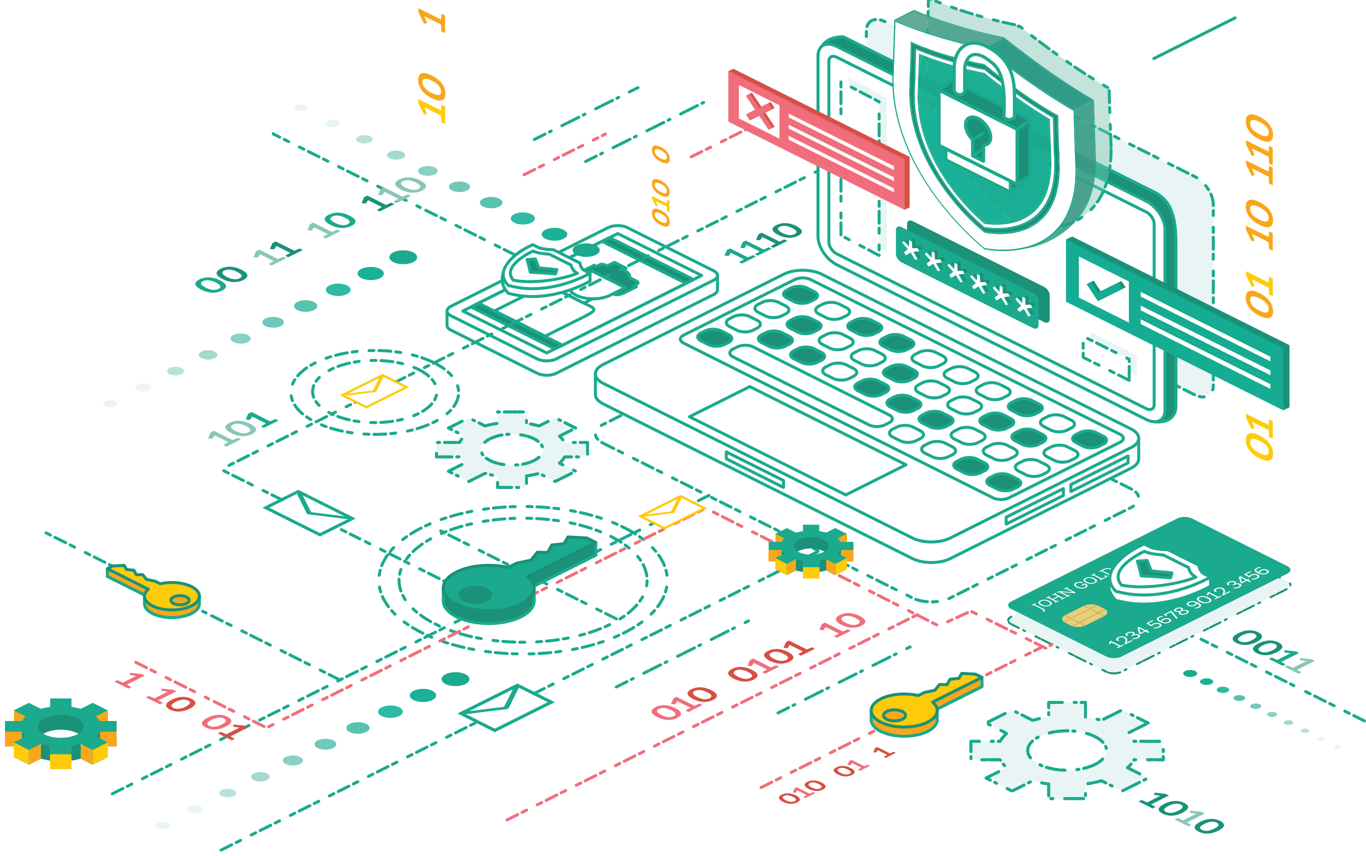
Realigning Security for Retail and Consumer Goods

Responsible remediation:
Defying COVID-19

www.hcltech.com



The realignment of buying priorities, personal lifestyles, and work practices, that are forced on us by the COVID-19 pandemic may represent a seismic shift in the Retail and CPG Industry. Consumer adoption of technology-enabled commerce channels is likely to deepen and broaden permanently, even in segments which have till date, resisted the large-scale migration from stores to online.

As stores, offices and manufacturing facilities close across the world to manage the spread of COVID-19 pandemic, the Retail and CPG Organizations operating in essential and non-essential segments are challenged to face following business scenarios:

- Leverage new connectivity tools and ways of working to support corporate staff working remotely.
- Scale ecommerce operations and switch focus to digital consumers' experiences, as consumers turn to order online.
- Create strategies to manage inventory stuck in closed stores that needs to be moved to make way shelves fulfillment.
- Adopt scenario planning with value chain partners for global supply chain disruptions likely to impact sourcing, manufacturing, and logistics.

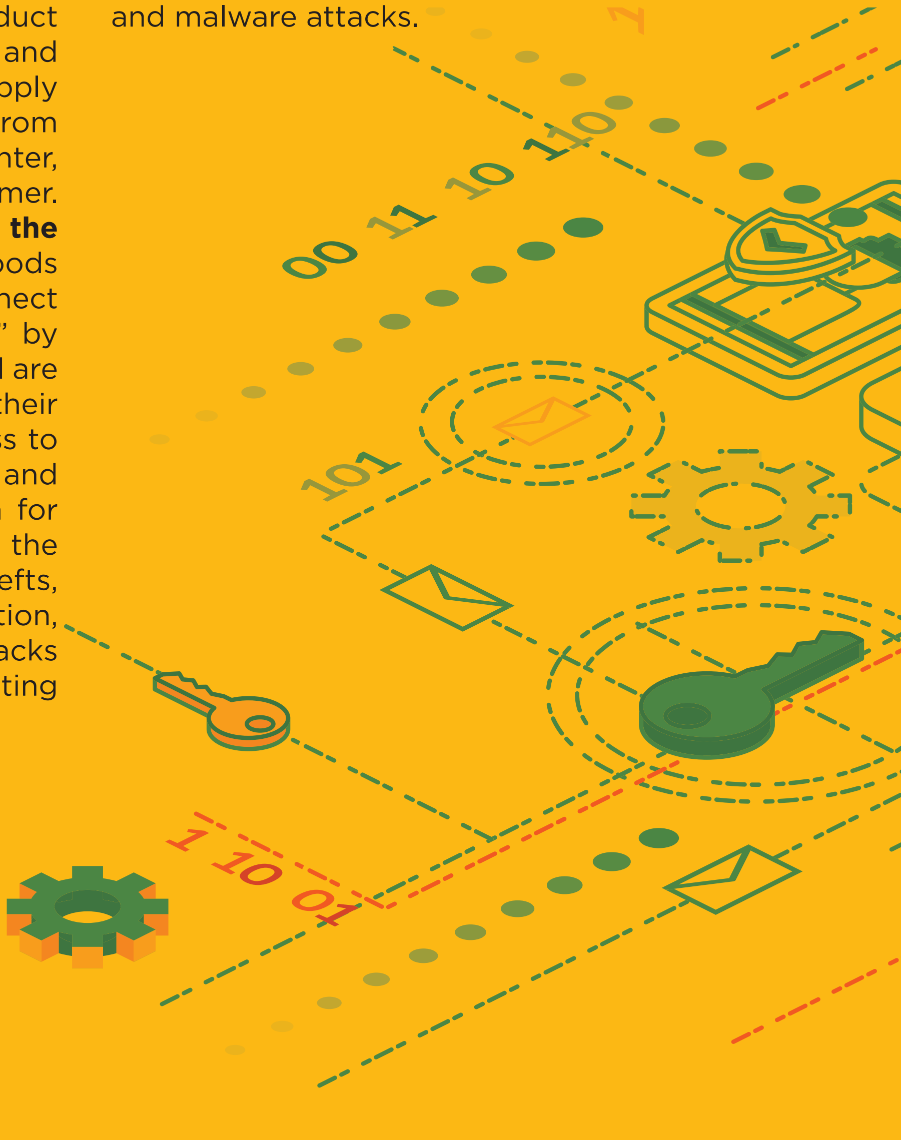
This leads to the transformation of Retail and CPG business operations which puts various ecosystem components such as **Point of Sale (POS)** to **Supply Chain Warehouses** to **Point-to-Point Transportations** to **e-Commerce** channels, at risks, associated with Vulnerability and Cyber-Security. Sometimes in a bid to reach to the end consumers faster, the organizations often build applications or platforms without implementing common security standards, allowing cyber threat manifestations to happen and invade into their IT landscape, more so the Legacy systems which can't keep up with new Cybersecurity demands.

Distributed Path to Cyber Invasions and Attack Points for Retail & CPG Organizations

Retail Organizations are storing more consumer data than ever before - across an increasing range of digital platforms, thus providing cybercriminals with more valuable data to target. As the retail chains interact with ecosystem partners – vendors/ distributors/sister-chains through network devices, their network infrastructure connected to POS systems increasingly become an inlet for Cyberattacks, causing infrastructure damage, besides resulting in the loss of reputation, slowed financial growth, and increased legal liability.

Additionally, Consumer Goods Organizations offer distinct brands, handle product development and manufacturing, and maintain complex-but-predictable supply chains. The flows of goods happen from plant to warehouse, to distribution center, then to the store, shelf, and the consumer. **COVID–19 seems to have disrupted the entire value chain flow.** The Consumer Goods Organizations are constantly vying to connect with the "socially restricted consumers" by scaling their e-commerce operations and are looking for opportunities to strengthen their supply chain ecosystem to enable access to consumers, leverage market solutions and sometimes, access sources of raw data for B2B/B2C engagements. This opens up the probabilities of data breaches, frauds, thefts, phishing attacks, brand impersonation, brand-jacking, cybersquatting, DDOS attacks and trademark infringement - impacting sales and affecting the end-consumers.

Finally, with the lockdown of the countries across the globe, the workforce has been forced to move their workplace from office to home. This has brought few challenges from both user as well as corporate perspective. Corporates need to run their business to an extent that they can avoid the current economic crisis. Users need to work from home in a similar fashion as they were working from office with as much productivity as possible. The possible path to purchase of the "Retail and CPG" products through online brings severe possibilities of the consumers data breach through ransomware and malware attacks.



Cybersecurity Challenges in Retail and CPG Organizations

Retailer Networks & Web Applications

- As retail chain interacts with multiple other chains/ vendors through network, needs to be secured completely
- Applications on required systems and consumer facing applications needs to be free from vilnerabilities and strongly secured

Digitalized Business

- As the business is becoming digital and online driven, there are increased number of digital customer engagement channels, new technologies & services coming up, cloud journey and expanded use of data that intoduces new vulnerabilities

Regulations & Compliance

- Securing customer information in critical responsibility of every retail industry
- Authorities are focussing on new and tougher data privacy regulations such as GDPR, PCI-DSS addressing geo/region specific requirements

Elaborate Partner & Vendor Ecosystem

- Retail Companies are working with an increasing number of third parties and supply chain partners-leading to multiple connection exchanges, resulting in increased cyber risks

Data & Privacy

- Minimize the risk of cyberattacks by discharging monitoring and managing confidential dat where it is stored

Competitive in Marketplace

- There is an increasing alarm of risk while industry is trying to enhance customer experience through onine services like “same day deliver”’ mobile shopping, online sales Session”

Our Understanding of Client Requirements and Our Solution Portfolio

HCL has a sound interpretation of Retail & CPG business security & compliances and we understand the challenges & point areas which are likely to be exposed by threat vectors. Various points of attacks that we understand can endanger Retail & CPG Organizations business landscape are seen as below:

Point of Sales (POS) Breaches

- Direct accessibility to POS systems
- Lack of Point-to-Point Encryption (P2PE)
- Vulnerabilities on OS, servers on which POS is running

Digital Risk

- Malwares being used at POS (eg: Lock POS), applications and infra
- Malicious links & downloads
- Sophisticated malware injection techniques
- Sophisticated Phishing techniques

E-Commerce Web Applications

- SQL Injection
- Admin Credentials theft · Theft of PII data of end customers

Considering the current pandemic situation when the complete enterprise workforce is working from home, below are additional challenges faced by the Retail and CPG Organizations:

Current Infrastructure Issues:

- Capacity issues of existing setup
- Data center connectivity issues
- Security vulnerabilities with traditional VPN infrastructure
- Visibility of network traffic

User Activity & Productivity:

- Monitoring of users' activity & productivity
- Preventing end users to fall prey to phishing attacks
- Sharing of critical user credentials with a co-worker leading to malicious attack techniques

Secure & Seamless application access:

- Secure access to all applications for remote users
- Granular control of traffic to internal applications on cloud and on-premise environment, as well as SaaS applications
- Monitoring of third-party access to enterprise environment

With our combination of advisory and technology solutions, we help organizations not only embed advanced security features across their systems but also develop a cybersecurity aware culture. Moreover, our specialization in the **consultation-implementation-operation** follows an agile approach that keeps pace with a constantly changing technological paradigm to make sure that our customers stay one-step ahead of every danger.

Point of Sale (POS) Security : Our Endpoint protection and encryption solution that facilitates credit/debit card data transmission directly from POS unit to Gateway without hitting the POS device directly, ingrained with POS software scanning for malware detection.

Brand Protection : Our Social Media and Digital Risk Protection Service protects your brands, prevent hacks, and avoid costly compliance violations by using leading threat intelligence tools to detect advanced phishing, email protection and fraud attempts by scanning major social media spaces as well as monitors clear, deep and dark web - monitored by our Cybersecurity Fusion Centre (CSFC).

Anti-phishing : HCL has partnered with industry leading provider of advanced phishing threat protection, combining human intelligence with machine learning to prevent, detect, and respond automatically to advanced email phishing threats.

Application Security on-Demand : Our On-demand Application Security Services (DAST) aims at protecting business programming language codes and the data stored within the system through advanced processes, technology and industry policies. This also includes executing scans of both internal and external websites.

Remote Access/ Work from Home : Our Remote Access solution is a software defined cloud-based service following a zero-trust strategy, which will ensure a secure access of all types of enterprise users to the applications hosted in the infrastructure while they are working from home in the current situation. It will provide additional security in terms of multi-factor authentication and micro-segmented access from user to applications.

Our Key Differentiators and Value Advantage:

300+ Client Relationships

3500+ Security Professionals

20+ years of cumulative experience

7 CSFC & 40+ GDCs

40+ Partner Alliances

25 billion events processed / day

Threat Intel Fusion from 40+ Sources

Security Enablement @ day 1

Dynamic Frameworks and Accelerators

SAFE

SecIntAI

DIGI-I-FORT

IDaaS

BRiCS

iBCM - iDRM

Data Privacy

HCL's Solution Partner Network

HCL has technology solutions partnership with vendors to ensure our customers stay abreast of the technological innovations and leverage customized solutions for their specific needs.

Case Study: Creating Defense for a Cosmetic Manufacturer

HCL helped a leading US-based cosmetics manufacturer defend its business against cyber threats across their global networks. With HCL's security solution framework, the company was able to:

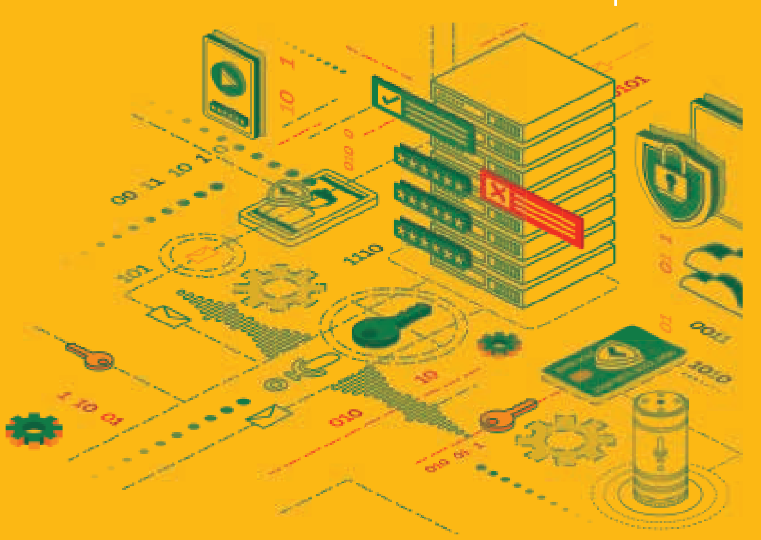
- Implement a new security architecture, including, a Central Security log management solution
- Seamlessly manage perimeter level security across locations
- Deploy multi-layer protection against zero day threats at network and endpoint layer
- Ensure malware containment between inter- and intra-networks

Key Features

- Standardization and consolidation of technologies like firewall, IPS, VPN, URL
- Highly scalable proxy solution
- 24x7 Security Operations, Monitoring & Management
- Multi-Technology Fit-for-Purpose solution to meet industry best practices and compliance requirements
- Vulnerability Scanning and Policy Scanning for 3000 IP(s)

Key Benefits

- Protect 400+ security devices
- Encompass 25,000+ endpoints
- Secure 3000+ servers
- Defend 15,000 events per second



For more details contact: **cs_marketing@hcl.com**