Can Enterprise Architecture Defend Against Supply Chain Attacks? A Retail Sector Perspective

Fangping Ning
University of Melbourne
fangping614@gmail.com

Hairuo Zhao
University of Melbourne
hairuoz2000@gmail.com

Jiawei Wang
University of Melbourne
kimw84321@gmail.com

Yiran Ai
University of Melbourne
aiyiran2025@gmail.com

Rod Dilnutt
University of Melbourne
rpd@unimelb.edu.au

Leila Meratian Esfahani
University of Melbourne
lmeratian@unimelb.edu.au

Abstract

This report looks at how enterprise architecture (EA) in the retail sector can be adapted to mitigate the risk of supply chain attacks (SCA). Many retail companies use outside systems and third-party platforms. This makes it easier for attackers to get in through trusted links. We looked at two real cases: SolarWinds and Blue Yonder. After analyzing these cases, we found four problems when retail companies suffered supply chain attacks. These depend too much on one vendor, not knowing what third-party systems are doing, not having strong plans for when problems happen, and giving third parties too much access. To solve these problems, we give suggestions from three EA layers: business process, information systems, and technical infrastructure. These suggestions include having backup plans, separating system parts, using shared monitoring tools, and making access rules better. This study will be helpful for researchers and architects working in retail. It can enhance system resilience without losing speed and performance.

Keywords: *Enterprise Architecture, Supply Chain Attack, Retail Systems, Cybersecurity, System Resilience*

1. Introduction

Enterprise Architecture (EA) is important in the retail industry. It helps companies manage business activities, control systems, and connect digital platforms (Chakraborty et al., 2023). With the retail sector using more digital platforms such as Customer Relationship Management (CRM), Point-of-Sale (POS), and Supply Chain Management (SCM), these systems often connect to outside vendors and third-party platforms (lavanyapg, 2024). This open and connected setup improves efficiency but also brings more security risks. One major risk is the supply chain attack (SCA). In this kind of attack, hackers use trusted third-party software or service links to get into the retailer's system (Alkhadra et al., 2021). These attacks can cause major disruptions to retail operations, including delivery delays, inventory failures, and customer service breakdowns. In this report, we examine two real-world cases to illustrate how these consequences unfold in practice.

Some studies have looked at how to adjust EA to deal with supply chain attacks, but there is little research focusing on the retail industry. Retail firms are particularly vulnerable to supply chain cyberattacks. According to recent industry data, 38% of retail organizations have experienced such attacks (Lindner, 2025). So, we aim to adjust EA more specifically for the retail sector. This leads to our research question:

How can enterprise architecture in the retail sector be adapted to mitigate the risk of supply chain attacks?

This question is important because many real supplies chain attacks have hurt retail companies. In the SolarWinds case, attackers got into many systems through a software update (Martínez & Durán, 2021). In another case, a ransomware attack on Blue Yonder caused problems with delivery and inventory for several large retailers (AP News,

2024; Semantic Visions, 2024). These events show that supply chain attacks can cause delays, data loss, and customer service issues. This harms business and loses customer trust.

It is important to study how EA can help retail companies with supply chain attacks. This report focuses on the retail sector. It uses the three-layer EA structure to suggest solutions. These solutions aim to reduce risks and improve safety when working with outside systems.

2. Literature Review

2.1. Enterprise Architecture in the Retail Sector

Enterprise Architecture (EA) is a method that helps companies manage business processes, systems, and technologies in a clear way. It connects business and IT. It is helpful to plan, combine, and control systems across the company (Kotusev et al., 2016). In retail, EA helps companies respond to customers' needs and make decisions using data (Chakraborty et al., 2023).

EA and enterprise applications are different. EA is the overall design and governance of all systems in a company (Psaraftis & Poulimenakou, n.d.). Enterprise applications are tools that work within the EA framework, such as Supply Chain Management (SCM) and Customer Relationship Management (CRM). These systems are part of EA, but EA also includes the planning, connection, and control of these systems (lavanyapg, 2024).

TOGAF® has four main domains: Business Architecture, Application Architecture, Data Architecture, and Technology Architecture. In the ADM cycle, Application and Data are placed together under Phase C: Information Systems Architectures (Hengky et al., 2024). In this report, we follow the same structure. We use three layers: Business Process Layer, Information Systems Layer, and Technical Infrastructure Layer. This three-layer model is also common in retail system design. It is simple and practical for analysing enterprise architecture in the retail sector. (Fernando & Paiva, 2020).

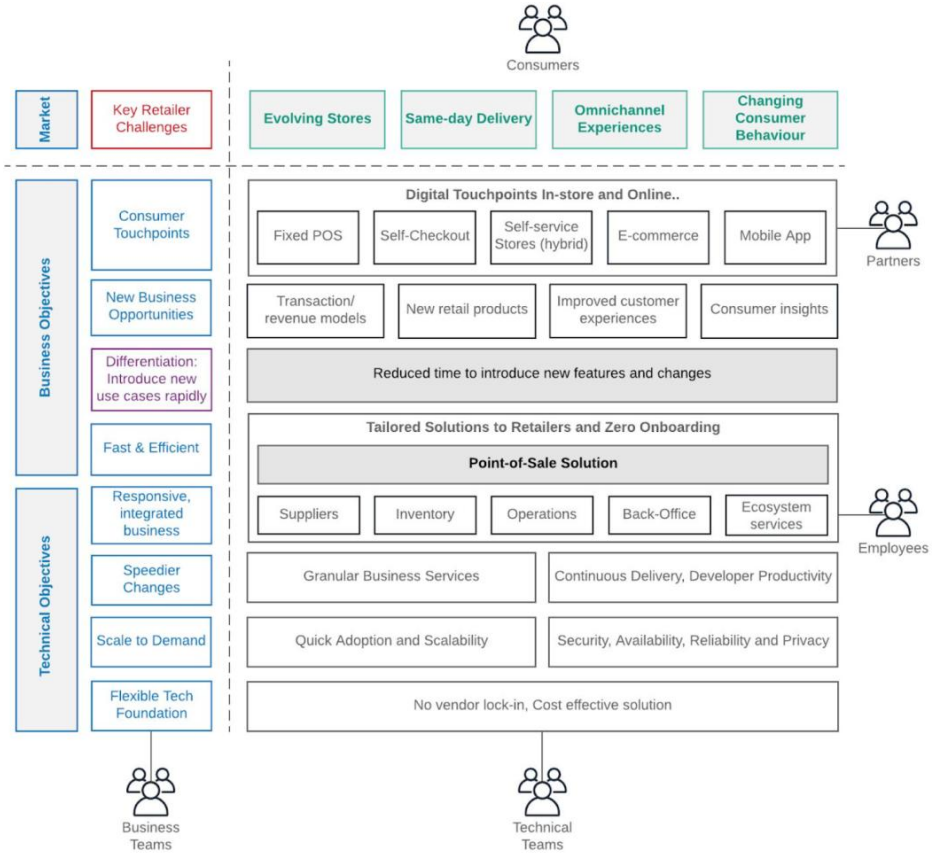

Figure 1 Business Process Layer

Figure 1 shows **the Business Process Layer** in retail. It includes customer-facing tools, such as self-checkout, online stores, and mobile apps. It also includes back-end systems like inventory and operations. This layer helps retailers manage customer-facing and back-end processes in a clear way. These tools are designed on shared workflows and goals. For example, order systems and delivery systems are linked to sales interfaces. This helps the business run smoothly from front-end to back-end. It supports fast changes, new business models, and services across many channels. This is possible because the business workflows are modular. Companies can adjust to one process, like pickup or checkout, without changing the whole system. By connecting business goals with system functions, it helps reduce the time to launch new ideas. Business needs are mapped directly to digital functions. This reduces the gap between planning and implementation (Fernando & Paiva, 2020).

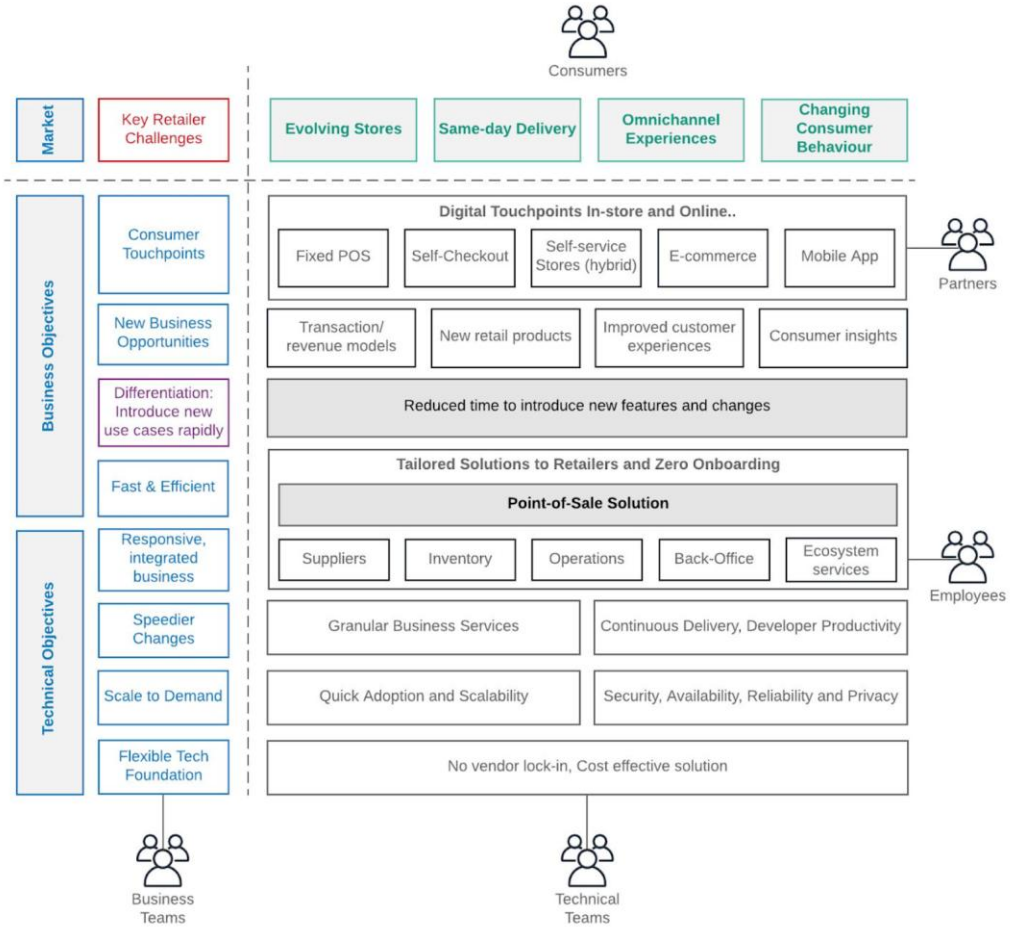

Figure 2 Information Systems Layer

The information systems layer connects business tasks with technical systems. It includes tools like POS, CRM, warehouse systems, and supplier platforms. It also manages how data moves between these systems. Figure 2 shows how the systems work together inside the store. It also shows how they connect with external services using APIs and platforms. For example, the POS system sends sales data to the warehouse system to update stock levels. CRM receives the same data to record customer purchase history. ERP connects with supplier systems to manage orders and deliveries. This data flow allows each system to perform its task using real-time and consistent information. It avoids information gaps and reduces manual data entry. When data is updated in one system, the change is reflected across others. This shared information enables coordination between departments. For example, the sales team and the delivery team can both access the same order status from their systems. This improves business efficiency and reduces delays (Fernando & Paiva, 2020).

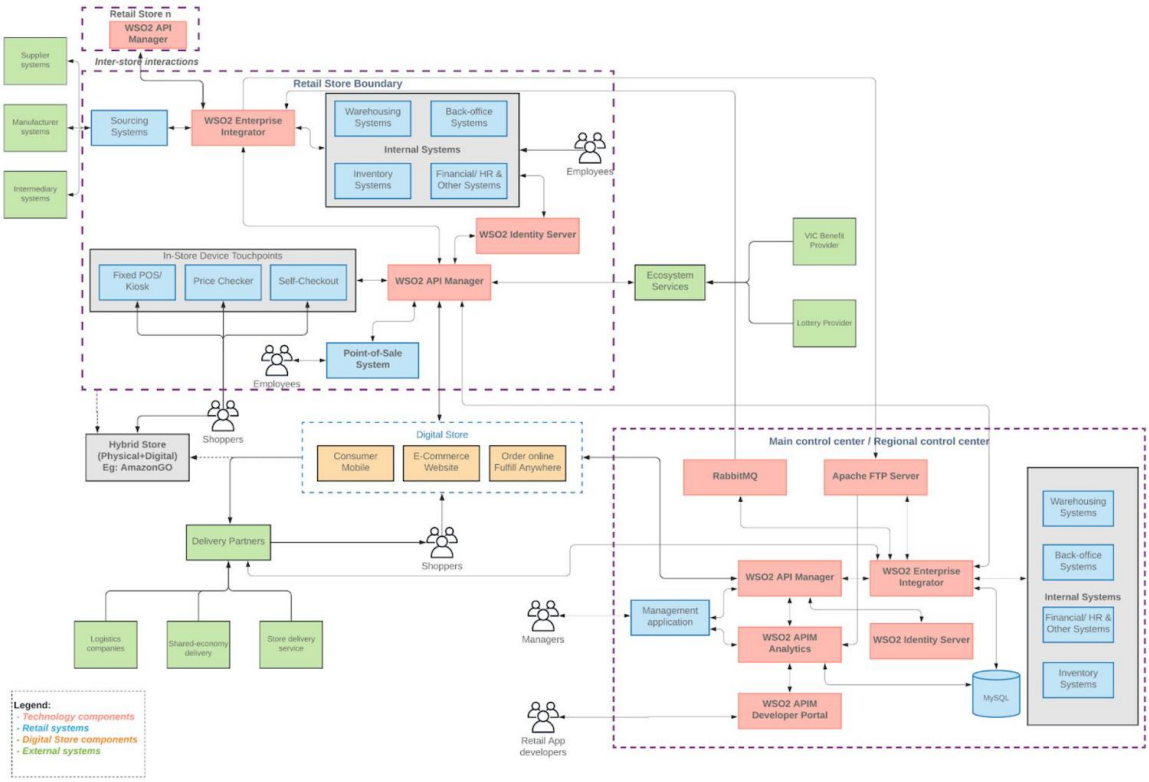

Figure 3 Technical Infrastructure Layer

The technical infrastructure layer supports the whole system. It helps the retail system run safely, quickly, and reliably. As shown in Figure 3, this includes tools like identity systems (CIAM), API gateways, platforms for integration, developer tools, analytics engines, and messaging tools. These tools connect different systems inside and outside the company. API gateways and integration platforms manage system calls from third parties using standard interfaces to send and receive data. They also monitor every data exchange in real time. This helps the company connect with partners quickly and safely. Analytics and monitoring tools collect system logs and performance data. When there is a slow response or failed connection, the tools send alerts. This helps staff fix problems before the system breaks down. It reduces downtime and improves system reliability. (Fernando & Paiva, 2020).

These three layers form a clear framework. They help explain how retail EA supports business tasks. They also show how systems work together and connect with external vendors and services. The business process layer helps retailers design and adjust workflows to meet customer needs. The information systems layer ensures data can flow between systems and departments to support daily operations. The technical infrastructure layer provides the tools to secure, monitor, and scale the system efficiently.

2.2. Supply Chain Cyber Attacks

A supply chain attack is a kind of cyber-attack where the attackers do not attack the organizations directly, instead they attack the software developers and providers (Alkhadra et al., 2021). There are three main sources of software supply chain attacks such as open-source software supply chains, commercial software products, and foreign-sourced threats (Muhammad Zeeshan Malik & Bukhari, 2023). According to Tharayil (2025), the reason behind the setback in Morrisons's operations in November 2024 is the cyberattack on its software provider Blue Yonder. Blue Yonder is a supply chain software provider serving several major retailers across the UK and the US. It provides SaaS-based solutions such as supply chain planning, warehouse management, and labour management, which are deeply embedded in the operational infrastructure of organizations (Blue Yonder, 2023). According to ENISA (2021), supply chain attacks start by targeting one or more software providers. Once attackers enter the software providers' system, or infect their products, they can get access to the assets of customer such as sensitive data.

The mechanism of the supply chain attack is shown in Figure 4 where the attackers install malware in the normal applications provided by software providers. After that, attackers may gain access to sensitive data when the targeted organizations install updates that contain malware (Muhammad Zeeshan Malik & Bukhari, 2023).

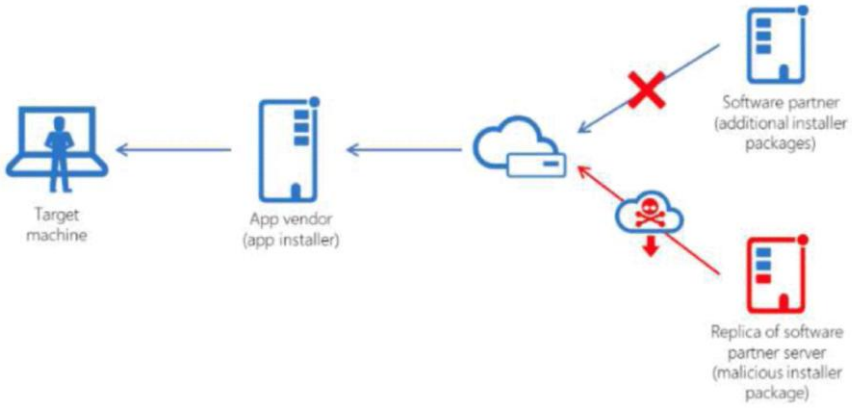

Figure 4 Software Supply Chain Attack

Supply chain attacks would disrupt critical supply networks and operations, compromise product integrity, and negatively impact critical infrastructure functions, which in turn can lead to the leakage of customer private data and cause direct financial losses (Squillace & Cappella, 2024). Moreover, such attacks pose significant threats to organizational reputation, as breaches decrease customer trust and public confidence. For instance, during the Blue Yonder ransomware incident, Morrisons faced operational failures that disrupted fresh food replenishment (Refna Tharayil, 2025). The failures would severely damage the organization's relationships with business partners and stakeholders, who may reconsider future collaborations due to perceived security vulnerabilities.

2.3. Why Retail is Especially Exposed to SCA

There are three main reasons why the retail industry is more vulnerable to supply chain attacks than other industries: dispersed system structures, heavy reliance on external systems, and limited security resources.

Firstly, due to the nature of their business, retail enterprises have a dispersed system structure with different departments operating independently. Different business departments often have their own independent systems. For example, warehouses use WMS systems, stores use POS systems, and customer management uses CRM systems. These systems come from different vendors and use different technical standards, making integration difficult (Kotusev et al., 2016). Additionally, these systems typically do not share data, operating independently and creating 'data silos' (Fernando & Paiva, 2020). As a result, when companies attempt to implement unified security policies or conduct risk monitoring, this structural separation makes it difficult to identify weaknesses and respond to risks in a time-sensitive manner (Fortinet, 2022).

Secondly, the operations of retail enterprises rely heavily on external systems and service providers. These external systems include third-party payment platforms, logistics systems, electronic invoicing systems, customer marketing platforms, and so on. Although these services can improve business efficiency, they are also one of the potential attack entry points. Once the systems of any of these service providers is hacked, attackers may bypass traditional firewalls through integrated interfaces or automatic update programmes and penetrate the main system of retail enterprises (Williams, 2024). This type of attack, known as a 'trust path' attack, is difficult to detect and is a typical example of a supply chain attack (Hämäläinen & Nadesan, 2022). Incidents such as SolarWinds and Kaseya have affected thousands of service users, including many companies in the retail industry.

In addition, retail companies' security protection mechanisms are not very well developed. On the one hand, low profit rates in the industry make companies more inclined to invest their budgets in promotions or inventory rather than security protection (Gordon et al., 2003). On the other hand, many retail companies do not have specialised cybersecurity teams, and even if they do, they are small and unable to cover all systems or stores (Fortinet, 2022). In this context, it is difficult for companies to implement proactive defense measures, and they can only rely on basic access control and post-incident remediation. Once an attack occurs, companies often respond slowly, resulting in significant impacts and even system-wide disruptions.

3. Case Analysis

To better understand the mechanics of supply chain attacks, this section presents two case studies. The first case, SolarWinds, serves as a typical example that illustrates how attackers exploit trusted relationships between organizations and their third-party suppliers to penetrate broader networks. The second case, Blue Yonder, shifts the focus specifically to the retail sector. It demonstrates how digital supply chain dependencies make retail enterprises particularly vulnerable to upstream disruptions, which reveals how architectural decisions expose retailers to substantial risk, reinforcing the urgent need for architecture-level safeguards in retail supply chain environments.

3.1. Case Analysis: SolarWinds - A Prominent Supply Chain Attack

Many of SolarWinds' clients used a system called Orion, which is a performance monitoring solution designed to track the status of IT assets across client networks. Orion had privileged access to these networks and collected performance data and other sensitive information. In 2020, attackers inserted a backdoor known as Sunburst into Orion. SolarWinds unknowingly distributed the compromised software as a routine update, leading thousands of customers to install the malware through their automatic update systems (Fortinet, 2023). As a result, over 18,000 customers and 40 public and private sector entities—including government agencies, technology firms, insurance providers, financial institutions, and retail companies across continents—were affected, resulting in significant damage (Martínez & Durán, 2021). In this case, SolarWinds, acting as a third-party supplier, became the weakest security link in its clients' supply chains, making it an ideal target for attackers to access thousands of organizational networks. (Cloudoptics, 2024).

Although the SolarWinds incident occurred in the context of an IT software supply chain, the core issues it revealed are highly relevant to the retail sector, and potentially even more dangerous. Retail enterprises are heavily dependent on third-party systems, including payment gateways, logistics platforms, CRM tools, and SaaS-based ERP systems. As a result, the architectural vulnerabilities in retail supply chains closely mirror those exposed by the SolarWinds case, making the retail sector a high-risk target for supply chain attacks.

3.2. Case Analysis: The Blue Yonder Ransomware Attack

On November 21, 2024, Blue Yonder—a leading SaaS provider of AI-driven supply chain solutions—was targeted by the ransomware group Termite. The attackers infiltrated internal infrastructure, encrypted operational systems, and exfiltrated over 680 GB of data, including databases, configuration files, and sensitive client information (Semantic Visions, 2024). As a containment measure, Blue Yonder suspended its cloud services for several days, leading to widespread service outages (AP News, 2024).

Major retail clients, including Starbucks, Morrisons, and Sainsbury's, experienced immediate operational disruption. Starbucks was forced to revert to pen-and-paper scheduling and payroll tracking as its workforce management systems went offline (New York Post, 2024). Morrisons reported warehouse system failures that hampered inventory visibility and disrupted fresh food replenishment (Tech Monitor, 2024). Sainsbury's logistics operations were delayed due to the collapse of automated routing functions (Supply Chains, 2024).

These cascading failures did not result from breaches of the retailers' internal systems but from their architectural dependency on an external platform deeply integrated into core functions. Blue Yonder's APIs were tightly coupled with client-side ERP, logistics, and forecasting modules, leaving no functional redundancy or segmentation to localize the impact. As ENISA (2021) has emphasized, supply chain attacks often exploit systemic integration exposure rather than technical vulnerabilities. This incident underscores how upstream disruptions can propagate rapidly within retail ecosystems when architectural safeguards against third-party failure are absent.

3.3. Insights from Case Studies: Core Architectural Challenges in Retail

Challenge 1: Excessive Dependency on a Single Third-Party Vendor

The Blue Yonder case shows a growing issue in retail enterprise architecture: the heavy reliance on a single third-party provider for essential operations. In many cases, retailers had integrated Blue Yonder's services across essential operations without establishing alternative systems, which left them exposed when the platform failed. Few had modular designs or backup vendors in place to maintain continuity. This kind of dependency is common in modern retail and increases the risk of widespread disruption. As ENISA (2021) notes, integration without resilience leaves systems exposed to upstream failures. Ivanov (2021) similarly warns that without contingency plans, centralizing core digital services can lead to operational collapse—especially in time-sensitive retail environments.

Challenge 2: Lack of Visibility into Third-Party Security Posture

The Blue Yonder and SolarWinds cases reveal a common weakness in retail architecture: limited visibility into third-party security. Retailers using Blue Yonder had no insight into the vendor's security protocols and learned of the breach only after service disruption. SolarWinds clients similarly trusted software updates without knowing how internal access was managed. In both cases, integration occurred without transparency or oversight. ENISA (2021) refers to this as "blind integration"—where critical services are embedded into operations without governance. As supply chains grow more connected, this gap increases the risk of upstream failures spreading across retail systems.

Challenge 3: Inadequate Business Continuity and Backup Solutions

Preventing IT downtime is more cost-effective than dealing with its consequences. Robust backup solutions and a well-thought-out business continuity plan can help organizations maintain critical operations and recover swiftly during IT disruptions (Modern Networks, 2024). However, this remains a significant challenge.

An effective business continuity plan involves establishing alternative processes and ensuring that employees are trained to implement them (Modern Networks, 2024). In the retail sector, core processes such as inventory planning, order routing, and workforce scheduling are heavily reliant on uninterrupted digital access, often with few or no fallback options.

Comprehensive backup solutions should include regular data backups as well as reliable, tested recovery procedures (Modern Networks, 2024). Retailers without alternative methods for registering items and processing payments are particularly vulnerable (Semantic Visions, 2024).

This reflects a broader trend in the retail industry, where rapid digital adoption has outpaced investments in system resilience. As Ivanov (2021) emphasizes, continuity measures should be integrated into the system architecture from the outset—designed, tested, and ready to deploy—rather than developed reactively after failures occur.

Challenge 4: Excessive Access Privileges Granted to Third-Party Systems

A critical weakness exposed by the SolarWinds incident was the excessive access privileges granted to third-party systems (Stechynskyi, 2025). Since Orion was treated as a trusted application, its operations were not restricted by internal security policies or access controls, and these privileged permissions became the attack vector for exploitation. This high level of access, while operationally convenient, created an ideal scenario for attackers.

The SolarWinds case helps illustrate how supply chain attacks exploit trusted third-party systems, while the Blue Yonder incident shows how such risks play out in retail environments. Together, they reveal four core challenges in retail enterprise architecture: overdependence on vendors, limited visibility, weak continuity planning, and excessive third-party access. These challenges frame the discussion that follows on how retail systems should be architected to better defend against supply chain attacks.

4. Discussion

Based on the four main problems revealed in the two supply chain attack cases, the following section discusses adjustment strategies across three critical layers of enterprise architecture: the Business Process Layer, the Information Systems Layer, and the Technical Infrastructure Layer.

4.1. Solution 1: Architectural Mitigation of Single SaaS Vendor Dependency

To reduce dependency risk on a single SaaS platform within the information systems layer, we propose three targeted architectural improvements:

Modular Decoupling of Core Functional Components

In the Information Systems layer, core retail functions—such as forecasting, order routing, and inventory control—should be restructured into modular services connected via standardized APIs, an approach widely recognized for improving system flexibility and fault isolation (Wolfart et al., 2021). This allows individual components to continue operating during partial system failures. For instance, order management processes should not be critically dependent on the real-time availability of forecasting modules. As highlighted by ENISA (2021), modular system design also minimizes the blast radius of external service outages in supply chain attacks.

Hybrid Redundancy Integration

In the Business Process Layer, Critical services should be backed by secondary vendors or internal alternatives through "warm standby" setups. For instance, a logistics optimization module can be connected to two parallel platforms—using the primary under normal conditions and switching to the secondary when required. Ivanov (2021) found that embedded digital redundancy significantly reduces recovery time during supply chain disruptions.

Automated Failover Logic at the Middleware Level

In the Technical Infrastructure Layer, middleware and enterprise service buses should embed automated failover mechanisms such as fallback routing and load rebalancing to maintain essential functions during external platform outages. These mechanisms are widely recognized as key to ensuring high availability and fault tolerance in enterprise integration architectures (Papazoglou, 2003; Boyer, 2022). Configurations must be tested regularly through simulation to ensure reliability under failure scenarios. For example, Azure Service Bus enables high availability and regional failover, allowing message workflows to continue during SaaS disruptions (Microsoft, 2024). Embedding such resilience at the integration layer also reduces reliance on individual vendors, thereby mitigating the risks of vendor lock-in (Hezso, 2024).

4.2. Solution 2: Address the Lack of Third-Party Visibility

For retail companies, third-party systems are becoming increasingly complex, spanning areas such as payment, logistics, ERP, and marketing. As observed in case studies, the lack of visibility into third-party systems is one of the major contributors to supply chain security risks in the retail industry.

Structuring Vendor Capability Management

At the Business Process Layer, retail companies should analyse the capabilities of each key third-party partner and integrate this information into the organization's governance processes. These capabilities typically include the vendor's role within the enterprise system, interface integration methods, security classification, and data processing capabilities (World Economic Forum, 2021). By doing so, retailers can clearly define each third-party provider's capability boundaries, interface behaviors, and compliance status, thereby building a governance-oriented enterprise architecture that enhances transparency over third-party data flows.

Visualizing Third-Party Interfaces

At the Information Systems Layer, implementing data flow visualization can help retail enterprises better understand and monitor how data is exchanged with third parties. To achieve this, a retail company can establish an API management platform, which serves to centrally manage all inter-system interfaces (IBM, 2021). By requiring all system calls and data exchanges to pass through this platform, the organization ensures that every data transaction is monitored and traceable. This allows the construction of end-to-end data flow diagrams, making the movement, access, and processing of data across systems more transparent.

Real-Time Monitoring with the ELK Stack

The ELK Stack is a log aggregation platform that consolidates logs from different system modules into a centralized environment for collection, analysis, and visual reporting (Sematext, n.d.). In the context of retail enterprises, data dimensions captured by the ELK Stack may include third-party API call frequency, IP addresses of calling systems, and accessed API paths. This enables real-time monitoring of data activities initiated by external platforms, thereby enhancing operational observability and third-party risk awareness.

4.3. Solution 3: Improving Continuity Through Enterprise Architecture

To address the issue that retail companies may have insufficient consideration of business continuity and supply chain risks in their enterprise architecture design, we propose the following measures.

Third-party dependency contingency plan
In the Business Process Layer, enterprises rely on default external platforms that are always available, and once interrupted, business operations cannot continue normally. To address this issue, enterprises should identify their dependencies on third-party services during the business process modelling stage and design degrade processes and temporary alternatives. At the same time, business continuity planning tools can be used to assess the capabilities of critical links in business processes and design risk contingency plans (Kotusev et al., 2016).

System recovery path
In the Information Systems Layer, enterprises often only connect to one external platform and lack backup systems and switching mechanisms. Once the main system fails, business operations cannot continue. Enterprises can clearly identify which systems depend on external services in the architecture model and refer to ISACA's ISCP model to establish recovery paths and operation plans for each critical system (ISACA, 2021).

Technical architecture design planning
At the Technical Infrastructure Layer, companies often lack unified monitoring and interface management for external platforms. When platform issues occur, it is difficult to identify the cause and quickly switch resources. To address this, companies should establish a unified technical architecture plan, integrate platform, network, and other components into the architecture design, and clarify their relationships and switching paths. For example, the IAF framework can be used to ensure that the infrastructure architecture supports system deployment, scalability, and disaster recovery (Jack Van't Wout & Al, 2010).

4.4. Solution 4: Access Control and Threat Response Optimization

The SolarWinds supply chain attack revealed that many companies lacked robust access control policies for third-party software vendors, which allowed attackers to infiltrate internal systems through trusted suppliers.

Access Control

At the Technical Infrastructure Layer, the integration of the strengths of both Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) could enforce authorization at two levels to ensure access to required resources is properly managed. In the retail industry, many internal departments such as sales, inventory, and marketing use different systems. Also, third-party partners such as delivery companies, payment providers or software providers often connect to internal systems. Therefore, it is important to make sure that these third parties do not have the permission to access the core systems or sensitive data, such as customer information and sales records.

As illustrated in Figure 5, the access control process starts when a user logs in with their credentials. Once authenticated, access permissions are comprehensively evaluated. RBAC gives access based on roles, such as cashier or store manager. ABAC adds more control by checking extra details like the person’s job title, location, and the time they are logging in. RBAC enforces the principle of least privilege by verifying the user’s role and associated permissions, while ABAC adds flexibility by considering multiple attributes such as job position, role, location, and access time. This hybrid model blocks third-party systems from getting into the core data layer unless they have special permission, thereby enhancing security and adaptability in dynamic organizational environments (Jyosthna et al., 2024).

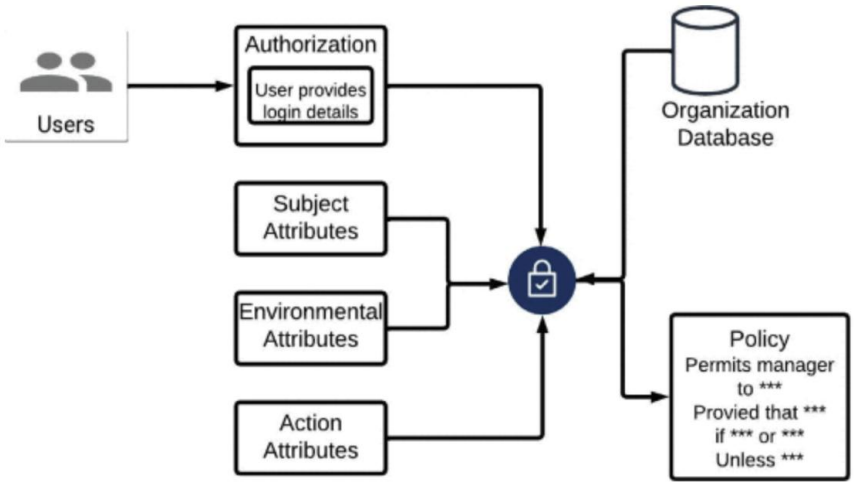

Figure 5 Architecture Diagram

5. Conclusion

This study explored how enterprise architecture (EA) in the retail sector can be adapted to reduce the risk of supply chain attacks (SCA). By looking at two real-world cases—SolarWinds and Blue Yonder—we identified four core architectural challenges: overreliance on a single vendor, lack of visibility into third-party systems, weak business continuity planning, and excessive access privileges granted to third parties. These issues increase the chance of large-scale disruptions when supply chain attacks occur. We discussed solutions across the three key layers of EA: the business process layer, the information systems layer, and the technical infrastructure layer.

This study has some limitations. Firstly, it is based on secondary data and case studies without empirical testing or interviews with industry professionals. Secondly, the analysis mainly focuses on large retailers with high digital maturity. Small or less mature organisations may face different constraints. Lastly, the study focused mainly on security issues, without considering cost, user experience, or operational trade-offs.

This research has several implications. **Theoretically**, it contributes to the discussion of EA as a framework not only for efficiency, but also for security resilience—especially in the context of supply chain attacks. **Practically,** it provides actionable guidance for retail IT managers and architects to enhance system reliability and risk awareness. **For policy,** the findings can support the development of EA governance rules in retail that include external system controls and resilience requirements.

Based on the three-layer EA structure, we make the following recommendations:

At the business process layer, retailers should include continuity planning during process modeling. This involves identifying third-party dependencies, setting up fallback processes, and using redundancy through alternative vendors where needed. Clear definition of partner roles is also important for maintaining business flow during disruptions.

At the information systems layer, companies should adopt a modular design for core functions, such as forecasting and inventory, so that each service can work independently. In addition, visualizing data flows and monitoring third-party APIs through central platforms can improve transparency and system control.

At the technical infrastructure layer, organisations should improve access governance and secure integration. Automated failover logic at the middleware level, unified monitoring systems like the ELK stack, and hybrid access control models (RBAC + ABAC) can help detect issues early and maintain security during system failures.

These recommendations can help retailers improve resilience against supply chain threats without sacrificing operational efficiency. Future research may build on these ideas by testing them in real-world architecture implementations or exploring how EA can support security across different industries.

6. Bibliography

Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021). *Solar Winds Hack: In-Depth Analysis and Countermeasures*. IEEE Xplore. https://doi.org/10.1109/ICCCNT51525.2021.9579611

AP News. (2024, November 26). *Ransomware attack on software supplier disrupts operations for Starbucks and other retailers*. AP News. https://apnews.com/article/ransomware-attack-disrupts-starbucks-morrisons-4281388e1b2d196a5fc10fa0c996c7ed

Blue Yonder. (2023). *Blue Yonder | World's Leading Supply Chain Platform*. Blueyonder.com. https://blueyonder.com/

Boyer, J. (2022). *Reference Architectures - IBM Automation - Event-driven Solution - Sharing knowledge*. Github.io. https://ibm-cloud-architecture.github.io/refarch-eda/introduction/reference-architecture/

Chakraborty, S., Jyothi, N. M., Sushil Lekhi, Dutta, U., Sachin Dasrath Mestry, & Prasad, R. (2023). *Multi Technology Ensembled Optimized Enterprise Architecture for Retail Industry*. https://doi.org/10.1109/ciisca59740.2023.00036

Cloud Exit Strategies: Why and How to Avoid Vendor Lock-in. (n.d.). Www.isc2.org. https://www.isc2.org/Insights/2024/04/Cloud-Exit-Strategies-Avoiding-Vendor-Lock-in

Cloudoptics. (2024, August 16). *Case Studies: Lessons Learned from Major Supply Chain Attacks and How to Apply Them*. Cyber Security - Threat Intel. https://cloudoptics.ai/cybersecurity-updates/compliance/case-studies-lessons-learned-from-major-supply-chain-attacks-and-how-to-apply-them/

CyberScoop. (2024, December 9). *New "Termite" ransomware group claims responsibility for Blue Yonder cyberattack*. CyberScoop. https://cyberscoop.com/termite-ransomware-blue-yonder-disruption/

ENISA. (2021, July 29). *Threat Landscape for Supply Chain Attacks*. Www.enisa.europa.eu. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Fernando, C., & Paiva , L. (2020, July 30). *Future Retail: A Business and Technical Architecture - DZone Integration*. Dzone.com. https://dzone.com/articles/future-retail-a-business-and-technical-architectur

FocalPay. (2025). *Why retailers need a backup solution to protect checkout operations*. Focalpay.se. https://focalpay.se/news/why-retailers-need-a-backup-solution-to-protect-checkout-operations

Fortinet. (2022). *Evolving retailer networks require a new security architecture perspective* [White paper]. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-evolving-retail-networks.pdf

Fortinet. (2023). *SolarWinds cyber attack*. Fortinet. https://www.fortinet.com/tw/resources/cyberglossary/solarwinds-cyber-attack

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Hämäläinen, A., & Nadesan, R. (2022). *Enhancing supply chain cybersecurity with blockchain* (Master's thesis, Halmstad University). DiVA. https://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-47158

Hengky, N., Dazki, E., & Indrajit, E. (2024). Proposed Implementation uses TOGAF ADM and ArchiMate - Enterprise Architecture in Retail Industry. *Sinkron*, *8*(4), 2172–2184. https://doi.org/10.33395/sinkron.v8i4.14052

IBM. (2021, October 6). *API Management*. Ibm.com. https://www.ibm.com/think/topics/api-management

Indrasiri, K. (2019). *Connected Retail Reference Architecture*. Wso2.com. https://wso2.com/whitepapers/connected-retail-reference-architecture/

ISACA. (2021). *Information system contingency planning guidance*. *ISACA Journal, 3*. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

Ivanov, D., Blackhurst, J., & Das, A. (2021). Supply chain resilience and its interplay with digital technologies: making innovations work in emergency situations. *International Journal of Physical Distribution & Logistics Management*, *51*(2), 97–103. https://doi.org/10.1108/ijpdlm-03-2021-409

Jack Van't Wout, & Al, E. (2010). *The integrated architecture framework explained : why, what, how*. Springer.

Jyosthna, P. M., Anirudh Varma Mandapati, Matam Surya Teja, Sachin Kumar Ray, & B.Yashwanth Sai Kumar. (2024). *Enhancing Security and Flexibility with Combined RBAC and ABAC Access Control Models*. https://doi.org/10.1109/iccsp60870.2024.10543482

Kotusev, S., Singh, M., & Storey, I. (2016). *Enterprise architecture practice in retail: Problems and solutions*. *Journal of Enterprise Architecture, 12*(3), 28–38.

lavanyapg. (2024, November 25). *Retail data solutions reference architecture - Microsoft Cloud for Retail*. Microsoft.com. https://learn.microsoft.com/en-us/industry/retail/retail-data-solutions/architecture/ra-retail-data-solutions

Lindner, J. (2025, May 1). *Retail Cybersecurity Statistics Statistics: Market Data Report 2025.* Worldmetrics.org. https://worldmetrics.org/retail-cybersecurity-statistics/

lwsmith10011. (2018, May 15). *Business Architecture for Retail Transformation - lwsmith10011 - Medium*. Medium. https://medium.com/@lwsmith10011/business-architecture-for-retail-transformation-7687ea0863be

Martínez, J., & Durán, J. M. (2021). Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. *International Journal of Safety and Security Engineering*, *11*(5), 537–545. https://doi.org/10.18280/ijsse.110505

Microsoft. (2024). *Enterprise integration with message broker and events - Azure Architecture Center*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/architecture/example-scenario/integration/queues-events

Modern Networks. (2024, November 11). *The Business Impact of IT Downtime*. Modern Networks. https://modern-networks.co.uk/news/business-impact-of-it-downtime

Muhammad Zeeshan Malik, & Bukhari, A. (2023). *Protection Mechanism against Software Supply Chain Attacks through Blockchain*. https://doi.org/10.1109/comtech57708.2023.10164932

New York Post. (2024, November 26). *Starbucks bosses using pen and paper to pay employees after ransomware attack*. New York Post. https://nypost.com/2024/11/26/business/starbucks-using-pen-and-paper-to-pay-workers-after-ransomware-attack/

Papazoglou, M. P. (2013). Service-oriented computing: concepts, characteristics and directions. *Proceedings of the 7th International Conference on Properties and Applications of Dielectric Materials (Cat. No.03CH37417)*. https://doi.org/10.1109/wise.2003.1254461

Psaraftis, E., & Poulimenakou, A. (n.d.). *Digital governance design framework approach in Retail, CPG industry1*.

Semantic Visions. (2025, April 8). *The Blue Yonder Ransomware Attack: A Wake-Up Call for Supply Chain Resilience*. Semantic-Visions.com; Semantic Visions. https://www.semantic-visions.com/insights/the-blue-yonder-ransomware-attack-a-wake-up-call-for-supply-chain-resilience

Sematext. (n.d.). *ELK Stack Tutorial: Getting Started with Log Management*. Sematext. https://sematext.com/guides/elk-stack/

Squillace, J., & Cappella, J. (2024). *Examining How Targeted Cyber Attacks on Critical Supply Chain Networks Can Lead to Economic Collapse and Civil Unrest*. https://doi.org/10.1109/southeastcon52093.2024.10500029

Sridharan, A., & V Kanchana. (2022). *SIEM integration with SOAR*. https://doi.org/10.1109/incoft55651.2022.10094537

Stechynskyi, I. (2025, January 15). *Supply Chain Security Problems: 7 Best Practices to Solve Them | Syteca*. Syteca. https://www.syteca.com/en/blog/supply-chain-security

Supply Chains. (2025, May 8). *The Blue Yonder Cyberattack: A Critical Lesson for Supply Chain Security*. SupplyChains Magazine. https://supplychains.com/blue-yonder-cyberattack/

Tech Monitor. (2025, January 30). *Morrisons struggles with supply chain disruption following Blue Yonder cyberattack*. Tech Monitor. https://www.techmonitor.ai/technology/cybersecurity/morrisons-struggles-supply-chain-disruption-blue-yonder-cyberattack

Tharayil, R. (2025, January 30). *Morrisons struggles with supply chain disruption following Blue Yonder cyberattack*. Tech Monitor. https://www.techmonitor.ai/technology/cybersecurity/morrisons-struggles-supply-chain-disruption-blue-yonder-cyberattack?cf-view

vpadmin. (2023, September 13). *The All-in-One TOGAF Guide*. Visual Paradigm Guides. https://guides.visual-paradigm.com/the-all-in-one-togaf-guide/

Williams, E. (2024). The most prominent cyber security threats targeting industries. *Computer Fraud & Security*, *2024*(4). https://doi.org/10.12968/s1361-3723(24)70016-5

Wolfart, D., Assunção, W. K. G., da Silva, I. F., Domingos, D. C. P., Schmeing, E., Villaca, G. L. D., & Paza, D. do N. (2021). Modernizing Legacy Systems with Microservices: A Roadmap. *Evaluation and Assessment in Software Engineering*. https://doi.org/10.1145/3463274.3463334

World Economic Forum. (2021, March 23). *Principles for Board Governance of Cyber Risk*. World Economic Forum. https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk

WYATTE GRANTHAM-PHILIPS. (2024, November 26). *Ransomware attack on software supplier disrupts operations for Starbucks and other retailers*. AP News. https://apnews.com/article/ransomware-attack-disrupts-starbucks-morrisons-4281388e1b2d196a5fc10fa0c996c7ed