ShopNow

Building a better tomorrow for buyers and vendors (especially vendors)

1. Third-Party Mapping

Third Party	Role	Processed Data	Impact in Case of Compromise	Dominant STRIDE Threats
Stripe (Payment Provider)	Processes payment	**Transactions** (amount, currency, status), **customer identity** (name, email), **billing data**, **payment IDs**, **webhook events**, **tokens/API keys**	**Critical** -> Business and fraud impact. Diverted payments, fraudulent refunds, manipulation of amounts, theft of payment credentials, loss of customer trust, legal and compliance risks.	**T (Tampering)** : Risk of payment amount manipulation or fraudulent refunds.
Hosting / Cloud Provider	Hosts front-end, back-end, database, storage, network, IAM, backups	**Complete application data**: accounts (emails, password hashes), orders, delivery addresses, logs, secrets, configurations, databases, files, backups	Critical : Massive data, full system access. Risk of exfiltration,ransomware,code modification, deletion of db and backup. GDPR sanction, reputation damage.	**E (Elevation privilege)** : IAM takeover = full system compromise.
CDN / Reverse Proxy / WAF	Acceleration , DDoS protection, TLS termination, WAF rules, caching	**Web traffic**, **user IP addresses**, headers, potential cookies. **Certificates TLS**, security rules, access logs	High : interception and alteration traffic. WAF bypass, malicious injection into assets.Leakage of logs/ips, slow website. Risk via misconfiguration (caching sensitive content).	**D (Denial of service)** : Service unavailability directly impacts business continuity
Email provider for transaction	Sends emails: account creation, password reset, order confirmations, security alerts	**Emails**, message content, metadata (IP, device), reset/activation tokens if included, mailing lists	**High**: credible phishing,password resets, reputational damage, email service disruption,leakage of customer lists (GDPR risk).	**S (spoofing)** : Phishing or malicious password reset impersonation
Analytics / Tag Manager	Measures audience, events, conversion, user journey	**Online identifiers** (cookies/IDs), page views, events, sometimes email/customer ID if misconfigured tracking, IP/User-Agent	Medium : Leakage of browsing data (privacy risk) GDPR issues,risk of performance degradation if scripts enabling malicious client-side injection.	**T (Tampering)** : Supply-chain javascript injection risk
Service SMS / OTP 2FA	Sends OTPs, 2FA codes, notifications	Phone numbers, OTP codes, metadata	**High** if 2FA-dependent: bypass of 2FA via SIM swap/routing attack, unavailability = login impossible, fraud if OTP intercepted	**S (Spoofing)** : OTP interception or SIM swap leading to account takeover.

2. Supply Chain Risks Analysis

2.1 Stripe

Stripe is a business-critical dependency, as it directly processes payment transactions. Any compromise would have an immediate financial, regulatory, and reputational impact.

a - Technical Risks

API Key Compromise : If a Stripe API key is leaked, an attacker could:
- Create fraudulent transactions
- Access transaction metadata
- Manipulate refunds or customer billing information

This represents a critical risk affecting integrity and confidentiality, with direct financial losses.
Webhook falsification or Spoofing : If webhook signatures are not cryptographically validated, an attacker could simulate a “payment successful” event, leading to order validation without actual payment. This directly compromises transaction integrity.
Manipulation of transaction flows : A misconfigured TLS setup could allow Man-in-the-Middle attacks, enabling interception or alteration of transaction data, including payment amounts or currencies.
Service unavailability : Stripe down = payments could not be processed leads to financial losses

b - Contractual Risks

Insufficient SLA : Weak availability guarantees reduce ShopNow’s ability to enforce service continuity or compensation during outages.
Weak incident notification clauses : Delayed notification of a security incident can significantly increase the Mean Time to Detect (MTTD), worsening the overall impact of a breach.

c - Compliance risks

Data Transfer outside the EU (GDPR) : Stripe may rely on subcontractors or infrastructure outside the EU, creating uncertainty regarding data localization and lawful transfer mechanisms.
PCI-DSS non compliance : Although Stripe is PCI-DSS certified, ShopNow remains responsible for the security of its integration. A misconfiguration could result in non-compliance despite using a certified provider.
Data Storage : Retention policies at Stripe may not fully align with ShopNow’s internal data minimization requirements

2.2 CDN

The CDN distributes client-side resources and therefore represents a high-risk supply chain entry point impacting end users directly

a - Technical Risks

Malicious injection (XSS) : If the CDN is compromised, malicious JavaScript can be injected into legitimate assets, enabling large-scale data exfiltration. This risk is particularly severe due to its stealth and scale.
TLS misconfiguration : Support for outdated protocols or weak cipher suites may allow traffic interception or downgrade attacks.

b - Contractual Risks

Lack of content integrity : Without contractual commitments on content integrity, ShopNow has limited recourse in the event of asset manipulation.
Insufficient availability SLA : CDN downtime directly affects site accessibility, impacting revenue and potentially leading to repudiation disputes.

c - Compliance risks

Storing sensitive data in areas not compliant with GDPR : Misconfigured dynamic endpoints could result in sensitive data being cached and distributed across non-compliant regions, violating GDPR requirements.

2.3 Cloud Provider

The cloud provider hosts core backend services and databases, making it a systemic risk.

a - Technical Risks

IAM privileges escalation : Over-permissive roles or misconfigured access controls can allow attackers to escalate privileges and compromise multiple services
Hypervisor Compromise : A breach at the virtualization layer could result in a massive exposure of personal data and backend systems.
Unintentional network exposure : Misconfigured security groups or firewalls may expose internal services directly to the internet.

b - Contractual Risks

Ambiguity in the share responsibility model : Misunderstandings regarding security responsibilities can leave critical controls unmanaged.
Insufficient security commitments RPO/RTO : Weak recovery guarantees increase business continuity risk in case of incident or outage.

c - Compliance risks

Data residency issues : Data may be stored or backed up in regions that do not meet regulatory requirements.
Missing certifications (ISO 27001) : Lack of recognized certifications (ISO 27001, SOC 2) reduces assurance regarding the provider’s security maturity.

2.4 Email Provider

Email services directly impact customer trust and brand reputation.

a - Technical Risks

API token leak : Compromised tokens enable phishing campaigns sent from legitimate domains, significantly increasing success rates.
Misconfugration of SPF, DKIM, DMARC : Weak email authentication enables spoofing and impersonation attacks.
Exposition of logs containing customer data : Logs may store email addresses or order metadata, creating an indirect data leakage risk.

b - Contractual Risks

No commitment of data encryption : Emails stored unencrypted at rest increase the impact of a provider-side breach.
No active notification in cas of data breach : Late breach detection limits ShopNow’s ability to react and notify users in compliance with GDPR.

c - Compliance risks

Unregulated international data transfer : Transfer data over restricted areas may result in GDPR violation.
Misuse of data for marketing purposes : Customers data are used for their own purposes and are not suppressed accordance with GDPR

2.5 Analytics /Tag Manager

Analytics tools execute third-party code in the client’s browser, making them a high-impact but often underestimated risk.

a - Technical Risks

Excessive data collection : If the main account is compromised an attacker can inject malicious script to capture payment data or exfiltrate them.
External script dependencies : If the provider’s servers are compromised, ShopNow becomes a secondary delivery for malicious code..
Unavailability or slowdowns : This compromission could lead to an impact on performance and slowdowns with front-end.

b - Contractual Risks

Data reuse : Some providers can use the collected data for aggregate statistical purposes, so ShopNow could lose the control of the data.
No guarantees of the integrity of the scripts : Absence of strong contractual protections for account security increases supply chain exposure.
Late notification in case of compromise : Can conduct an invisible attack lasting several days.

c - Compliance risk

GDPR and consent : Cookies placed without valid consent and failure to comply with CNIL requirements
Transfer apart from EU : Data hosting and processing in inadequate countries
Abusive behavior analysis : Behavior analysis that could be intrusive.

2.6 Service SMS

The SMS provider directly impacts identity security and Zero Trust enforcement.

a - Technical Risks

SMS interception or redirection : If the telecom operator is under attack the OTP could be intercepted and bypass the MFA.
Compromise of the SMS service API : Send massive fraudulent SMS.
Service unavailability :OTP delivery failures may prevent administrators from accessing critical systems.
Mismanagement of the logs : Storing the OTP in plain text and leaving the PII exposed.

b - Contractual Risks

Insufficient SLA (OTP delivery) : No OTP delivery time guarantee
No commitment of data encryption : Messages stored unencrypted increase breach impact.
Lack of transparency with subcontractors : Complex chains involving multiple operators reduce visibility and accountability.

c - Compliance risks

Sensitive personal data : Phone numbers and authentication metadata require heightened protection.
Excessive email storage : Non alignment with the data minimization policy.
International transfer via non EU operators : Delivery to operators that are outside the EU (GDPR)

3. Risk Mitigation Measures

For better enforcement of contractors, third-party providers and payment solutions providers, an understandable stack but also technical and support guarantees are in order, as to let ShopNow get up and running after a major outage outside our departments reach.

As for now, third-parties and service providers must offer these minimum levels of service :

Contractual measures

For the remaining section, ShopNow's employees and associates, hereby named "the client", will enforce relations with third-party vendors/contractors/parts - namely "the partner" - through legal, business and technical teams to the best of everyone's knowledge, expertise and approbation power.

Security clauses

The partner will provide services with which the best security levels are in place. The stack will be audited independently and reports will be made readable for the public, or at least the client for entrusting processes.

ISO certifications will be mentioned on the partner's website whenever applicable and be validated by a pertinent entity responsible for their distribution and enforcement.

Audits

Audits will be regularly conducted within the partner's assets to ensure the solution's security at heart, and an additional audit will be conducted by an independent structure about security and resilience of the connection between the client's and the partner's solution.

The providing of recent and independent penetration test reports for software and/or infrastructure will occur **every 2 years**.

SLAs

The partner will do his best to provide a consecutive and uninterrupted service for the client's benefit. To strengthen this collaboration, the partner engages himself to have at least :

- A 99,99% uptime for a running fiscal year.
- A 24h/24 7d/7 response support for at least the lowest support solution (email/text message) with an answering time of **less than 1 hour**.
- A Technical Account Manager for direct support during business hours with an answering time of **less than 15 minutes**.
- (if applicable) A least one replica of data outside the current country of main data hosting with fail-over connection.

Incident notification

The partner will respect a contractual delay of maximum **48 hours** to warn the client about (but not restrained to) any security, technical, contractual, business problem, or anything that could impact the quality of service provided by the partner.

In case of major outage, hacking process or anything that could severely impact production, client's customers confidentiality or anything related to a severe incident, the partner will inform, by direct lines of communication or dedicated warning instance or by any means **as soon as detection occurred**, so the client may take action on his side.

Technical controls

Network segmentation

The partner will provide technical service from inside the partner's own network, with all securities that can be provided. The only outside bounds and bridges will be taken to a minimum as to provide services without providing security vulnerabilities.

The networks of the client and the partner will not - unless explicitly specified so by the two parties involved - will not overlap, nor being placed in the same region or the same infrastructure.

Limited tokens

Active sessions between the partner's and client's resources will be performed through a secure and temporarily defined manner using session tokens, with clear identification of both parties' monitoring solutions, without any possibility for third-party benevolent or malicious actors to identify scope, resources or actors involved in the process, through the principle of open secret sharing.

Any token will be affected to a dedicated and restricted pipeline, following the principle of "for each door it's own key", meaning that every token will be short-lived for a specific task, without possibility to assign one to another task.

Restricted scopes

The partner will have access to resources by name only, and from the partner's own network. Every access will be monitored on both ends, including active sessions and actions as to build any possible timeline of good or bad actions.

Key rotation

If applicable, every persistent key access will be changed on both ends every **3 months** at most, by automated or manual action. If any secrets must be shared, both parties agrees on using ephemeral, encrypted and confidentially shared services such as PrivateBin (or any tool offering the same level of privacy, confidentiality and security) with "burn after" policies at first reading and 1 hour lifetime on encrypted zero-knowledge servers.

Call monitoring

Every call about technical issues must be monitored by the partner's relevant teams, as to track the average response time, answer duration and good technical assessments. A rating will be provided bi-annually for the answer teams and actions must be taken for lack of answer time.

PS : Avis personnel. Je sais que c'est une pratique demandée par les clients, et imposée d'office dans les centres d'appel. Evidemment, pour les besoins de l'exercice je les mets tels quels. Mais c'est un traitement inhumain et cruel. Les employés sont au téléphone toute la journée avec des gens désagréables, et assurer un service de qualité avec un temps d'appel inférieur à 15 minutes et une résolution complète en moins de 5 minutes, avec sanctions en cas d'échecs alors qu'on a 6 heures d'appel non-stop sans pause pipi dans les pattes… ça mériterait la pendaison pour les patrons qui imposent ça. Juste un coup de gueule.

Organizational controls

Periodic third-party reviews

On an annual basis, the client and the partner will meet to discuss the full perimeter of the current contract, updating, adding or deleting every clause that should require so. Discussions will also include the client's technical specifications updates and infrastructure changes, as well as new commercial propositions the partner may propose.

On this annual basis, the partner will be audited to ensure that every technical and contractual content and appendixes are respected and enforced as discussed. Every modification will be logged in a transcript and stored for an unlimited amount of time.

Traditional questionnaires about internal controls, including but not limited to Cloud Security Alliance's CAIQ or SIG Core will be taken to assess the partner capacities.

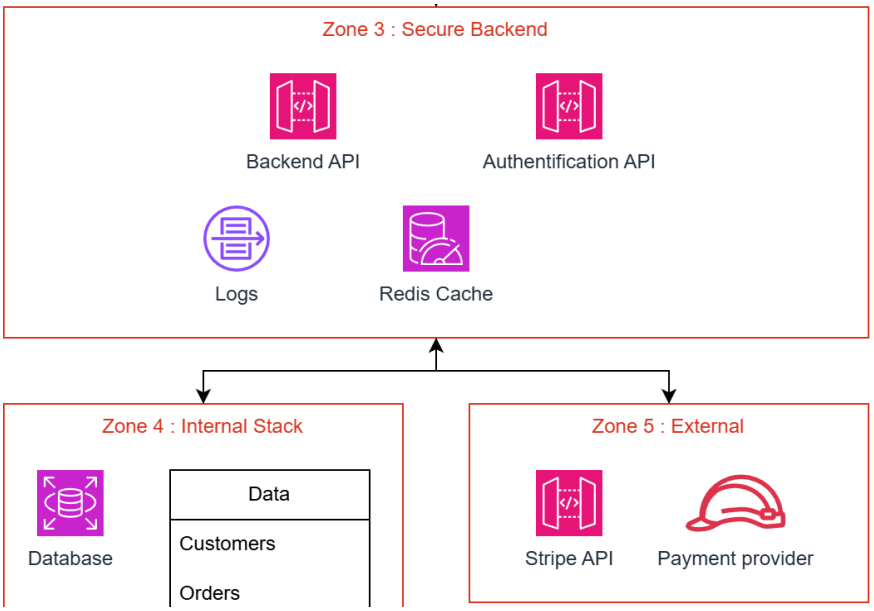
Strict due diligence processes

Before each execution of the present contract, the client and the partner will discuss the full extent of the partner accesses, rights and capacities :

- The data accessible will never contain any Personal Identifiable Information (PII) of the final client's customers, nor their Financial or Intellectual data and/or property.
- The client's intellectual properties will never be of any part of the partner portfolio. The only elements the partner will remain in charge and possession of is but not limited to : the data, IT resources, network capacities or proprietary software solutions or any solution the partner gives access to the good execution of the present contract.
- The partner accepts that any data, resource or software solution may not lock the client from moving to another business partner, if the present partner lacks to fulfill his part of the contract. The partner is informed that the contract may be broken by his part, would the client lack to fulfill his proper part of the contract.
- The partner will provide a complete list, as well as their professional insurances of any forth-party, and submit them to the client approbation.
- Least, the partner will provide a full report on insurances, financial stability independent checking, Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP) so the client may put his trust in the right place.

4. Zero-Trust integration

The current stack state gives third-parties uncontrolled access to the backend zone :



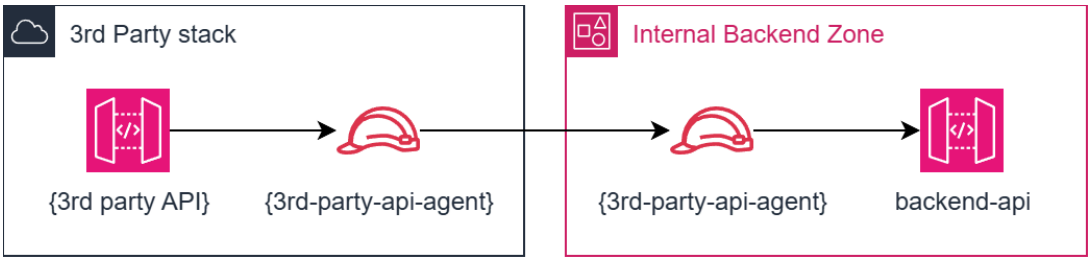
No third-party should have more access than strictly necessary.
Any third-party should provide beforehand :

- A full, exhaustive list of requirements for the execution of the solution, or at least a complete and exhaustive document base.
- A fully named list of resources that will access internal resources
- A fully comprehensive High Level Design (HLD) guide of the solution technical deployment (on-premise, hybrid, cloud-based elements)

Any interaction will be logged on both parties monitoring solutions, including resources accessed, actions done and any geolocalisation indicator (such as IP address).

Any authenticated action will take place from the perspective of a service account whose role will be “assumed” by a named and non-moving resource from the third-party stack. This way, impersonation and actions shouldn't be extended by any malicious or non-caring actor.

An up-to-date version of any third-party relation would resemble this :



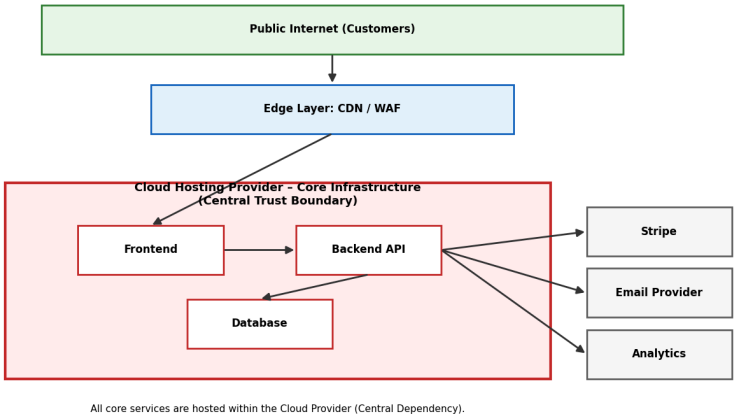
An IaC piece of deployment should look like this :

```
data "aws_iam_policy_document" "assume_role_policy" {
  statement {
    actions = ["sts:AssumeRole"]

    principals {
      type        = "AWS"
      identifiers = ["arn:aws:iam::{PARTNER_ACCOUNT}:role/3rd-party-api-agent"]
    }
  }
}

data "aws_iam_policy_document" "api_push_policy" {
  statement {
    actions   = ["execute-api:Invoke"]
    resources = ["arn:aws:execute-api:region:account-id:api-id/*/POST/*"]
  }
}

resource "aws_iam_policy" "api_push" {
  name   = "3rd-party-api-push-policy"
  policy = data.aws_iam_policy_document.api_push_policy.json
}

resource "aws_iam_role" "internal_role" {
  name               = "3rd-party-api-agent-internal"
  assume_role_policy = data.aws_iam_policy_document.assume_role_policy.json
}

resource "aws_iam_role_policy_attachment" "api_attachment" {
  role       = aws_iam_role.internal_role.name
  policy_arn = aws_iam_policy.api_push.arn
}
```

Therefore, no action will be taken directly, only “passed on” with the strict minimal requirements.

5. Most Critical Third-Party Risk for ShopNow

The cloud hosting provider (infrastructure provider) represents the most critical third-party risk for ShopNow.



The other service providers handle specific business functions (payments or email notifications for examples). The hosting provider has full access to the core infrasatrcture including :

- Application servers (front-end & back-end)
- Databases containing customer account and order history
- Storage systems and backups
- Secrets,API Keys and environment configurations
- IAM

If this provider were compromised, the consequences would be the most critical and catastrophic for this reasons :

- Total data breach (credentials, PII, history transaction)
- Service disruption (complete unavailability of the platform)
- Data tampering (modification or deletion of records)
- Ransomware risk affecting production with backups
- Privilege escalation enabling attackers to pivots across all the systems

If we apply the STRIDE perspective, the dominant threats are :

- **Elevation of Privilege (E)** compromise of IAM roles or admin accounts
- **Information Disclosure (I)** large-scale data exfiltration
- **Tampering (T)** alteration of application code or databases
- **Denial of Service (D)** infrastructure-level outages

From a Zero Trust perspective, this provider must be treated as an external and non-trusted zone. Apply strong authentication mechanisms, strict least-privilege access controls, continuous monitoring, key rotation,network segmentation, and contractual safeguards.

Since the entire application stack is hosted within this provider’s infrastructure, it constitutes the core backbone and central trust boundary of ShopNow, meaning that any compromise at this level impacts the entire ecosystem.

6. Actions that must be taken immediately

These actions must be implemented in the short term (0-3 months) as they directly reduce exposure to identified supply chain risks.

6.1 - Enable automatic rotation of Stripe API keys

Reducing the validity period of an API key limits the risk of compromise, especially for sensitive services like Stripe. An exposed key can be used to create fraudulent payments, access data, or modify critical settings. To mitigate this risk, regular key rotation (less than 90 days) is necessary, keys should be stored in a secure secrets manager, and their updates should be automated within CI/CD pipelines. Old keys should be deleted immediately after the transition, and any suspicious activity should be logged. This approach significantly reduces the risk of leaks and aligns with a Zero Trust model by prioritizing ephemeral credentials.

6.2 - Restrict API scopes to the bare minimum

Applying the principle of least privilege means limiting each API key to the bare minimum required. Many integrations mistakenly use keys with full access, which amplifies the damage in the event of a breach. Therefore, keys should be separated by environment (dev, staging, prod) and dedicated keys should be created for specific uses: read-only, payment creation, or webhook validation. Global keys should be prohibited, and each use case should be clearly documented. This approach significantly reduces the potential impact of a compromise by restricting the privileges available to an attacker.

6.3 - Implement cryptographic validation for webhooks

The goal is to prevent the falsification of payment confirmations transmitted via webhook. Without signature verification, an attacker could simulate a "Payment successful" message and validate an order without any actual payment. To prevent this, the HMAC signature sent by Stripe must be verified, compared to the webhook secret key, and any invalid request rejected. Failed attempts must be logged, and a timestamp control added to block replays. These measures guarantee the integrity of the payment flow and prevent direct fraud.

6.4 - Implementing Subresource Integrity for the CDN

The goal is to prevent the execution of modified scripts on a compromised CDN. An attacker could inject malicious JavaScript to steal sensitive data. Therefore it’s necessary to add the integrity attribute with SHA-256 hash enable script CSP, block unsigned inline scripts and regularly check hashes. Even if the CDN is compromised the browser will block any altered script, ensuring client-side protection.

6.5 - Add SIEM rules specific to third-party calls

The goal is to quickly detect any suspicious activity related to external services like Stripe. A supply chain attack can go unnoticed without proper monitoring. Therefore, SIEM alerts must be configured for spikes in API calls, multiple webhook failures, unusual IP addresses, an increase in OTPs sent, or repeated errors. These rules significantly reduce the MTTD in the event of an incident.

6.6 - Review the SLAs and incident notification clauses

This point aims to ensure a rapid and legally compliant response in the event of a breach. A notification delay increases the risks of non compliance and operational impact. Contracts must include a notification period of less than 48 hours, certified security guarantees, availability of at least 99,9%, monitoring of subcontractors and the right to audit. This reduces legal risk and improves crisis management

6.7 - Conduct a quick audit of critical suppliers

The goal is to assess the actual security maturity of technology partners. Many are integrated without prior verification. Therefore, it’s necessary to send a security questionnaire (ISO 27001, SOC 2), analyze public reports and classify suppliers according to their criticality. This process helps prioritize risks and include third parties in overall security governance.