A deep dive into SECURITY PRACTICES at Talon.One

Talon.One

Intro:
Talon.One's security vision

Since the start, Talon.One was built with enterprise-grade security in mind. From compliance to data encryption, we are designed to meet the highest security standards, and proactively protect client and user data. This report provides a comprehensive look at our security practices and how they protect our customers across the globe.

Talon.One was founded and has its headquarters in Germany, home to some of the most stringent data privacy laws in the world. **Trust** and **transparency** are the foundational pillars on which our security strategies are built and executed.

With a robust system in place to manage risks related to information security, Talon.One sets the bar for security standards in the promotion and loyalty software space, and clients know they can rely on us for maximum information security and data protection. That's why Fortune 500 companies including Live Nation Entertainment and Kraft Heinz trust Talon.One with their loyalty and promotion strategies.

Looking for more information on our security practices? Please reach out to **infosec@talon.one**, and one of our security team members will be in touch.

ABOUT TALON.ONE

Talon.One is an API-first loyalty and promotion engine that helps enterprises deliver data-driven, effective and personalized promotions. Talon.One allows users to click together simple rules to build rich promotional campaigns at scale, across both in-store and online channels.

Talon.One's security checklist

Infrastructure and platform security

Security structure

- Autoscaling across three availability zones
- Ensuring uptime and resilience with managed Kubernetes Cluster
- Third party management policy

Platform security

- Data encryption in rest and transport
- API tester to troubleshoot campaigns
- IP restrictions and whitelisting
- Audit logs
- Separate live and sandbox environments

Operational and organizational security

Operational security

- Business continuity and disaster recovery
- Host and network security
- Malware protection
- Vulnerability management and penetration testing
- Incident management

Security compliance and certificates

- ISO 27001
- SOC II
- GDPR
- CCPA

Product security

Access and permissions

- Enforced Single Sign-On (SSO)
- Sophisticated user permission schemes
- Role-based control and access (RBAC)
- Two-factor authentication

Promotion and loyalty fraud detection and protection

- Identity hashes
- Issue controls
- Budget controls
- Transfer controls
- Geolocation controls
- Receipt controls
- Monitoring and resolution

Security structure

Data center security

The Talon.One platform, hosted globally on Google Cloud Platform, ensures the implementation of top-tier security measures aligned with the red security level. Our data center infrastructure is designed with Virtual Private Clouds (VPCs) to provide a secure, isolated environment for our operations. This is further enhanced by hosting private Kubernetes clusters on these VPCs, featuring autoscaling across three high-availability zones for reliability and performance. Additionally, we maintain strict network security protocols, including fixed IP addresses and IP whitelisting, and align with Google Cloud's rigorous certification and compliance frameworks, including ISO and SOC II standards.

Database security is a cornerstone of our approach, with Aiven database clusters hosted within the internal VPCs to fortify against external threats. These clusters are supported by point-in-time recovery (PITR), regular security upgrades, and daily backups, ensuring data integrity and availability.

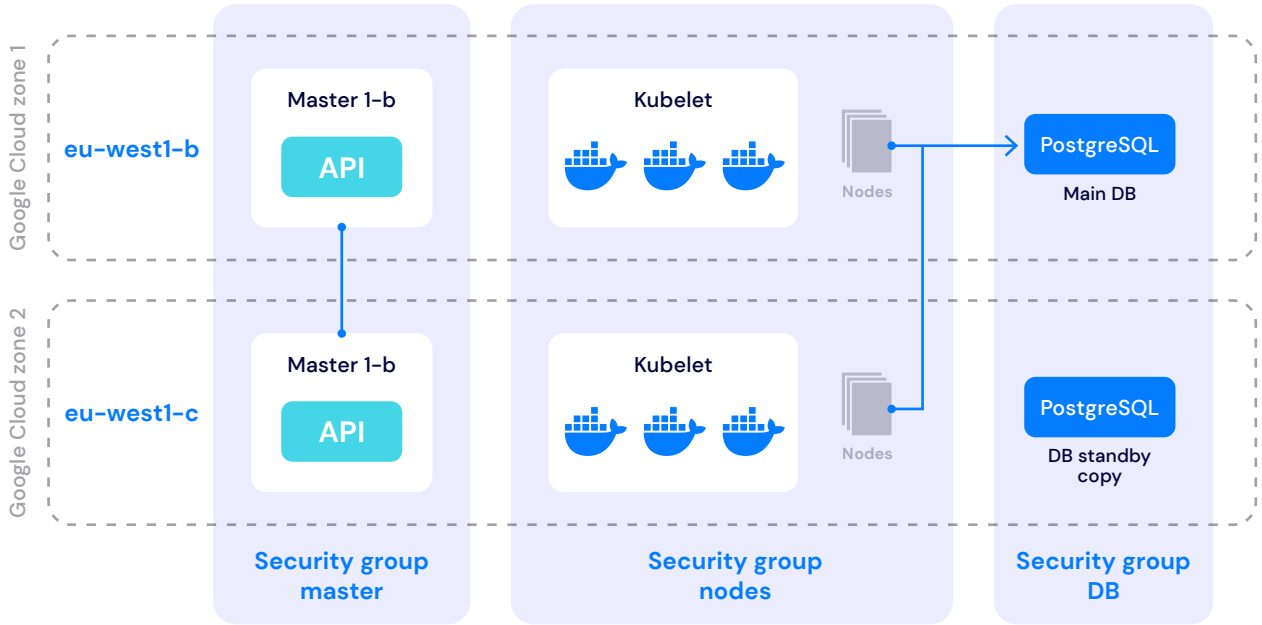
Server infrastructure security

Using a Kubernetes cluster, we span three Google Cloud availability zones in each cluster, guaranteeing high availability for our services. This includes synchronized masters in each region to maintain integrity and accuracy.

Our cluster is equipped with automated health checks, ensuring continuous monitoring of hardware and software.

For our database servers, we employ an active-active setup with standby copies in a separate availability zone. In the event of a critical failure, automatic handover ensures seamless continuity of service. Additionally, our backup mechanism allows us to restore data to any point within the last seven days - which can be extended further if required.

Each customer instance is securely stored within its own Virtual Private Cloud (VPC), ensuring isolation and safeguarding sensitive data.



With our Multi-Region Fallback Database, our clients experience unparalleled availability and data resilience across multiple regions, providing a reliable and scalable solution for critical applications. For instance, if a server hiccup happens in Europe, the system instantly flips over to a backup server in another region without missing a beat. This means your customers can keep shopping without interruption.

Third-party management policy

Talon.One's third-party management policy ensures the protection of the company's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers. It also maintains an agreed level of information security and service delivery in line with supplier agreements.

Access and permissions

Authentication and authorization

Talon.One's platform supports Single Sign-On with SAML 2.0. If a client decides not to use SSO, we employ two-factor authentication (2FA) for them. All remote communications occur over an encrypted tunnel, accessible only via a two-factor authentication, with authorized devices and specific configurations. Unique user IDs are required to gain access to all systems and applications.

Our SSO Automatic Provisioning and Deprovisioning feature manages account access, enhancing security and efficiency. This is how the process works for new Talon.One users:

1. **User authentication**
   A new user logs into the system using SSO credentials verified by an Identity Provider (IdP) like Okta, OneLogin, or Azure AD.

2. **User profile retrieval**
   After authentication, the IdP fetches the new user's profile from a central directory.

3. **Application mapping**
   The IdP correlates user profile attributes to required data in various company applications and services using predefined mappings.

4. **User data sharing**
   The IdP automatically shares relevant user attributes with target applications, enabling account creation, role assignment, and profile data population in Talon.One platform.

5. **Application access**
   With SSO credentials, the user gains access to applications, with roles and permissions set based on IdP-provided data.

And when an employee leaves the company or their role changes:

1. **User departure or trigger**
   Deprovisioning can be manual by the client's HR or IT, or automatic based on predefined conditions.

2. **Revoking application access**
   The IdP initiates deprovisioning by revoking the user's access to all applications.

3. **Data archiving or deletion**
   User data is archived or permanently deleted based on company policy and legal requirements.

4. **Notification**
   HR, IT, and app admins receive notifications to ensure a smooth transition.

5. **Audit and reporting**
   The entire process is logged and audited for compliance and security, with reports generated for oversight.

Permission and user role control

Talon.One's product roles and permission protocol is designed with the "least privilege" principle in mind. This principle states that users are only granted the level of access absolutely required to perform their job functions. Talon.One's primary method of assigning and maintaining consistent access controls and access rights is through the implementation of Role-Based Access Control (RBAC). Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

Logging

The ability to track and audit system activities and data access is crucial for evaluating the right access controls and data rules. Talon.One carefully chooses secure login measures such as two-factor authentication (2FA) that match the sensitivity of the data and the potential risk of unauthorized access, considering the overall security and access control setup.

Talon.One platform security

Encryption management

Talon.One has selected an IT infrastructure that can be securely managed. All data transmitted is encrypted with HTTPS (TLS 1.2+). HTTPS is enforced for all communications to Talon.One and unencrypted traffic is rejected. Al data at rest is protected by hard disk encryption using AES-256 in CTR mode with HMAC-SHA256 for integrity protection.

IP restrictions and whitelisting

IP whitelisting is a crucial feature in Talon.One's security vision as it enhances network security by restricting access to trusted IPs only. After our clients create their campaigns, Talon.One can whitelist their IP addresses, meaning only pre-approved and verified IP addresses can interact with the critical systems and sensitive data. More information on how to do this can be found here.

API security

Talon.One's platform hosts two types of APIs, making it highly scalable and robust: Integration API, which is used for real-time/ live integrations (i.e. checkout, ecommerce interactions, etc.) and Management API, which is used for configuration of campaigns, generation of coupons, management of promotions as a general rule, and more.

In both cases, unique identifiers are applied to every API call and response. Plus, with Talon.One's Management API Keys, our customers can control the level of access they want to provide to their employees. Also, Talon.One's API tester enables our customers to troubleshoot a campaign without the need to rely on any external software.

Separation of live and sandbox environments

Talon.One offers a sandbox mode where you can test your campaigns before release. You can also start by releasing small-scale incentives (e.g., for a particular location or store only) to check your campaigns for any potential weakness without risking burning the whole promotional budget on the first campaign.

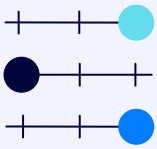
Fraud detection and protection

Talon.One has robust identity hashes and security measures in place to detect and prevent all forms of promotions fraud including misuse of personal information, automated scripts or bots depleting online promotions, coupon farming operations, account takeovers, and the distribution of counterfeit offers.

Our built-in product features prevent fraudulent activities in multiple ways, keeping your loyalty programs and promotions campaigns safe and secure:

Issue controls

Set budgets on device ID or IP address as a unique identifier, ensuring each device/ IP only gets a limited number of loyalty points for each purchase.



Transfer controls

Set criteria around what loyalty points you can transfer and when, e.g. only being able to transfer spend points and not welcome offer points.

Geolocation controls

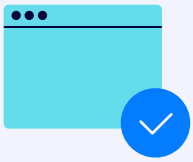
Make sure only customers who are in a specific location can access your promotions.

Receipt controls

Set per-profile budgets on the number of point receipts customers can receive, e.g. only 1 point gift receivable per week.

Monitoring

Set up alerts and monitoring to flag any suspicious activity, in real-time.



Resolution

See what went wrong (including when and by who) through campaign audit logs.

Security in operations and development

Business continuity and disaster recovery

Our business continuity plan identifies Talon.One's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for our clients.

Talon.One's database servers have a standby copy in a second availability zone with automatic handover in the case of catastrophic failure and a separate backup mechanism allowing us to go back to any point in time within the last 7 days. A disaster recovery test, including a test of backup restoration processes, is performed on an annual basis.

Talon.One has never had to revert to a full backup in a production environment for any customer due to its highly resilient setup.

Host and network security

Our implemented business continuity plan identifies Talon.One's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for our clients.

Talon.One's database servers are supported by a separate backup mechanism allowing us to go back to any point in time within the last 7 days. A disaster recovery test, including a test of backup restoration processes, is performed on an annual basis.

Monitoring

Through real-time analysis of network traffic, system logs, and user activities, we can promptly detect and respond to suspicious behavior or anomalies that may indicate a potential threat. This proactive approach allows us to identify and mitigate security vulnerabilities before they escalate into full-fledged attacks, minimizing the risk of data breaches and system downtime. Additionally, continuous monitoring enables us to maintain optimal performance and reliability by quickly addressing any operational issues or performance bottlenecks.

Vulnerability management and penetration testing

Talon.One has a regular process for vulnerability scanning on servers, workstations, network equipment and applications, as well as for remediating newly discovered security vulnerabilities on servers, workstations, network equipment and applications.

We also undertake independent penetration tests of our platform by an external third-party at least once a year.

Malware prevention

Safeguarding against malware is a top priority. Through regular updates, firewalls, antivirus software, and employee training programs, we ensure that our processes are strong and up-to-date.

Security compliance and certifications

ISO 27001 is an information security standard created by the International Organization for Standardization (ISO), an independent organization dedicated to ensuring consistency and quality in technology processes. Conforming with the ISO 27001 means Talon.One has a robust system in place to manage risks related to information security, covering people, policies and technology.

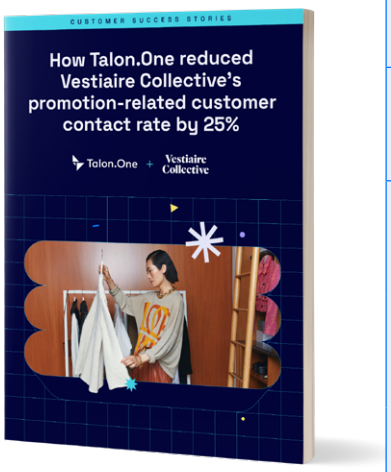
Talon.One fully meets **European Union's General Data Protection Regulation (GDPR)**, guaranteeing that our data handling practices adhere to the highest standards of privacy and protection. We prioritize transparency, security, and consent in all aspects of data processing, aligning with the regulations set by the EU.

SOC II Compliance refers to adherence to the Service Organization Control 2 framework, which evaluates an organization's controls related to security, availability, processing integrity, confidentiality, and privacy of customer data. Talon.One meets SOC II standards, demonstrating our commitment to top-level security practices. By undergoing rigorous audits and assessments, we ensure that our systems and processes meet or exceed industry benchmarks for data protection and operational reliability.

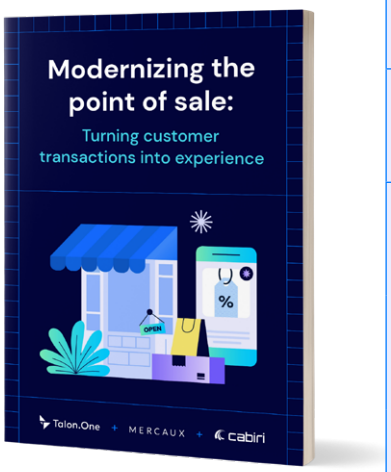
CCPA compliance consists of rules that organizations must adhere to in order to safeguard the data privacy rights of California residents. Talon.One is fully CCPA-compliant, demonstrating complete transparency regarding its data collection and usage practices, while implementing rigorous security measures to protect user data.

RELATED RESOURCES

The Personalization Playbook: Strategies for IT leaders



How Vestiaire Collective cut promo-related customer contact by 25% with Talon.One



Transforming the point of sale with a composable strategy