webfleet

Certified information security and data privacy telematics

TÜV SÜD ISO 27001

ISO 27001

Certified Information Security Management System

www.tuv-sud.com/ms-cert

BRIDGESTONE

Solutions for your journey

The purpose of this whitepaper is to provide detailed information to our business partners, interested parties and customers regarding the ISO/IEC 27001 certified Webfleet Telematics Service Platform. It contains the level of information required to support all interested parties with due diligence and risk analysis activities, as well as support data protection officers and work councils with their data privacy initiatives.

At Webfleet, we're committed to the security of information and data privacy.

We invest continuously in our engineering, proven technologies, processes and people to ensure that we can always provide the most reliable telematics service on the market.

The power of Webfleet Telematics Service Platform

ISO 27001 INFORMATION SECURITY CERTIFIED
Our service platform and our mature processes have been certified ensuring that our customers benefit from the highest level of protection for information security and data privacy.

HIGHEST STANDARD EV SSL ENCRYPTION
Secure, encrypted login and data transfer to the service platform. You can trust your data is safe and secure.

LOCAL INSTALLATION
Nationwide and international installers.

FIRST CLASS SUPPORT
from local resellers and system integrators.

APP CENTER

APP CENTER
Proven integrations and add-on apps available in App Center.

It's no surprise we're a global leader in fleet management and telematics.

As one of the world's largest providers of telematics services, continual investment in our service is important. We're always improving to make sure that we are the best partner for your business – now and in the future.

Content

1 INFORMATION SECURITY MANAGEMENT SYSTEM

What is ISO/IEC 27001?

The ISO/IEC 27001 international standard was developed in order to provide a standard means of protecting information assets. Information is defined as any physical or virtual asset which can be deemed valuable to the organisation. Our strategy for the continued protection of these assets as well as the data of our customers, are covered through our Information Security Management System (ISMS).

As a management system, it ensures that all processes and information assets are regularly reviewed holistically throughout the organisation, and aligned to the Webfleet baseline for acceptable risk.

> *"The ISO 27001 certification underpins that we're in complete control of our processes and even more importantly, that our client data is in safe hands, which is crucial for us providing a business critical fleet management "Software as a Service (SaaS) solution."*
>
> **Jan-Maarten de Vries,**
> President of Fleet Management Solutions,
> Bridgestone Mobility Solutions

Our ISMS certified scope

Our Information Security Management System (ISMS) covers all of our critical business processes necessary to secure the informational assets related to the Webfleet Telematics Service Platform. This includes the architecture, engineering, quality assurance and IT services provided to the Webfleet B.V at our Technology Headquarters in Germany, as well as our secure data center co-locations located within the European Union. This is in accordance with the ISO/IEC 27001 standard and implemented as detailed in our Statement of Applicability.

We implemented an ISO/IEC 27001 compliant management system in 2012, and have maintained this certification through yearly internal and external assessments to ensure our compliance with this international standard. The certification is one of the most recognised management standards in the field of information security management incorporating or exceeding most of the controls recommended by PCI or ISAE 3402 standards, which we believe makes Webfleet a best-in-class provider of Software as a service (SaaS) for fleet management.

The certification can be verified on the certificate/client directory of the certification body TÜV SÜD.

2 INFORMATION SECURITY POLICIES

Webfleet is committed to the security of the Webfleet Telematics Service Platform, as well as to that of our organisation. This includes all information assets involved in the development, testing, and operations as stated in our ISMS scope.

This commitment is outlined in our Bridgestone Group code of conduct:

Go to Bridgestone Code of Conduct

and in our privacy policy:

Go to Webfleet Privacy Policy

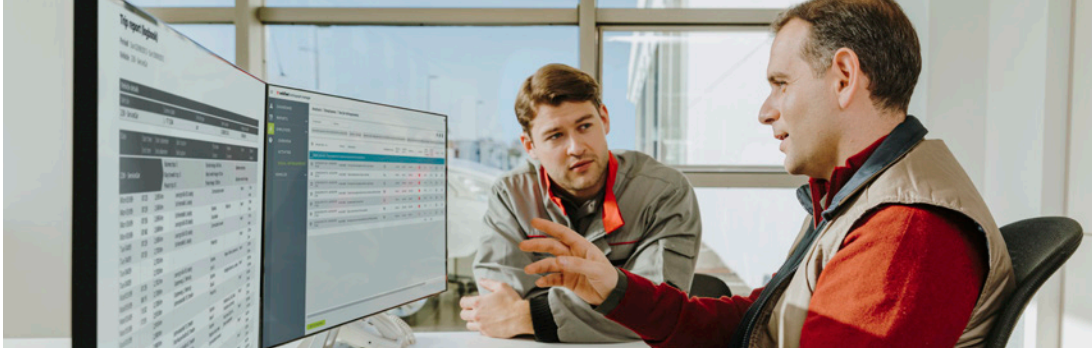
The cornerstone of Webfleet' commitment to information security is our set of security policies and programmes which cover the organisation of information security as well as:

- **Human resources security**
- **Asset management**
- **Access control**
- **Cryptography**
- **Physical and environmental security**
- **Operations security**
- **Communications security**
- **System acquisition, development and maintenance**
- **Supplier relationships**
- **Information security incident management**
- **Information security aspects of business continuity management**
- **Compliance and data privacy**

These policies are reviewed both internally and externally by non-partial authorities on a regular basis to ensure compliance with the ISO/IEC 27001 standard as well as all relevant legislation, to ensure that they maintain their continued effectiveness and integrity.

All employees and suppliers of the Webfleet Development Germany GmbH should comply with the security policies or contractually established requirements. Regular information security awareness training and documentation is provided to our employees to maintain a high level of information security awareness within the company. All aspects of security are covered in the scope of the documents and trainings and cover such issues as clean desk and safe use of the internet, secure coding, working safely from remote locations, and the correct procedure for labelling and handling of sensitive data.

Additional information is provided based on ad-hoc skill trainings to ensure that all employees are aware of their responsibilities to information security and are up to date with the latest technologies and vulnerabilities related to the operations of Webfleet Telematics Service Platform and the organisation for which they are responsible. All documentation is designed to be digestible in order to ensure the effectiveness of those policies.



3 ORGANISATION OF INFORMATION SECURITY

Information security is everyone's business

Webfleet employs a full-time information security team, integrated in our engineering, and IT departments, supported by some of the best and brightest talent within the industry in information, application, and network security. This team is responsible for maintaining the company's information security shield, developing and reviewing our various security policies and posture to ensure that all possible risks are managed, aligned with the company strategies and appetite for risk management. For data privacy related topics, our external data privacy officer coordinates with the information security team to ensure compliance and communication with our interested parties and internal teams.

At Webfleet, some standard information security and data protection activities include:

- **Continual review and improvement of security policy and procedures related to our high-availability network, redundant systems, and world class services based on the best practices and standards within the international community as well as the incorporation of custom designed controls through a multi-layered approach**
- **Conducting regular technical security design and implementation level reviews on all layers of the organisation within the scope of the ISMS**
- **Providing continual feedback to top management regarding the status of the information management system and any risks which might require a management review**
- **Monitoring of all technical systems to ensure real-time reaction to all incidents whether security or information related**
- **Providing incident management services to provide a tactical overview and analysis of information security assets and the threats to them**
- **Maintaining strict controls of our separated network environments for development, testing, and production through such programmes as vulnerability management, capacity management, patch management, static code analysis and review, aligned with the best practices of such standards like ITIL and ISO 20000 for service management**
- **Maintaining contacts within the security community, local law enforcement, as well as Webfleet Group legal and HR teams to ensure legal and regulatory compliance and internal auditing**
- **Providing physical security review and awareness in our office and data centre facilities**

4 HUMAN RESOURCES SECURITY

Information security is crucial prior to, during, and after the termination of employment. This includes selecting the right employees or contractors and providing them continual customised training.

Human resources ensures that our most important assets, our employees are protected aligned with local and national working regulations, and to communicate contractually their role in supporting and maintaining information security within the organisation in order to protect our customers' data and our intellectual property.

Employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Upon hire, Webfleet verifies an individual's education and previous employment, and performs internal and external reference checks. Where local labour law or statutory regulations permit, Webfleet may also conduct criminal, credit, immigration, and security checks where appropriate for the role. The extent of background checks is dependent on the desired position.

Upon acceptance of employment at Webfleet, all employees are required to execute a confidentiality agreement and must acknowledge receipt of and compliance with policies in the Webfleet IT user manual and all other policies and procedures related to the scope of their employment.

In order to comply with legislation, our staff are bound to data secrecy in their employee contracts which is aligned with the EU General Data Protection Regulation (GDRP), as well as other relevant privacy legislation. Additionally, all employees are regularly trained and educated with corporate security and data protection regulations which might affect them to reduce the company's overall operational risk. The use of subcontractors in our development and operational departments is kept to a minimum and additional controls are implemented to maintain a high security perimeter.

The confidentiality and privacy of customer information and data is emphasised in our policies and during new employee orientation where employees are provided with security training as part of the new hire orientation. In addition, each Webfleet employee is required to comply with the company's code of conduct. The code outlines Webfleet' expectation that every employee will conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and even competitors. Depending on an employee's job role; additional security training and policies may apply.

Webfleet employees handling customer data are required to complete additional requirements in accordance with these policies. Training concerning customer data outlines the appropriate use of data in conjunction with business processes as well as the consequences of violations. Every Webfleet employee is responsible for communicating security and privacy issues to designated Webfleet security staff. The company provides confidential reporting mechanisms to ensure that employees can anonymously report any ethics violation they may witness.

5 ASSET MANAGEMENT

Responsibility and classification of information

At Webfleet, all informational assets are assigned an asset owner as well as a risk owner.

The responsibility of these individuals is to identify and maintain the proper management and classification of Telematics assets aligned with the various policies and procedures for information security. During regular auditing of our information systems, the information security team coordinates with all asset/risk owners to verify and maintain compliance.

Media handling and disposal

All media at Webfleet is subject to secure policies and procedures for proper handling. Media is any format in which information might be contained including, but not limited to physical hard disks, USB sticks, compact discs, paper, electronic documentation and communications. We employ a media life cycle which includes the secure handling and disposal of all relevant media in scope.

When any media is retired from Webfleet' systems, physical disks containing customer information are subjected to a data destruction process before leaving Webfleet' premises. First, policy requires the disk be logically wiped by authorised individuals. The erasure consists of a full write of the drive with all zeroes (0x00) followed by a full read of the drive to ensure that the drive is blank with a follow up inspection to confirm that the disk has been successfully wiped. These erase results are logged by the drive's serial number for tracking. Finally, the erased drive is released to inventory for reuse and redeployment.

If the drive cannot be erased due to hardware failure, it must be securely stored until it can be sent for secure destruction. Secure destruction is performed through our ISO 27001 certified media destruction vendors which includes reviews of protocols for all outgoing media. Webfleet performs regular internal audits for compliance with our media disposal policy.

6 ACCESS CONTROL

User access management and responsibilities

Webfleet has extensive controls and practices in place to protect the security of our customer's information. Our Platform runs in a multi-tenant, distributed secure environment. Rather than segregating each customer's data onto a single machine or set of machines, the data from all platform customers (consumers, business, and even our own data) is distributed amongst a shared infrastructure composed of Webfleet' many homogeneous machines and located across Webfleet' Active/Active ISO/IEC 27001 compliant data centres located in Germany.

Webfleet Telematics Service Platform uses a distributed file system designed to store large amounts of data across large numbers of computers. Structured data is then stored in a large distributed database built on top of the file system. Data is chunked and replicated over multiple systems such that no one system is a Single Point of Failure (SPOF). Data chunks are given random file names and are not stored in clear text so they are not humanly readable. The layers of our platform require that requests coming from other components are authenticated and authorised. Service-to-service authentication is based on a security protocol that relies on a platform system to broker authenticated channels between application services. In turn, trust between instances of this authentication broker is derived from x509 host certificates that are issued to each platform production host by a Webfleet internal certificate authority.

Access by production application administrative engineers to production environments is similarly controlled. A centralised group and role management system is used to define and control engineers' access to production services, using an extension of the above-mentioned security protocol that authenticates engineers through the use of a personal x509 certificate that is issued to them. Policy requires that administrative access to the production environment for debugging and maintenance purposes be based on secure shell (SSH) public key authenticated connections. For both scenarios, group memberships that grant access to production services or accounts are established on an as-needed basis.

The security controls described above rest on the foundation of the integrity of the production platform. This platform in turn is founded on:

- **Physical security protection of the data centre environment**
- **Integrity of the production operating system environment**
- **Limited, as-needed system administrator (root) level access to production hosts granted to a specialised group of employees whose access is monitored**

These aspects of the Webfleet security practices are covered in more detail in subsequent sections of this document.

Authentication controls

Webfleet requires the use of a unique user ID for each employee. This account is used to identify each person's activity on Webfleet' network, including any access to employee or customer data. This unique account is used for every system at Webfleet. Upon hire, an employee is assigned the user ID by Human Resources and is granted a default set of privileges described below. At the end of a person's employment, policy requires that the account's access to Webfleet' network be disabled from within the HR system.

Where passwords or passphrases are employed for authentication (e.g., login to workstations), systems enforce Webfleet' strong password policies, including password expiration, restrictions on password reuse, and sufficient password strength. Webfleet makes widespread use of two-factor authentication mechanisms, such as certificates and one-time password generators.

Authorisation controls

Access rights and levels are based on an employee's job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Our employees are only granted a limited set of default permissions to access company resources, such as email, Webfleet's internal portal, and HR information. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Webfleet' security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorisation settings and the approval process to ensure consistent application of the approval policies. An employee's authorisation settings are used to control access to all resources, including Service Platform data and production systems.

System logging

Webfleet' policy is to log administrative access to all of our systems and data. These logs are reviewable by Webfleet security staff on an as-needed basis in order to support forensic activities or in order to protect the perimeter of our security countermeasures, and are mirrored on a separate server in which the logs are not editable.

7 CRYPTOGRAPHY

Webfleet invests in state-of-the-art hardware and software solutions including proven cryptographic technologies to ensure that informational assets and confidential data are transferred and maintained via high encryption and in a secure manner. This is critical in maintaining the security of our customer's data, and operational integrity of our systems.

Webfleet environments are optimally protected against any threats, and that our operations team is alerted in real-time to any intrusion attempts both internal and external.

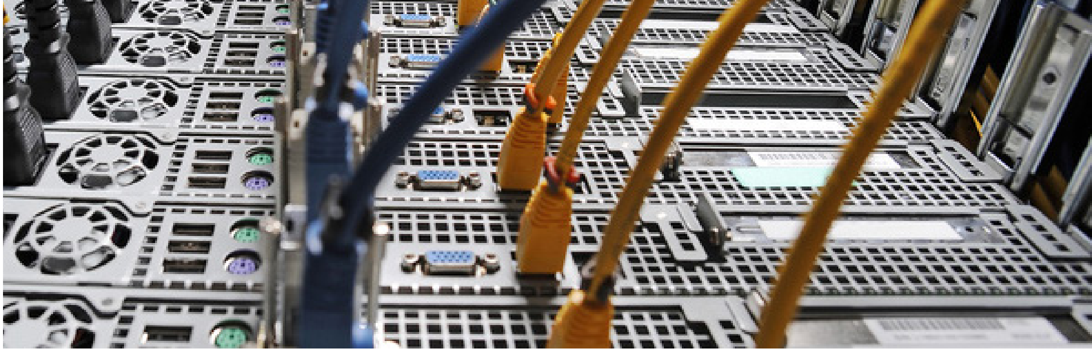
Secure data transfer

Webfleet provides a secure SSL/TLS data transfer of Service Platform data (UI or Platform API's).

SSL/TLS certificates are provided by an industry leader for cryptographic security. 2048-Bit certificates are provided for delivering the perfect balance between performance and strong security and is also recommended by the National Institute of Standards and Technology (NIST) and the German Federal Office for Information Security (BSI).

In addition, the SSL/TLS certificates support:

- **256-bit and 128-bit https AES encryption. Https is used by default for accessing data using the UI or Platform API's**
- **SHA-256 encryption which meets the highest EU government cryptographic standards**
- **Extended Validation (EV) authentication level which is the highest possible achievable level**



8 PHYSICAL AND ENVIRONMENTAL SECURITY

Webfleet maintains strict separation of its physical, logical and environmental information and infrastructure in order to provide the most secure experience possible for our customers and their data.

This also includes the protection of information equipment involved in the processing perimeter of our operations.

Some examples of how physical and environmental security are controlled:

- **System hardening based on the Center for Internet Security (CIS) standard for operating system, database, and network device hardening**
- **Regular review, testing and deployment through our patch management programme**
- **Centralised management of access control lists based on role based access control (RBAC) best practices to ensure all access is restricted only to those who require this access, and this access is monitored and logged in order to provide investigative evidence in the event of system tampering**
- **Regular monitoring and audit including log files**
- **Real-time monitoring and alert of all operational systems both of physical and virtual assets**
- **Intrusion Prevention systems with real-time alerting using Network-based (NIPS), Wireless (WIPS), Network Behaviour Analysis (NBA) and Host-based Intrusion Prevention Systems (HIPS). By incorporating IP systems from various vendors, we are able to use several detection methods including signature-based, statistical anomaly-based, and stateful protocol analysis detection**

Geographical/physical separations

Webfleet’ data centres are geographically distributed and aligned with the requirements of the ISMS. They also employ a variety of physical security measures to maintain our security perimeter. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks; however we place high value on our locations and vendors being ISO/IEC 27001 certified when possible.

The standard physical security controls implemented at each of Webfleet’ data centres are composed of well-known technologies and follow generally accepted industry best practices such as:

- **Custom designed electronic card access control systems**
- **Alarm systems**
- **Interior and exterior cameras**
- **Security patrols**

Physical access to areas where systems, or system components, are installed or stored is segregated from general office and public areas such as lobbies. Cameras and alarms for each of these areas are centrally monitored for suspicious activity, and the facilities are routinely patrolled by security guards. Webfleet' facilities use high resolution cameras with video analytics and other systems to detect and track intruders. Activity records and camera footage are kept for incident review, should it become necessary for forensic purposes. Additional security controls such as thermal imaging cameras, perimeter fences and biometrics may be used when necessary. Access to all data centre facilities is restricted to authorised Webfleet employees, approved visitors, and approved third parties whose job it is to operate the data centre.

Webfleet also maintains a visitor access policy and set of procedures stating that data centre managers must approve any visitors in advance for the specific internal areas they wish to visit. The visitor policy also applies to any employees of Webfleet who do not normally have access to data centre facilities. Webfleet audits who has access to its data centres on a regular basis to help ensure that only appropriate personnel have access to the Webfleet space as required to perform their job functions. Webfleet restricts access to its data centres based on role, not position. As a result, even most senior executives at Webfleet do not have access to Webfleet' data centres

Environmental security

Webfleet' computing clusters are architected with resiliency and redundancy in mind, helping minimise single points of failure and the impact of common equipment failures and environmental risks. Dual circuits, switches, networks, and other necessary devices are utilised to provide redundancy. Facilities infrastructure at the data centres has been designed to be robust, fault tolerant, and concurrently maintainable.

Power

To support Webfleet' 24x7 continuous operations, redundant electrical power systems are provided by the data centres. A primary and alternate power source, each with equal capacity, is provided for every critical component in the data centre. Upon initial failure of the primary electrical power source — due to causes such as a utility brownout, blackout, over-voltage, under-voltage, or out-of-tolerance frequency condition — an Uninterruptible Power Supply (UPS) or Diesel Rotary Uninterruptible Power Supply (DRUPS) are intended to provide power until the backup generators can take over. The diesel engine and diesel rotary backup generators are capable of providing enough emergency electrical power to run the data centre at full capacity for a period of time until normal power can be restored.

Climate and temperature

Air cooling is required to maintain a constant operating temperature for servers and other computing hardware. Cooling prevents overheating and reduces the possibility of service outage. Computer room air conditioning units are powered by both normal and emergency electrical systems. Additionally, oxygen reduction systems are in place to reduce the amount of oxygen available in the data centres to the minimum required for our employees to work in the space, yet not enough that a fire may occur. This provides the perfect balance and security that we require for our Service Platform systems.

Fire detection and suppression

Automatic fire detection and suppression equipment helps prevent damage to computing hardware. The fire detection systems utilise heat, smoke, and water sensors located in the data centre ceilings and underneath the raised floor. In the event of fire or smoke, the detection system triggers audible and visible alarms in the affected zone, at the security operations console, and at the remote monitoring desk. Manually operated fire extinguishers are also located throughout the data centres. Data centre technicians receive training on fire prevention and extinguishing of fires, which also includes the use of fire extinguishers. Most of our data centres also provide a nitrogen reaction system which can be activated to remove any remaining oxygen out of the air, thereby neutralising the effects of possible fire risk.

9 OPERATIONAL SECURITY

Active/active data centre setup overview

Webfleet is currently running two data centres in active/active setup. The multi-homing infrastructure and the load balancing equipment permit the utilisation of internet uplinks, application servers and services from both locations simultaneously.

Both data centres are connected via 3 redundant gigabit connections to provide a performant and stabile ring of communication channels between services located in both centres. During normal operations, both data centres are configured to share the load, but each data centre is able providing all services without performance impacts to customers, therefore our services are protected against disasters and business contingency is ensured meeting the reliability needs of our customers.

Data centre security

Webfleet operates two independent data centres in the European Union due to the high level of data privacy standards which are required for data centres located in the EU. Both centres are sited underground in two different cities within Germany provided from two separate vendors and operated in an active/active configuration ensuring the highest availability and full disaster recovery capabilities even due to events related to force majeure.

Both data centres provide very high levels of security and are detailed as followed:

Data centre 1 (Germany)

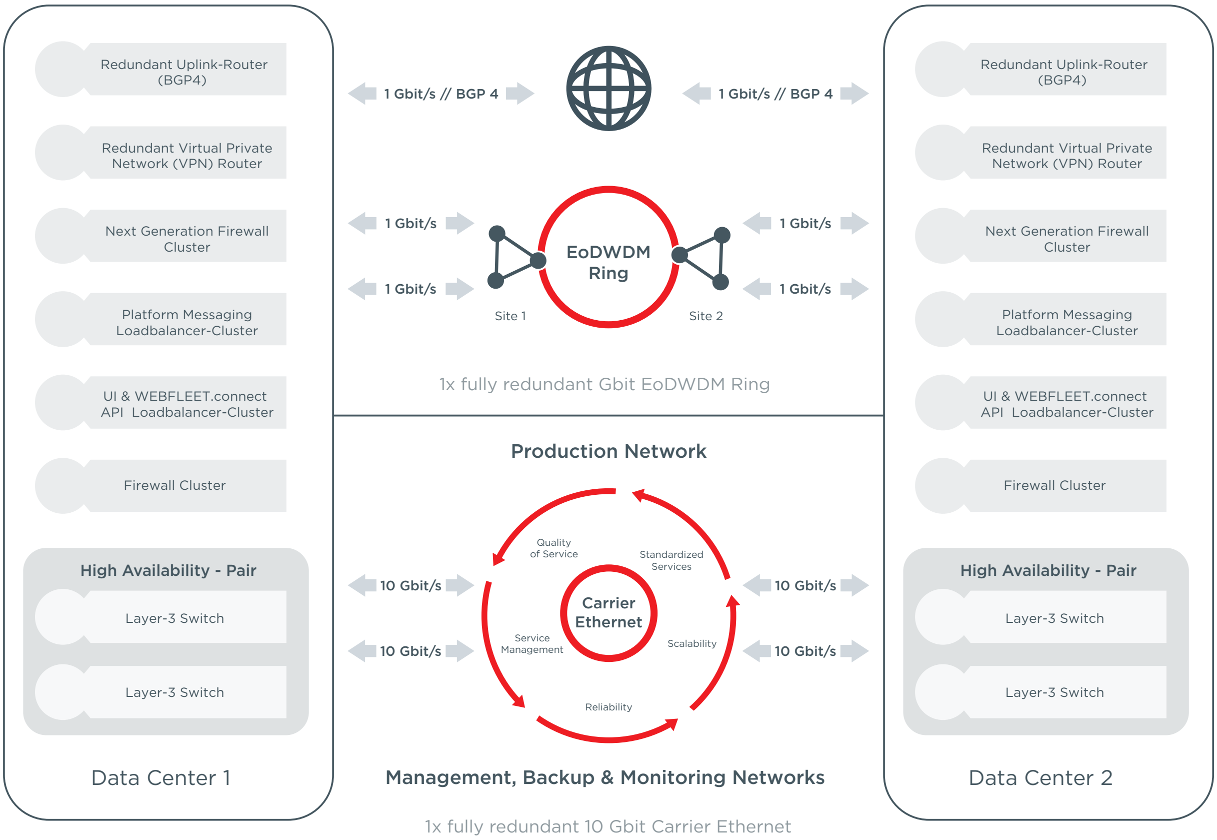
- **Separated areas with secured access only for authorised IT administrators team employees of Webfleet**
- **ISO 27001 Certified**
- **Three-stage access control for physical access**
- **N+1 redundant high performance UPS**
- **N+1 emergency power generator**
- **Regular monthly tests**
- **N+1 independent air conditioning systems**
- **Permanent oxygen reduction for fire prevention (~15%)**
- **Windowless underground facility**
- **24x7 monitoring**
- **Multiple house lead ins for WAN connectivity**
- **Alert sensors for humidity, smoke, vibration, etc.**
- **Video surveillance with 30 day recording to support security investigations**

Data centre 2 (Germany)

- **Separated areas with secured access only for authorised IT administrators of Webfleet**
- **ISO 27001 Certified**
- **Three-stage access control for physical access**
- **Redundant high performance UPS**
- **Emergency power generator**
- **Regular monthly tests**
- **Multiple independent air conditioning systems**
- **24x7 monitoring**
- **Multiple house lead ins for wide area network connectivity**
- **Alert sensors for humidity, smoke, vibration, etc.**
- **Video surveillance with 30 day recording to support security investigations**

High level network overview

The following high level overview of our network configuration between both data centres helps give an impression or our active/active data centre setup:

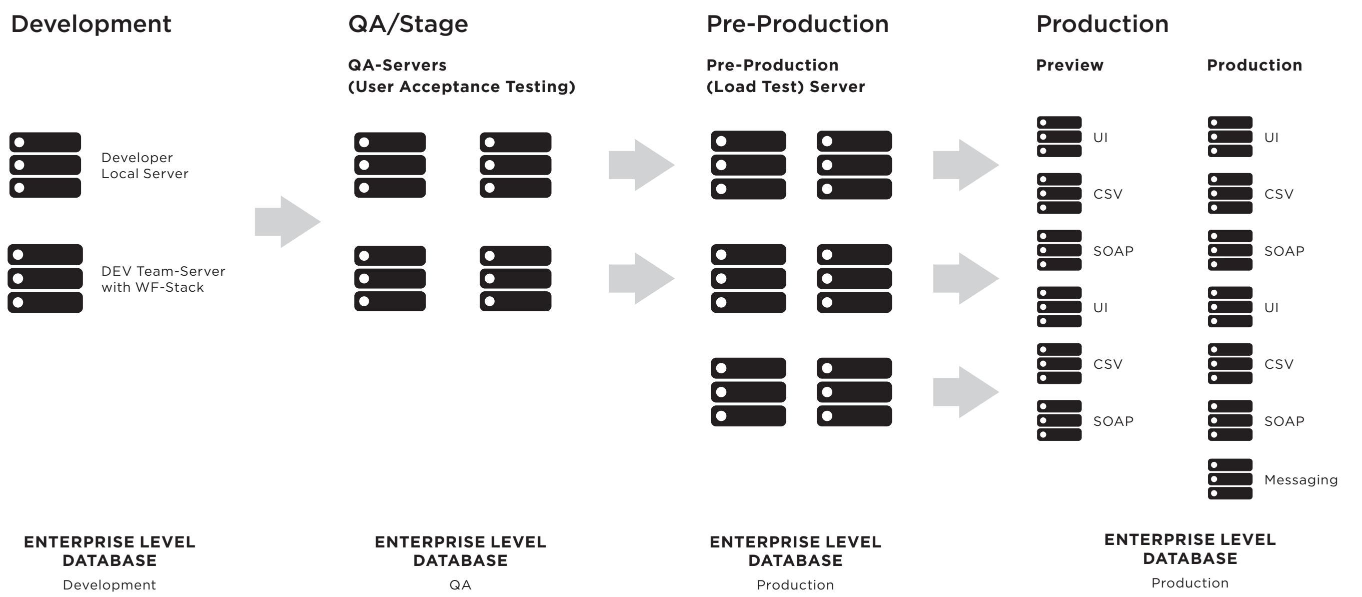


Redundant Uplink-Router (BGP4)
Redundant Virtual Private Network (VPN) Router
Next Generation Firewall Cluster
Platform Messaging Loadbalancer-Cluster
UI & WEBFLEET.connect API Loadbalancer-Cluster
Firewall Cluster
High Availability - Pair
Layer-3 Switch
Layer-3 Switch
Data Center 1
1 Gbit/s // BGP 4
1 Gbit/s // BGP 4
1 Gbit/s
1 Gbit/s
1 Gbit/s
1 Gbit/s
EoDWDM Ring
Site 1
Site 2
1x fully redundant Gbit EoDWDM Ring
Production Network
Quality of Service
Standardized Services
Carrier Ethernet
Service Management
Scalability
Reliability
10 Gbit/s
10 Gbit/s
10 Gbit/s
10 Gbit/s
Management, Backup & Monitoring Networks
1x fully redundant 10 Gbit Carrier Ethernet
Redundant Uplink-Router (BGP4)
Redundant Virtual Private Network (VPN) Router
Next Generation Firewall Cluster
Platform Messaging Loadbalancer-Cluster
UI & WEBFLEET.connect API Loadbalancer-Cluster
Firewall Cluster
High Availability - Pair
Layer-3 Switch
Layer-3 Switch
Data Center 2

Acronym legend

EoDWDM	Ethernet over Dense Wavelength Division Multiplexing – high performance connection for high bandwidth requirements
BGP4	Border Gateway Protocol – Standard gateway protocol to exchange routing and reachability information between autonomous systems on the Internet. BGP4 allows for aggregation of routes including autonomous system paths
VPN	Virtual Private Network – enables sending and receiving of data across shared or public networks in a secure manner as if connected to a company network
UI	User Interface
API	Application Programming Interface – An interface which allows for users to connect to the Service Platform over various methods
Gbit	Gigabit

Logically separated operations environments



Network security

Webfleet employs multiple layers of defence to help protect the network perimeter from external and internal attacks. Only authorised services and protocols that meet Webfleet' security requirements are permitted to traverse the company's network. Unauthorised packets are automatically dropped. Webfleet' network security strategy is composed of the following elements:

- **Control of the size and make-up of the network perimeter. Enforcement of network segregation using industry standard firewall and Access Control List (ACL) technology**
- **Systematic management of network firewalls and ACL rules that employs change management, peer review, and automated testing**
- **Restricting access to networked devices to authorised personnel**
- **Routing of all traffic through custom front-end servers that help detect and stop malicious requests**
- **Create internal aggregation points to enable better monitoring**
- **Examination of logs for exploitation of programming errors (e.g., cross-site scripting) and generating high priority alerts if an event is found**

Webfleet is operating approximately 50 HP ProCurve switches per data centre with redundant connections to each server (bonding) and additional separated connections for Backup and Management on dedicated switches. All connections take advantage of Gigabit technology to provide optimal performance and almost no noticeable network latency.

Logically separated network environments

Webfleet ensures optimal protection against external and internal threats to our informational assets. This is accomplished by separating the networks, for example the Demilitarized Zone (DMZ), development, testing, production, and office environments with Role Based Access Control (RBAC), and deploying multiple Next-Generation Firewall (NGFW) clusters for separating the different zones:

- **Multi-tier architecture with firewall clusters to separate the network zones**
- **Next-Generation firewalls (multiple active/active clusters per data centre)**
  - Threat and Intrusion Prevention Systems (IPS)
- **Application level firewall providing protection against:**
  - Layer 7 DoS and DDoS
  - Brute force
  - Cross-Site scripting (XSS)
  - Cross-site request forgery
  - SQL injection
  - Web scraping
  - Parameter and HPP tampering
  - Sensitive data leakage
  - Session hi-jacking
  - Buffer overflows
  - Cookie manipulation
  - Various encoding attacks
  - Broken access control
  - Forceful browsing
  - Hidden fields manipulation
  - Request smuggling
  - XML bombs/DoS
- **Restrictive rules and policies**
- **Daily reporting and regular audits**
- **Real-time monitoring and notifications**
- **Different firewall vendors**
- **Triple level protection against email threats (viruses, SPAM, etc.)**

System monitoring

Webfleet operates a redundant and distributed monitoring system to monitor all of our physical and virtual hosts and services. In addition to technical monitoring solutions, we have also incorporated checks within our system to enable us to achieve a near-replica of the user experience in regards to processing or http-response times.

In addition, external monitoring is in place from multiple international locations to assist with the real-time identification of any connectivity or availability issues when reaching Webfleet' services such as internet peering issues. This monitoring is measuring our services from a customer point of view such as with the login to the User Interface and provides regular SLA reporting for internal management of the services. Additionally, the Webfleet operations team will be notified through multiple communication channels if any issues are detected

Webfleet maintains access logs for our web and application servers related to the Service Platform for up to ninety (90) days on our secure log servers. This allows customers may view user sessions for up to ninety (90) days. The storage times may vary depending on local legislation.

Monitoring

Webfleet' security monitoring programme is focused on information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. At many points across our network, internal traffic is inspected for suspicious behaviour, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open source and commercial tools for traffic capture and parsing.

A proprietary correlation system built on top of Webfleet technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behaviour, such as unexpected activity in former employees' accounts or attempted access of customer data. Webfleet security engineers look proactively for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and web bulletin board systems. Automated network analysis helps determine when an unknown threat may exist and escalate these to Webfleet security staff, and network analysis is supplemented by automated analysis of system logs.

Malware prevention

Malware poses a significant risk to today's IT environments. An effective malware attack can lead to compromised accounts, data theft, and possibly additional undesired access to a network. Webfleet takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect, and eradicate malware.

Webfleet deploys Next-Generation Firewalls (NGFW) and Intrusion Prevention Systems (IPS) to assist us in the prevention of malware and other anti-virus related scans. Our operations teams have been trained to deal with any security events which our systems detect, and require an incident response. We invest highly in this area to reduce our operational risks and the risk of data breaches with our customers important data.

All Service Platform production systems which are protected from internal and external access provide built-in virus protection. The signatures are updated daily and provided by the various vendors. Some non-windows servers do not have anti-virus installed due to their high performance demands, yet these systems have been hardened using industry best practices and are verified using the Center for Internet Security (CIS) benchmarking tools and other additional controls which are not allowed to be shared outside of the organisation, yet provide an extensive amount of security protection.

All windows based servers and workstations perform hourly checks for new signatures and updates which are installed immediately and automatically.

10 COMMUNICATIONS SECURITY

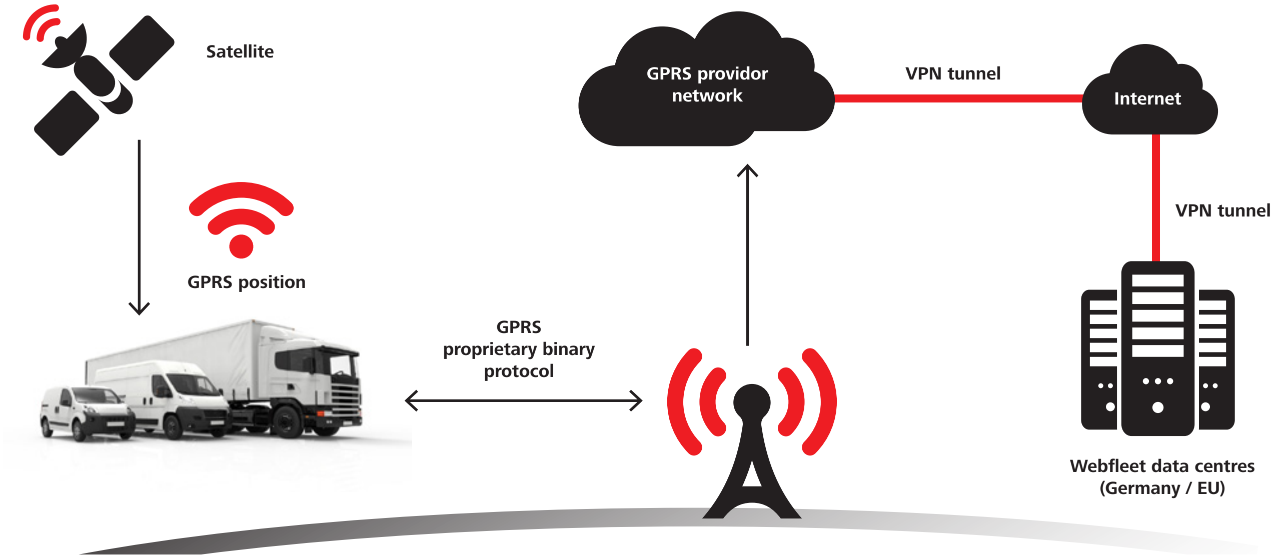
GPRS-connections

The Webfleet units, LINK (LINK 105 excluded) and PRO devices, are connected via GPRS to our infrastructure. The connections to the GSM-providers are based on VPN and provide either a 256 or 128 bit encryption. The VPN connections take advantage of the multi-homing configuration supporting high availability with an automatic failover. An example is the case of an outage to the uplink.

For the messaging servers where these units are connecting to, we are running several dedicated and high performance servers in each data centre which can handle a full load without our customers noticing a performance impact. All messages and data are distributed using our hardware load balancer clusters to maintain performance and ensure availability.

Service Platform information flow

Real-time fleet geo-location:
Webfleet provides a LINK tracking unit for some of its solution packages which are fitted into every vehicle within the fleet. The unit uses GPS satellite technology to establish its location every 10 seconds on average and then sends the coordinates of its location using GPRS to the secure Webfleet servers in Germany once every minute which in turn plot this position against the latest maps for viewing within Webfleet.



Using this method, the customer is able to view all of their vehicles on the screen at one time as an overview, and they will also have the ability to drill down to an individual vehicle at street level via the simple map control tools or mouse. To see more detail of the vehicle and its location, a user must simply increase the zoom level within the application.

Message processing

The core message processing contains more than 20 high-end servers, which are consuming the messages from the JMS systems, processing them and storing the data into a highly-available Enterprise Edition database system.

On each messaging server, a locally running map server is responsible for handling the reverse geocoding which converts the longitude and latitude to an existing address and enables our customers to have the freshest Webfleet map data.

The messaging servers including the JMS servers consist of more than 30 high performance servers in each data centre and are able to handle a full load continuously without experiencing processing delays or performance impacts to our customers.

Redundant Uplink Router (BGP4)

Redundant Virtual Private Network (VPN)

Next-Generation Firewall Cluster

Service Platform Messaging Loadbalancer-Cluster

User interface & Webfleet.connect API Loadbalancer-Cluster

Firewall Cluster

↓

GPRS Servers

Inbound Queue

Messaging Balancers

Messaging Dispatchers

↓

Enterprise Level Database

Internet connectivity

Webfleet operates multiple broadband internet uplinks from different vendors.

The internet uplinks for platform services are physically separated from the uplinks to the internet for office use (web browsing, email etc.) reducing any possible risk of impacts or dependencies to performance or security.

The redundant internet uplinks for the Service Platform are implemented as a multihoming solution having a provider aggregated Address Space (AS).

The benefit of having such a setup are the multiple internet uplinks from different vendors/ ISPs, which use/route the same IP address range over all existing uplinks. This provides additional security and reduces the risk from physical problems with the ISP connections or having the network as a potential single point of failure, but also from ISP-wide failures and nearly all types of configuration problems that might affect just a single ISP. If one uplink should fail, an automatic failover to one of the other uplinks is performed based on dynamic routing with BGP4 protocol. Failback works similarly and is also fully automated.

Load balancing

Webfleet operates multiple load balancer clusters per data centre, which is a standard networking method for distributing workloads across multiple computing resources. Additionally, the setup separates load balancing environments from customer facing systems such as the website, UI and Service Platform APIs, and from messaging related systems for maximum performance and availability and assists with removing possible intersystem dependencies.

The hardware based load balancer infrastructure is a proven solution from the global market leader for load balancing systems.

This solution provides advanced features and performance for load balancing such as:

- **Up to 10 Gbit/s L4/L7 Intelligent Traffic Throughput (per cluster node)**
- **More than 10 million concurrent connections at 1GB (per cluster node)**
- **Maximum SSL of 9,000 TPS (2k keys) for new connections (per cluster node)**
- **Application health knowledge**
  - health checks performed at the L7 Application level and automatically disables any non-healthy servers in the pool
- **Real time fault detection for failing servers providing IT Admins with detailed event information for fault correction**
- **Fast cache**
  - Performance acceleration
- **Advanced hardware compression**
  - Improves performance and reduces transfer volume
- **SSL hardware acceleration**

The implemented architecture allows Webfleet to quickly enhance our operating capacity and prevent any future resource limitations at an early stage through a combination of world-class hardware and our capacity management programme and our detailed monitoring capabilities before our customers experience any performance issues.

11 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

It is Webfleet' policy to consider the security properties and implications of applications, systems, and services used or provided by Webfleet throughout the entire project life cycle. Webfleet' security policies calls for teams and individuals to implement appropriate security measures in applications, systems, and services which are developed or acquired, aligned with any identified security risks and concerns. The policy states that Webfleet maintains a security team chartered with providing security-related guidance and risk assessment. Webfleet employs a variety of measures to ensure that the software products and services Webfleet offers to its customers meets the highest industry standards of software security. This section outlines Webfleet' current approach to software security; it may adapt and evolve in the future.

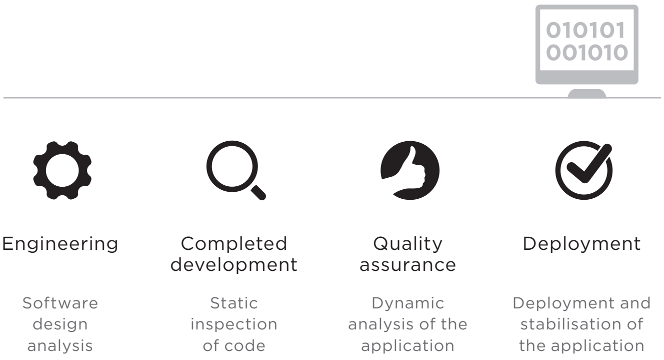
Service Platform Secure Software Development Life Cycle

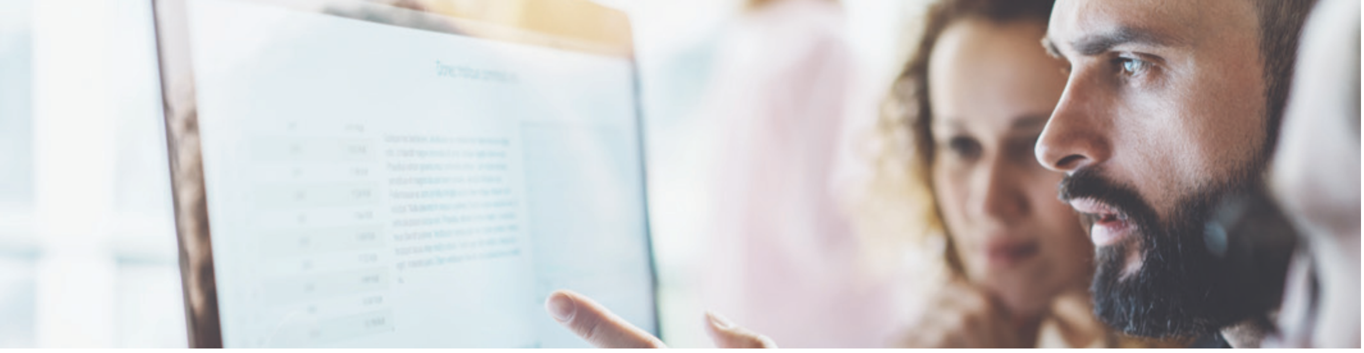
Webfleet maintains as part of its service management portfolio, a change management programme following the best practices of ITIL and ISO-20000. These processes are used throughout the development and operations landscape to ensure that not only our products are planned, designed, tested, approved, and implemented, but also all of our internal operations hardware and software as well as documentation related to the information management system is controlled through risk management, version control, change management and separated environments.

For the secure software development life cycle (SDLC), Webfleet has implemented a methodology aligned with the secure coding guidance which brings the advantages of many of the industry standard methodologies together, and developed a Project Creation Framework (PCF) which covers the major parts from the SDLC and other methodologies such as Waterfall and Agile Software Development. These are used for developing our platform and operating reliable software with a focus on quality, integrity, security and reusability combined with customer demands and reasonable time to market as a competitive advantage.

In regards to releases, Webfleet always focuses on separating feature releases from bug fix releases. All releases are integration and functionally tested by our dedicated QA testing team as well as load tested to measure performance.

For our customer facing systems, we incorporate the world class load testing tool Neoload to generate a higher load than we experience in our production environment with detailed monitoring applied to all layers in order to evaluate any impacts to any involved components such as web servers, J2EE servers, or the database back-end.


010101
001010
Engineering
Software design analysis
Completed development
Static inspection of code
Quality assurance
Dynamic analysis of the application
Deployment
Deployment and stabilisation of the application



For bug fix releases, each bug is classified based on customer/business impact and urgency and depending upon that classification, determines how we will build and test a release for example as an emergency change or adding to a normally scheduled bug fix version. All bugs reported from customer as well as internally reported for example from QA are logged and tracked accordingly.

Our release frequency is aligned with a monthly release cycle for many components as we are adopting continuous delivery as a method of controlling our development cycle and maintaining risk.

Due to our proven infrastructure including hardware load balancers, new releases can be deployed to our production environment with little or no customer impact.

Security consulting and review

With regards to the design, development, deployment and operation of applications and services, the Webfleet product and engineering teams provide the following primary categories of services in respect to secure coding.

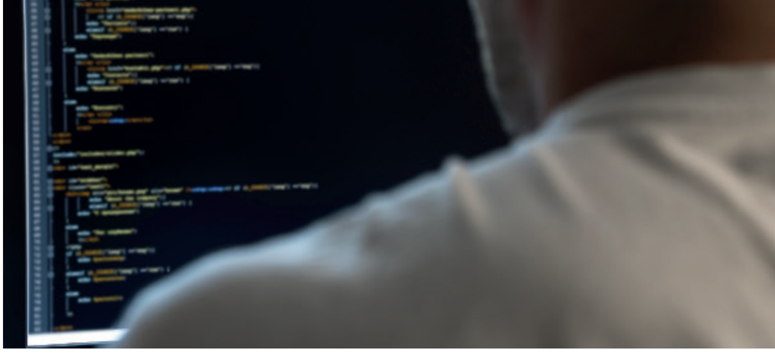
- **Security design reviews — design-level evaluations of project security risks and corresponding mitigating controls, as well as their appropriateness and effectiveness**
- **Implement security reviews — implementation level evaluation of code artefacts to assess their robustness against relevant security threats**

Webfleet recognises that many classes of security concerns arise at the product design level and therefore must be taken into consideration and addressed in the design phase of a product or service. Ensuring that such considerations are taken into account is the primary purpose of the product control framework which has the following objectives:

- **Provide a high-level evaluation of the security risks associated with the project, based on an exploration of relevant threats**
- **Equip the project's decision makers with the information necessary to make informed risk management decisions and integrate consideration of security into project objectives**
- **Provide guidance on the choice and correct implementation of planned security controls, authentication protocols or encryption**
- **Help ensure that the development team is adequately educated with regard to relevant classes of vulnerabilities, attack patterns, and appropriate mitigation strategies**

In cases where projects involve innovative features or technologies, it is the responsibility of the information security team to research and explore security threats, potential attack patterns, and technology-specific vulnerability classes related to such features and technologies.

Where appropriate, Webfleet contracts with third party security consulting firms to complement our existing information security skill set and to obtain independent third party review to validate in-house security reviews.



Security in the context of Webfleet's software development life-cycle

Security is at the core of our design and development process. Webfleet' engineering organisation requires that product development teams follow a specific software development process which is part of the historical culture of Webfleet and its software design success. Webfleet' security review processes are adapted to work within the product control framework. The success of this process relies upon Webfleet' quality-driven engineering culture and a few requirements defined by engineering management for project development processes:

- **Peer-reviewed design documentation**
- **Adherence to coding style guidelines**
- **Peer code review**
- **Multi-layered security testing**
- **OWASP Top 10 and SANS Top 25 Static Code Review**

The above mandates embody Webfleet' software engineering culture, where key objectives include software quality, robustness, and maintainability. While the primary goal of these mandates is to foster the creation of software artefacts that excel in all aspects of software quality, the Webfleet engineering and security team's experience also suggests that they represent significant and scalable drivers toward reducing the incidence of security flaws and defects in software design:

- **The existence of adequately detailed design documentation is a prerequisite of the security design review process, since in early project stages it is generally the only available artefact on which to base security evaluations**
- **Many, if not most, classes of implementation-level security vulnerabilities are fundamentally no different from low-risk, common functional defects. Most implementation-level vulnerabilities are caused by fairly straight-forward oversights on the developer's part**
- **Given developers and code reviewers who are educated with respect to applicable vulnerability patterns and their avoidance, a peer review-based development culture that emphasises the creation of high-quality code is a very significant and scalable driver towards a secure code base**

Webfleet software engineers collaborate with other engineers across Webfleet on the development and vetting of reusable components designed and implemented to help software projects avoid certain classes of vulnerabilities. Examples include database access layers designed to be inherently robust against query-language injection vulnerabilities or HTML template frameworks with built-in defences against cross-site scripting vulnerabilities.

Security education

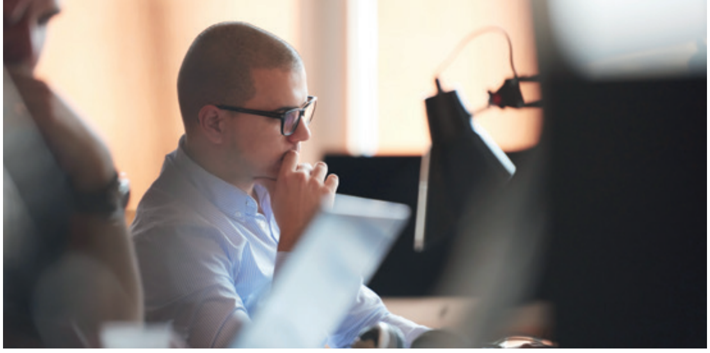
Recognising the importance of an engineering work force that is educated with respect to secure coding practices, the Webfleet security team maintains an engineering outreach and education programme that currently includes:

- **Security training for all new employees, especially engineering and operations teams**
- **The creation and maintenance of extensive documentation on secure design and coding practices**
- **Targeted, context-sensitive references to documentation and training material. For example, automated vulnerability testing tools provide engineers with references to training and background documentation related to specific bugs or classes of bugs flagged by testing tools**
- **Technical presentations on security-related topics**
- **Corporate security workshop, a recurring internal conference that brings together engineers from various teams at Webfleet who work in security-related fields and that offers in-depth technical presentations on security topics to our engineering teams**

Implementation-level security testing and review

Webfleet employs a number of approaches to further reduce the incidence of implementation-level security vulnerabilities in its products and services:

- **Implementation-level security reviews: Conducted by members of the Webfleet security team, typically in later stages of product development, implementation level security reviews aim to validate that a software artefact has indeed been developed to be robust against relevant security threats. Such reviews typically consist of a re-evaluation of threatsand countermeasures identified during security reviews**
- **Automated testing for flaws in certain relevant vulnerability classes. We use both in-house developed tools and some commercially available tools for this testing**
- **Security testing performed by software quality engineers in the context of the project's overall software quality assessment and testing efforts**



System hardening

Hardened in-house from the ground up, Webfleet' production servers are based on a stripped and hardened version of Linux that has been customised to include only the components necessary to run the Service Platform, such as those services required for administering the system and serving user traffic. The system is designed for Webfleet to be able to maintain control over the entire hardware and software stack and to help provide a secure application environment.

Webfleet' production servers are built on a standard Linux operating system (OS), hardened based on industry standard controls, and security fixes are uniformly deployed to the company's entire infrastructure. Using a robust change management system to provide a centralised mechanism for registering, approving, and tracking changes that impact all systems, Webfleet minimises the risks associated with making unauthorised modifications to our standard installed OS.

Vulnerability/patch management

Webfleet maintains all of its information assets through our extensive patch management policy for security and virus patches. Security patches for Linux, JDK or other components are installed first in a test environment before being rolled out to our production environment. This means that patches are functionally tested by our QA teams and load tested as well to ensure that security and performance are measured.

Webfleet performs vulnerability checks against all systems on a regular basis and should any gaps be detected, an incident is raised for our patch management team and corresponding change management procedures are followed for scheduling the package either for the next scheduled maintenance cycle or through emergency change procedures to patch security risks.

Webfleet also maintains relationships and interfaces with members of the security research community to track reported issues and Common Vulnerabilities and Exposures (CVE).

Penetration testing

Webfleet performs regular penetration testing both internally and externally to fulfil the requirements of the ISO 27001 standard and to prove that standard changes do not create any unknown security access which has not been requested. Internally we perform network scans on a daily basis with full vulnerability scans weekly to ensure that we are alerted to any vulnerability in real time.

We also work with our external security expert vendors whom perform regular external audits of our systems which includes black and grey box testing for our externally facing systems.

12 SUPPLIER RELATIONSHIPS

Security in supplier relationships

Webfleet invests heavily in protecting its internal informational systems, yet our risk analysis advises that we must also be aware of the security levels on the perimeter of our management system. Therefore, we take care to perform security risk analysis on our potential suppliers in order to establish the level of risk which we need to manage on the boundaries of our system.

When possible, we select vendors who also have been certified against the ISO 27001 or similar management systems, or who have been determined to have sufficient security controls in place to not increase our risk or risk appetite.

We also actively monitor our suppliers so that we are notified of any changes in their security profiles which in turn has a potential effect on our level of protection, and our ability to manage our risks.

Supplier service delivery

In addition to establishing background checks and identifying risks with our suppliers, we actively perform regular reviews of the our agreed services which are delivered to us, especially in response to the agreed security agreements in place in order to establish and control that the selected controls in place are adequate to maintain a secure perimeter for all of our informational assets and your data.

These regular reviews are also independently audited during our regular ISO 27001 certification audits to maintain that these are aligned with best practice, and our determined risk acceptance.

13 INFORMATION SECURITY INCIDENT MANAGEMENT

Identify, analyse, correct

Webfleet has an incident management process for security events that may affect the confidentiality, integrity, or availability of our systems or data. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key personnel are trained in forensics and handling evidence in preparation for an event, including the use of third party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities.

To help ensure the swift resolution of security incidents, the Webfleet security team is available to all employees. When an information security incident occurs, Webfleet's security team responds by logging and prioritising the incident according to its severity. Events that directly impact customers are treated with the highest priority. An individual or team is dedicated to remediating the problem and enlisting the help of product and subject experts as appropriate. Other responsibilities are deferred until the issue is resolved.

Webfleet security engineers conduct Post Incident Reviews (PIR) when necessary to determine the root cause for single events, trends spanning multiple events over time, and to develop new strategies to help prevent reoccurrence of similar incidents.

14 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Webfleet operates its Service Platform and its services aligned with the ISO 27001 standard which encompasses the incorporation of a disaster recovery plan for various contingencies. We perform regularly audits and tests of our systems to ensure that any recovery activities are successful and efficient to re-store services to our customers.

Due to our active/active data centre configuration, the probability of a major disaster affecting both data centres has been determined by our risk management team to be very unlikely, although disaster recovery plans have been created to cover such events regard-less of likelihood.

To minimise service interruption due to hardware failure, natural disaster, or other catastrophes, Webfleet implements a disaster recovery programme at all of its data centres. This programme includes multiple components to minimise the risk of any single point of failure, including the following:

- **Data replication and backup: To help ensure availability in the event of a disaster, platform data is replicated to multiple systems within a data centre, and also replicated to a secondary data centre**
- **Webfleet operates a geographically distributed set of data centres that is designed to maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between the data centres help ensure swift failover. Management of the data centres is also distributed to provide location-independent, around-the-clock coverage, and system administration**

In addition to the redundancy of data and separately located data centres, Webfleet also maintains a business and information security continuity plan for its technology headquarters in Leipzig, Germany. This plan accounts for major disasters, such as a natural disaster or a public health crisis, and it assumes people and services may be unavailable for up to thirty (30) days. This plan is designed to enable continued operations of our services for our customers. We conduct regular testing of our disaster recovery plan.

High availability

Webfleet Telematics Service Platform is based on a distributed and scalable architecture with multiple redundancies, load balancing and clusters to support capacity management for a maximum of scalability and high availability.

The production environment currently has the following capacities:

- **More than 100 up-to-date multicore servers containing (gross capacity)**
  - > 50 Terabytes of local disc storage
  - > 140 multi core CPUs
  - > 4 Terabytes of RAM
- **6 Fibre Channel Network Storages (SAN)**
  - Approx. 200 Terabytes gross capacity

In addition to the production environment, Webfleet operates fully separated and redundant development, stage and pre-production environments to provide for an optimal configuration for developing and testing of our world class Platform solution to ensure the maximum quality and performance, with approximately another fifty (50) servers which are dedicated to these environments.

Each release is functionally tested by a dedicated team of quality assurance experts including, but not limited to static code analysis, regression testing, and load testing using bleeding edge simulation software. This allows for the forecasting of workloads which deviate from that which is currently experienced within the production environment. This and other combined efforts assist us to ensure that our service platform remains performant and stable under all loads and that our code is tested against known vulnerabilities and approved through our change management processes before being deployed to production.

Server data protection

All servers are running with disk mirroring enabled using RAID-1, RAID-5, or RAID-10 in order to prevent data loss in the event that a hard disk should fail. All-important data including log or configuration files are backed up daily to our secure network storage in addition to our tape backup systems. For network storage, these files are stored for ninety (90) days to tape without limitation for monthly backups based on our secure backup policies.

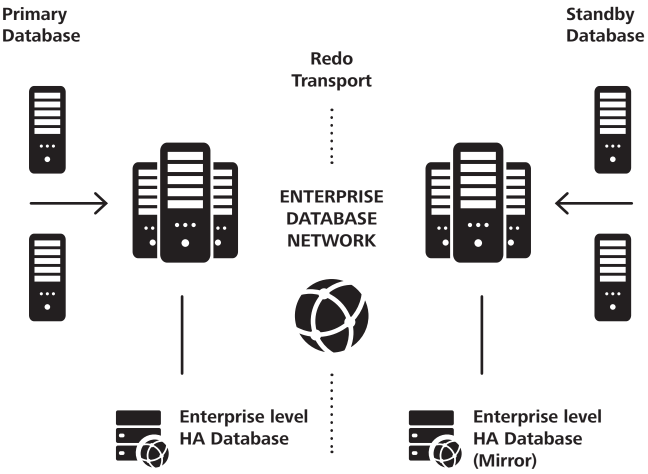
Database back-end data protection

Webfleet operates a highly-available Enterprise level database backend which runs on high performance server and SAN hardware.

This configuration is implemented at each of our data centres for our database servers, redundant SAN switches and SAN storage using our enterprise level backup solution to provide our customers with the highest level of availability.

Platform data as well as all confidential data are stored within the database, which is the leading enterprise class database with industry leading performance, security, reliability and scalability. Additionally, all database storage on our Storage Area Network (SAN) is secured with RAID-protection.

Enterprise Level Database Backup Solution


Primary Database
Standby Database
Redo Transport
ENTERPRISE DATABASE NETWORK
Enterprise level HA Database
Enterprise level HA Database (Mirror)

To ensure high availability of our database back-end, we operate a managed standby within our second data centre. This also enables us to have a minimum impact in case of a scheduled maintenance on our database back-end or data centre infrastructure of Webfleet. All transactions from our Master database are immediately synchronised and committed to our managed standby. This setup allows us to conduct a fast (automatic and/or forced) failover which is performed automatically or forced to the standby system with minimal customer impact.

The managed standby system located in our second data centre runs on a similar dedicated server and SAN storage as is in the primary data centre and the identical security controls provide protection within both locations.

Daily full backups of the database including the transaction logs are stored on network storage (NAS) and redundantly to tape (B2D2T).

By having full backups of our data including the transaction logs, it is possible to perform a point in time recovery. Using these recovery sets, we perform a monthly restore test of the data to ensure its integrity. On our NAS, we archive backups from the past seven (7) days while tape backups are archived for a longer period based on our backup policy.

Secure off-site backup tape storage

Webfleet stores our secure backup tapes in a high security offsite location provided by our security vendor who provides a regular pickup and delivery service approximately 40 kilometres away from the Webfleet location in Germany.

Data protection and backup security

Webfleet ensures that the risk of data loss or data corruption of our customers' data is managed to an absolute minimal risk level for issues which may be caused by technical issues or human error. Webfleet has implemented state-of-the-art hardware and software including a battery of controls to ensure the maximum level of protection to customer data and informational assets. Various controls have been implemented within the architecture of the Service Platform to support our information security strategy and compliance to regulations.

For example:

- **Two-step verification**
- **Customer determined Password length and strength**
- **Secure browsing connections (HTTPS)**

15 COMPLIANCE AND DATA PRIVACY

Legal information access process

Webfleet follows standard legal processes in responding to third party requests for user information. Information can only be obtained by third parties through legal processes such as search warrants, court orders, subpoenas, through a statutory exemption, or through user consent. Upon receipt of a request for information disclosure, Webfleet' legal team reviews the request for compliance with applicable law. Any data such as telemetry or location data is protected under data privacy laws and regulations, and we enforce the requirement that no data is provided to any third parties unless it is mandated by law. All data is stored and processed within the European Union in regards to legal data privacy regulations, and protects our international customer data.

Data Privacy

Webfleet is committed to protecting its customers' data and any further informational assets with the highest security controls available. To provide our tracking and tracing services, we need to collect and maintain numerous amounts of confidential data based on regulated data privacy regulations for each of the various collection methods which are regularly reviewed by our data privacy officer and an internationally accredited auditing body during certification audits. In order to meet and exceed the data privacy expectations of our customers and the legal regulations such as the EU GDPR, other relevant privacy legislation, and our internal policies. Webfleet maintains several physical, electronic and procedural controls for example:

Maximum security and integrity

- **Your data is in safe hands. We use proven security measures to safeguard your valuable data, so you can be confident that it's isolated and secure. All confidential data is stored within our secure data centres located in Germany to provide the maximum level of protection**
- **Next-Generation Firewalls (NGFW) and other security investments for protection against external and internal data breaches including monitoring**
- **Unique Platform user credentials or customer logins which are stored with the highest level of encryption in our secure data centres**
- **Highest Standard Extended Validation SSL Encryption for data transfer and digital certificates to authenticate that users are transacting with Webfleet**
- **Regular internal and external audits of our information management systems, data centres, and our data privacy processes**
- **Employee access to Personally Identifiable Information (PII) must be formally approved through our change management processes, and those who are authorised to process data are under employee agreement which is aligned with the requirements of the EU GDRP and relevant privacy legislation for the assurance of confidentiality**

Protecting driver privacy

1. **Safe data**
   Webfleet can only be accessed with a registered account name, user name and password
2. **You decide who sees what**
   With Webfleet, you can restrict the information each user can access on a 'need to know' basis
3. **Drivers control their own privacy**
   Once they're off-duty, drivers can switch to private mode on their Webfleet devices so the vehicle's location can't be tracked
4. **We put your drivers first, just like you**
   All of our solutions are driver-centric, so you can reassure your drivers that they'll be the first to feel the benefit of your investment in Webfleet

The Platform environments are completely separated from other systems or environments, such as the office or development environments, and access to productive servers is strictly limited to the Webfleet IT admins, and protected by multiple firewall layers using different vendors/and or platforms. Any access is securely logged and archived for supporting forensics procedures.

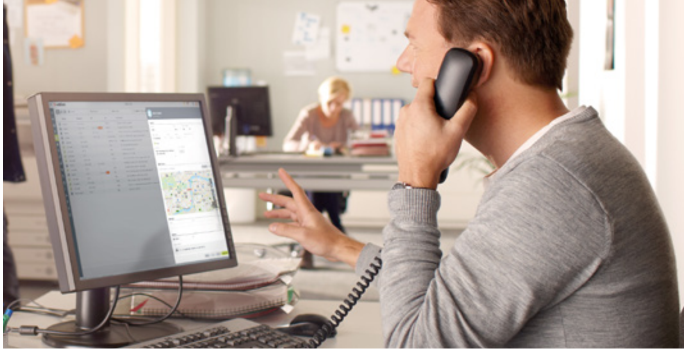
Data deletion

After a Webfleet user or administrator deletes information within their account, the data in question is removed and no longer accessible from that user's Webfleet interface. The data is then dereferenced and will be overwritten on the Webfleet back-end with other customer data over time. No customer data will be retrievable by a different customer should that previously allocated space be dereferenced and has been determined by our data protection officer to not pose a risk to our customers.

Furthermore, data privacy is part of the legal compliance of the ISO 27001 standard and the Webfleet Group.

Data retention schedule

Webfleet uses the following schedule for its data retention. This is important information that most work councils or data protection officers will be interested in when reviewing the Service Platform.



Webfleet Telematics Service Platform
Previous ninety (90) days: all detailed data including precise position data tracks

Webfleet Dashboard & Reporting
Current year plus previous two (2) calendar years: logbook, dashboard and reporting

Webfleet.connect API
Previous ninety (90) days: all detailed data including precise position data tracks

Webfleet.connect – API – Message Queue Service
Previous two (2) days: messages acknowledged, Previous 14 days: messages not acknowledged. Data is only stored if the customer creates a subscription for that service.

Webfleet Mobile
Previous ninety (90) days*: all detailed data including precise position data tracks

** Retention times may differ based on specific country related regulations.*

Digital Trust / Data Protection Officer

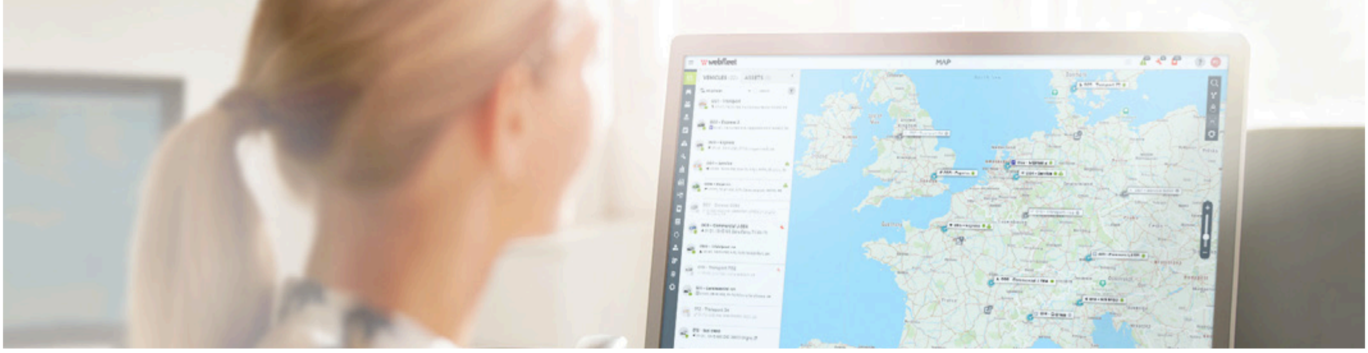
Webfleet technology is fully compliant with the EU General Data Protection Regulations as well as other global privacy legislation. Our full time certified Digital Trust and Data Protection Officer monitors compliance and provides guidance to the business, supported by the Digital Trust Management team.

Contact Info

For more information on on Digital Trust, Information Security and Data Protection please contact:
digitaltrust@webfleet.com

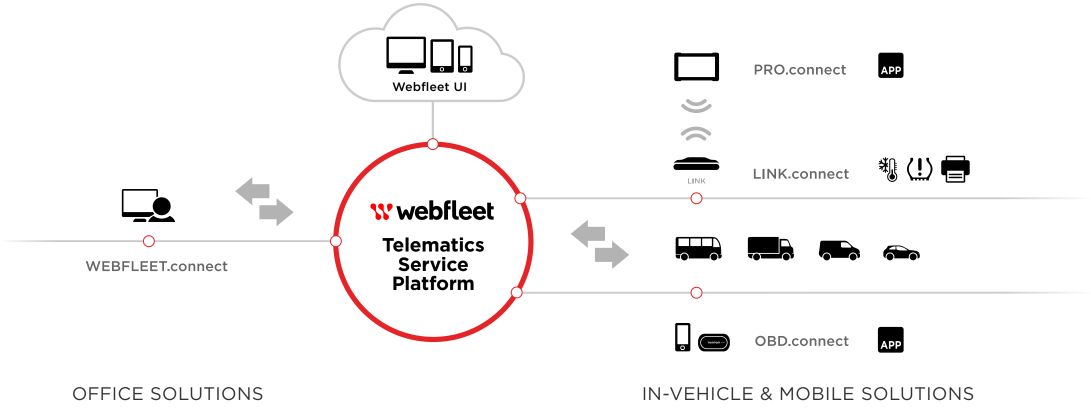
Alternatively you can write to:

Bridgestone Mobility Solutions B.V.
Legal Dept.
Beethovenstraat 503, 1083 HK Amsterdam,
Netherlands



16 PLATFORM SECURITY AND COMPLIANCE FEATURES

In addition to the various security controls described previously, which Webfleet has put in place to help protect the security and privacy of customer data, the Webfleet Telematics Service Platform provides several additional security options that can be utilised by a customer's administrators. We are always working to give customers more choices when managing their security control needs.



Web interface (UI) and Platform APIs

Webfleet fleet management can be integrated seamlessly with your current software and applications, giving you a comprehensive and fully connected fleet and workforce management solution. This means you can access all data, from mobile workforce, traffic and vehicle information to data from mobile devices, through your existing systems. You can work faster, smarter and more efficiently.

We have a wide network of reliable and trusted software and hardware alliance partners that have integrated Webfleet fleet management into their applications. With the help of Webfleet and our partners, you can:

- **Access dozens of existing partner apps**
- **Implement your solution quickly and easily**
- **Benefit from Webfleet's world-class API – Webfleet.connect**

With Webfleet fleet management, you can tap into the industry's richest set of integrated applications. Which means you don't have to transform the way you work – just improve it.

Visit our **App Center** to find out how you can integrate Webfleet fleet management with your current solutions. Or learn more about how integration works.

Webfleet operates for the UI and API's several dedicated and high performance servers. The various applications are separated into different zones on the server for performance and security reasons.

The server resources in each data centre can handle their full load capacity without any noticeable performance impacts to our customers. All requests are load balanced using our hardware load balancer clusters.

Webfleet Mobile

Additionally, the opportunities to connect to Webfleet have expanded allowing you instant access to the information you need to stay in control of your entire operation, no matter if you are trying to manage your dispersed business from the road or in the office.

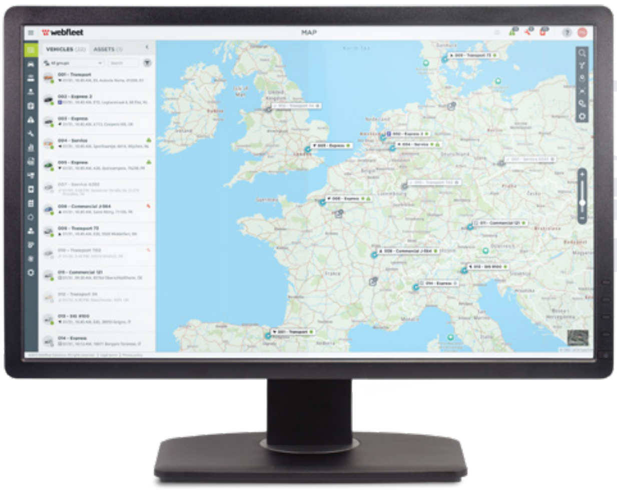
It offers the same great level of security in a flexible package allowing you to:

- **Manage on the move**
- **Offer better service**
- **Stay in control**

Webfleet Mobile is available from the Google Play Store as well as the Apple App Store.

Global leader in fleet management services:

The largest number of active subscriptions in Europe.



- **EASE OF USE**
- **RELIABILTY**
- **FAST ROI**
- **FUTUREPROOF**

Choose integrity. Protect the environment

Last but not least, we would like to remind you that not only is the importance to the protection of informational assets a priority for Webfleet, but knowing that we provide you the means with which to increase the protection of your informational assets, enabling you to protect your employees‘ data, as well as the world and the environment we live in.

Can your organisation become ISO 27001 certified by association?

ISO 27001 covers an agreed and approved scope achieved and reviewed during the certification process. If you or your organisation are looking to become certified, then having Webfleet as certified supplier will help you to reduce risk, and may make it easier for you to become certified.

If you are already certified, then having Webfleet as a strong partner will align with your existing information management systems, and further reduce your operational risk.

17 CONCLUSION

Webfleet is committed to maintaining the highest levels of information security on its computer systems, data centres, personnel, and customer data. This document has covered some of the standard highlights of our security implementation. Some controls however have not been mentioned and are not made public in order to help maintain the highest level of security.

These controls however do not have any negative impact on the protection of our customers‘ data, nor do they violate any regulation or legislation within the European Union. Our strategy is reflected throughout the organisation, and our Webfleet Telematics Service Platform provides multiple layers of controls at each level of data storage, access, and transfer.

Webfleet invests in the trust of our customers on a daily basis. You can be assured of the value placed on privacy and the professional protection of the confidentiality, integrity, and availability of your data.

Webfleet
www.webfleet.com

18 PLATFORM SERVICE LEVELS

Availability

Webfleet provides a minimum client observable average availability of 99.95% per month.

Unavailability in terms of this document is defined as beginning with the time of notification of Webfleet by the client and the ending with the time when

- **Webfleet is available again, or**
- **Webfleet has provided a reasonable workaround**

Unavailability caused by planned maintenance work that has been announced with a notice period as defined below does not contribute to the calculation of unavailability.

Exceptions

Availability, reaction and recovery times are only valid for services and components under the direct control of Webfleet. Therefore, the following exceptions apply:

- **Telecommunications or network connection failures (including but not limited to peering problems at the internet backbone)**
- **Denial-of-Service (DoS) attacks originating from the internet**
- **Hacking attempts or attacks against Webfleet‘ infrastructure**
- **Force majeure**
- **Changes in applicable legislation**

Parameters

According to the table below which defines the service level parameters, unavailability notices received by Webfleet will be answered or acknowledged within the maximum time to respond.

Scheduled maintenance

- **announced on the Webfleet login screen**
- **Max. 4h downtime per maintenance activity**
- **Max. 8h downtime per month**
- **Notification provided at least 5 business days before scheduled maintenance**
- **Performed during non-business hours (business days between 22:00 – 06:00 MESZ, weekends or public holidays)**

Unavailability of the Service

Unavailability of Service Platform components (communication and messaging, database, application servers or other modules, developed by and under Webfleet’ control).

Unavailability of the Infrastructure

Unavailability of the local network infrastructure, internet connection, firewalls, gateways, servers, or other critical hardware and equipment.

SLA	GMT	Time to respond	Time to repair
Unavailability of the service	Monday to Friday 08:00 - 17:00	30 Minutes	4 Hours
Unavailability of the infrastructure	Monday to Friday 08:00 - 17:00	30 Minutes	12 Hours