Security Domain	RFP/RFI/VSA Questionnaire	Responses	Customer	Date
Governance Risk & Compliance	Describe Netradyne overall Security and Compliance Posture	We have stringent levels of protection to secure our product(s) and underlying infrastructure. Netradyne adopt industry best security practices and is certified with ISO 27001:2022 and 27701:2019 recognitions. The same can be shared under NDA. Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management. Our solution is a SaaS offering which is hosted on secure, highly available & scalable AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs, which is the front end of Multi-Tier architecture, DBs are at back end and only accessible though Netradyne internal web API services to fetch the data for the requests. At perimeter and boundary level NGFW are installed which filters the traffic. WAF is also equipped along with IPS/IDS. Netradyne uses enterprise scale Security Solutions and tools providing RBAC & Least Privilege, Network Security, Firewall, UTM, APT, IDS/IPS to protect the systems. It has AES 256-bit encryption for data at rest and backups. It uses SSL/TLS 1.2+ for data in transit. We understand the critical nature of information security requirements and are committed to maintain the highest standards. We appreciate customer diligence in reviewing our security posture, and we look forward to addressing any concerns or additional requirements they may have. Our goal is to establish a partnership built on trust and confidence.	Standard Security & Compliance Response	8-Aug-24
Service Scope	What services do / will you provide to Customer?	In cab video safety camera and driver safety and performance management analytics and software platform and mobile application. Netradyne's Driveri processes and analyzes every minute of driving to provide fleet safety and performance analytics in real time as well as driver coaching in real time. Netradyne offers the most advanced vision based AI, edge computing, and machine learning with the highest video quality in the market.	Teletrac/Vontier	31-Mar-22
Service Scope	Please identify which services are in-scope with respect to your answers below.	Netradyne shall supply Hardware and Services to Customer's Subscribers in accordance with the terms and conditions outlined in the Strategic Market Agreement between Netradyne and Customer and Netradyne's Standard Terms. The hardware and services in scope are specified under Exhibit A of the Strategic Market Agreement between Netradyne and Customer. At a high level, this includes- - The Driveri hardware - Driveri service and feature sets depending on subscriber plans and territory	Teletrac/Vontier	31-Mar-22
Service Scope	Is there a written contract for the data processing you carry out related to those services that addresses the GDPR requirements? Please provide date of contract, any contract reference and the contract end date (if any).	Yes. The Strategic Market Agreement ("Agreement"), dated as of February 17, 2022 (the "Effective Date"), is by and between Customer US Ltd., a Delaware Corporation ("Customer") and Netradyne, Inc., a Delaware corporation ("Netradyne").	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	What personal data do / will you process? Please note this question includes ALL information processed on behalf of Customer and specifically includes customer data and / or employee personal data processed on behalf of any Customer/OpCo ("Restricted Data").	The following personal data will be collected and processed: •Video footage (no live view); •Telematics and analytics/associated metadata to the Events (including dates and times of the Events); •Location data (no live tracking); •Driver ID, name/DSP Company name. •Pedestrian faces and Vehicles license plates - This is Blurred	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	What is the source of the data that you (will) process? E.g. Customer, you or a 3rd party? For any 3rd party bought-in data, explain the contractual arrangements you have in place and how you ensure GDPR compliance in relation to such data.	Video footage, sensor data and Driver details uploaded from Driveri devices and customer systems.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	If you (will) supply personal data to us or (will) collect personal data on our behalf, how is this collected? For any personal data you supply to us, explain the process for collection and how this complies with the GDPR.	Data is collected via Video footages, Driveri app	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	What processes do / will you perform on personal data? If relevant, include details of any automated decision making or profiling on Customer's behalf.	Netradyne's Driveri processes and analyzes every minute of driving to provide fleet safety and performance analytics in real time as well as driver coaching in real time. GreenZone provides a driver score based on positive driving behaviour. Drivers are given an opportunity to weigh in on the findings to address any discrepancies or inaccuracies or provide more context.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Why is this personal data processed? For what purpose is / will such data be used?	Driver identification, co-relation of data with the fleet to provide real-time alerts	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Do you conduct any processing in relation to Restricted Data in addition to the processing identified in your existing / proposed contracts with Customer? If so, what is the nature and purpose for such additional processing? (This includes using any derivatives / adaptions of Restricted Data, including in an aggregated, pseudonymized or anonymized, linked or merged format.)	We will use additional processing for internal training and model improvements for feature enhancements	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	F	We do not collect process any special category / sensitive personal data	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Is / will any criminal convictions or offences data ("criminal data") (be) held or processed? If so, what data is this, for what purpose is it processed and what specific protections are in place?	NO	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Is / will any personal data relating to children (be) held or processed? If so, what data is this, for what purpose is it processed and what specific protections are in place?	NO	Teletrac/Vontier	31-Mar-22

Data Security/Privacy	What safeguards do you have in place to ensure Restricted Data is only processed on Customer's documented instructions?	We have pre-defined control measures for monitoring and alerting stored data in our platforms. We are also governed by ISMS policies for data security and protection.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Are there any processing activities involving Restricted Data for which you (jointly with Customer or alone) do / will determine the purposes and means of processing? If so, please outline the nature of these arrangements and what personal data this impacts.	This will need business inputs on the engagement with Customer	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	What level of assistance are you able to provide Customer in relation to the following (including details of relevant technical and organizational measures, timeframes, contact points and deliverables / documentation we can expect to receive):	This will need business inputs on the engagement with Customer	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Customer's obligation to respond to data subject requests? In particular, explain how your systems and processes are set up to deal with requests relating to: (i) information and access to personal data (ii) rectification / correction (iii) erasure (iv) restriction of processing (v) data portability (vi) objection (vii) rights in relation to automated decision-making and profiling. Please detail standard response times.	(i) Information & processes in regards to personal data can be displayed in Exhibit C of the Netradyne Driveri Terms of Service that is a part of the Reseller Agreement (ii) Netradyne will respond in a timely matter to rectify and correct necessary items. (iii) The process of erasing personal data can be reviewed in our Data Retention Policy (iv) This process can be viewed in our Data Retention Policy (v) TN has access to the user portal training platform and may view necessary footage within the time reflected in the Data Retention policy (vi) objection (?) (vii) The AI system assists with automated decision-making in regard to driver safety, profiling is not active within the system. Note: Above data is from the earlier DPIA of Amazon EU.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	ensuring compliance with the obligations under the GDPR with respect to security and data breaches?	We have 'Data Breach Response and Notification procedure' policy in place	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	data protection impact assessments (DPIAs) / consultations with data protection authorities?	We do have DPIA in place which can be tailored for TN	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	provision of information to demonstrate compliance with the GDPR, including as regards to audit rights / inspections? Please provide details as to any requirements / limitations for such audits.	Request Michael/Kristi to comment	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Please provide details of all relevant industry standards, codes of conduct and certifications you adhere to. E.g. ISO27001, UK Government Cyber Essentials scheme, approved codes of conduct and certification mechanisms under the GDPR.	Yes, Netradyne is certified under industry recognized information security standard ISO27001.	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Do you currently have a Data Protection Officer (DPO)? If you do not have a DPO, please explain why you consider this is not required and specify who else in your organization is responsible for data protection compliance.	Yes, Netradyne has appointed DPO who is responsible for all data protection compliance	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	If so, to whom does the DPO report and what is their remit?	DPO reports to CTO of the organization	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Is there a central record of processing activities maintained in a format that can be used to demonstrate processing activities to Customer? If yes, how often is this reviewed and updated? How can we access copies?	Currently we do not records of processing maintained. However the same can be maintained for TN	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Who, if anyone, in the organization at board level has responsibility for data protection and security? Please specify role and where that responsibility is documented, e.g., as part of a job description and/ or in relevant policies.	The CEO or CTO makes decisions about and approves the Company's general strategies on Personal Data protection. The Data Protection Officer (DPO) is responsible for the development and promotion of end-to-end Personal Data protection policies, as defined in DPO Job Description; and assists business in achieving their data protection goals.	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Do you have any specific internal committees, working groups, task forces or "champions" which are tasked with responsibilities for cyber security/ data protection compliance? If so, please provide details.	Netradyne Legal and privacy team monitors and govern Personal Data laws and changes to regulations working with privacy council	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Do you have an internal data protection policy (setting out the principles and legal conditions for collecting, handling, processing, sharing/ transferring and storing personal data)? If no formal policy exists, please describe your processes and procedures for addressing compliance and minimizing risk in these areas.	Yes, We have data protection policies (data collection policy, data usage policy and data retention policy).	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Have you carried out DPIAs in relation to all high risk processing activities you carry out that affect Restricted Data and implemented appropriate measures to address any risks identified? If no, please identify areas where a DPIA should be carried out and when this information will be available.		Teletrac/Vontier	31-Mar-22
Data Security/Privacy	How does your organization store personal information on behalf of Customer (e.g., electronically or in manual files or both)? Please provide details.	PII data is stored in AWS with encryption turned on, and encrypted at rest & in transit	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Does your organization allow storage of personal information on behalf of Customer on personal devices? Please provide details.	No	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	If information is stored electronically, is this within the organization or elsewhere? If elsewhere, identify the 3rd party (sub-processor) storing the data, detailing where (i.e. data center / server location) and how the data is stored and accessed.	Data is stored in AWS hosted environment in US region.	Teletrac/Vontier	31-Mar-22

Data Security/Privacy	If information is stored manually is this within the organization or elsewhere? If elsewhere, identify the 3rd party (sub-processor) storing the data, detailing where (i.e. offsite secure warehouse) and how the data are stored.	As Controller: We will never share any PII from a machine learning dataset with any third parties (other than contracted service providers to provide the Services). We have been very thoughtful about data management to comply with the principles of data minimization, built-in-privacy, end-to-end security, and visibility and transparency	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	If your organization processes sensitive personal data (or "special categories of personal data") on behalf of Customer, what special protections are used when storing this type of data?	Data confidentially and integrity controls are in place to ensure end-to-end encryption of all PII or sensitive data at rest, in transit, and store. Additional identity and access controls are in place for authorized users only which is governed by ISMS policies.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	In what format or in what medium is archived information stored?	Data is anonymized before archival. It is stored electronically in S3.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Where is the archived information stored? If it is stored with a 3rd party, identify that 3rd party (sub-processor) and where (i.e. data center / server location / offsite secure warehouse) and how it is stored.	Archived data is stored in AWS data center in US region.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Identify and describe in outline the security measures, policies and procedures in operation in your organization to keep all information processed on behalf of Customer secure. If no formal policies and procedures exist, please describe your processes and procedures for addressing compliance and minimizing risk in these areas. In particular:	A formal security and compliance governance program is implemented. Netradyne has a dedicated Information Security team. This team is responsible for the Information Security Program at Netradyne. Netradyne's internal security practices are governed by ISMS and aligned with CIS/NIST controls.	Teletrac/Vontier	31-Mar-22
Identity & Access Management	Describe the physical, administrative and technological measures, policies and procedures used in relation to physical and personnel access controls. Who has access to Restricted Data within the organization / outside the organization? How is access provided (e.g. security passes, keypads, barriers, security officers, password protection / restricted admin rights)? E.g. remote or physical access. Who authorizes such access?	NETRADYNE's security policies are defined around the principle of "least privilege" and "need-to know". Access governance is in place to protect confidentiality, integrity and availability of Netradyne data/assets. Access provision/de-provision happens based on their role and job function in coordination with HR, Asset Custodians and Asset Owners.	Teletrac/Vontier	31-Mar-22
Cryptographic Controls	Describe the physical, administrative and technological measures, policies and procedures used in relation to encryption, including the type of encryption and when it is used.	Netradyne has robust and latest encryption controls which protect data at Rest, In Transit, In Use and keys are securely managed. Robust controls are in place through server and transport layer authentication and transmission mechanisms, including certificates, HTTPS/TLS (SSL encryption), and advanced encryption security (AES). All communications to customers occur in a secure HTTPS encrypted request.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Describe the physical, administrative and technological measures, policies and procedures used in relation to anonymization/ pseudonymization. If you receive Restricted Data in this format, provide details of the nature of the data and the reason why it is received in this format. If you anonymize or pseudonymize Restricted Data before this is sent to a 3rd party, explain the nature of the data, identify the 3rd party and explain why it is sent in this format and explain the standards you adhere to / process you use.	Gaurav & Michael: Please comment	Teletrac/Vontier	31-Mar-22
Infrastructure Security	Describe the physical, administrative and technological measures, policies and procedures used in relation to firewalls and anti-virus/spyware/malware and also for ensuring security patches and updates are promptly applied.	We have defined vulnerability and patch management process in place.	Teletrac/Vontier	31-Mar-22
Product Security	Describe the physical, administrative and technological measures, policies and procedures used in relation to device security (including removable media usage, equipment disposal and offboarding procedures).	We have defined IT Asset Policy in place which covers aspects related to removable device maintenance and offboarding.	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Describe the physical, administrative and technological measures, policies and procedures used to ensure ongoing confidentiality, integrity (e.g. audit trail logs and validation processes), availability and resilience of processing systems and services.	NETRADYNE's security policies are defined and established to protect confidentiality, integrity and availability of Netradyne system.	Teletrac/Vontier	31-Mar-22
BCP & DR	Describe the physical, administrative and technological measures, policies and procedures used to restore the availability and access to personal data quickly if there is a physical or technical incident. What are your standard timeframes for restoration of availability and access to personal data in the event of a physical or technical incident?	NETRADYNE systems are hosted on AWS infrastructure which supports high availability. This will need business inputs on the engagement with Customer	Teletrac/Vontier	31-Mar-22
Security Incident Management	Do you have policies, procedures and response plans in place for detecting and dealing with data breaches? If so, what are they? If you do not have a formal plan, describe your processes and procedures for facilitating a quick and effective response to a data breach, including for: • data breach detection, investigation and mitigation • data breach remediation and review • notifying customers of data breaches and providing assistance • claims management • liaising with insurers • (where you are data controller) dealing with regulators and affected data subjects, and • PR response	We have 'Data Breach Response and Notification procedure' policy in place.	Teletrac/Vontier	31-Mar-22

Data Security/Privacy	How do you check that there has been no internal unauthorized access to personal data? What data audit facilities / mechanisms / testing are in place? With particular reference to any systems that process Restricted Data, please detail: • your processes for early detection of security vulnerabilities and data breaches • your processes for monitoring the effectiveness and resilience of your IT systems • the date of the most recent penetration testing exercise • what the outcome of that exercise was, and • the testing cycle/ when the next test is scheduled for.	Data confidentially and integrity controls are in place to ensure end-to-end encryption of all PII or sensitive data at rest, in transit, and store. Access controls and governance are in place. We have a strong Vulnerability Management program which includes periodic internal / external vulnerability assessments and penetration test on our IDMS Solutions to proactively identify, remediate and govern potential vulnerabilities.	Teletrac/Vontier	31-Mar-22
Security Incident Management	Do you have policies and procedures in place to report data breaches to Customer and what is the standard notification timeframe? Please specify mode of communication, who from your side would typically send this and any standard notification information to be provided.	We have 'Data Breach Response and Notification procedure' policy in place. Netradyne standard notification time is 72 Hrs.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	How long do you retain Restricted Data for (including post-contract / services)? Please attach relevant retention policies / schedules. If you retain any Restricted Data after the end of the services / your contract with us, what is the reason(s) for retention?	Videos including inward cameras can be retained for long term after anonymization based on chosen retention policy. (Type A, B, A_C).	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	How do you ensure that retention periods are followed? How do you monitor compliance with retention policies / schedules?	It is monitored through automated reports.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Can you easily and securely return all Restricted Data to us and delete all copies on your systems on our request? Detail any restrictions or exceptions to this.	It depends upon the Data retention policy customer chooses	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	What format(s) are you able to use for the transfer of Protected Data back to us?	This will need business inputs on the engagement with Customer	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	What are your standard timeframes for return and deletion of personal data to customers / clients?	We follow DRP and discuss with customer	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	How do you destroy personal information? Who authorizes destruction? Who carries out destruction? What agreements are in place with contractors who provide shredding and destruction facilities/services?	This will need business inputs on the engagement with Customer	Teletrac/Vontier	31-Mar-22
TPRM	Are any of your processing activities carried out by 3rd parties (sub-processors)? List them and describe the processes and location of the provider and the data.	Amazon Web Services Data Hosting USA Netradyne, India Engineering and Support - India Concentrix Customer Service - India Elancer Data Labeling - India	Teletrac/Vontier	31-Mar-22
TPRM	Who authorizes these processing activities?	This needs several line of approval such as function head, Infosec and DPO etc.	Teletrac/Vontier	31-Mar-22
TPRM	What due diligence / pre-contract audits are carried out on these sub-processors?	We have vendor due diligence process in place to assess vendor organization security posture	Teletrac/Vontier	31-Mar-22
TPRM	Are written agreements in place covering these arrangements? Do these flow down the provisions of our agreement with you and include the mandatory GDPR provisions (e.g. in GDPR Article 26 / 28)?	Kristi	Teletrac/Vontier	31-Mar-22
TPRM	Outline the security measures under which each subcontractor / sub-processor must operate.	All subcontractor / sub-processor are expected to bound by Netradyne's information security and privacy policies	Teletrac/Vontier	31-Mar-22
TPRM	Do the subcontractors / sub-processors used by your organization use any other organization to perform that service on their behalf? If so, list the organization and any written arrangements in place with regards to the services these 3rd parties offer.	No	Teletrac/Vontier	31-Mar-22
TPRM	How is compliance by subcontractors / sub-processors and their staff monitored?	We conduct annual TPRM review and assessment	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Do you transfer data (a) cross-departmentally; (b) intra-group; and/or (c) to 3rd parties outside the organization?	NA	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	How is data transferred (e.g., encrypted email, secure fax)? What security measures do you use to secure data in transit?	• Data is processed in device and transferred to cloud, All personal data is encrypted both in transit and at rest • In Transit – TLS 1.2 or above • At Rest (Cloud) – AES 256	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	In what countries are those people to whom you disclose the information (whether inside the organization or external) located?	Yes, all of the processors/sub-processors listed above are in India.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Where data is transferred outside the EEA, why this necessary?	Data Hosting Engineering and Support Customer Service Data Labeling	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Where data is transferred outside the EEA, what measures are used to ensure compliance with the GDPR (including which approved transfer mechanisms are used)? Are written agreements always used?	Netradyne will have an Intra-Group Data Transfer Agreement with its subsidiary (including an internal transfer impact assessment), and will have DPAs in place with its processor and subprocessor. These agreements will include SCCs as the data transfer mechanism, again because the data itself is hosted in the US by AWS.	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	Do you transfer any "special categories of personal data" outside the EEA? If so, where, to whom and for what purposes.	No	Teletrac/Vontier	31-Mar-22
Data Security/Privacy	How do you ensure that onward transfers of Restricted Data by subcontractors (or other 3rd parties) are legally compliant and secure?	Netradyne will have an Intra-Group Data Transfer Agreement with its subsidiary (including an internal transfer impact assessment), and will have DPAs in place with its processor and subprocessor.	Teletrac/Vontier	31-Mar-22
Training & Awareness	Do the staff in your organization receive training on data protection and other relevant law (i.e.. ePrivacy laws)? If so, please describe the nature of the training given, when it is given and identify who is responsible for carrying out the training.	Yes, we have robust security awareness and training program to educate employees on various aspect which includes data privacy and information security. Netradyne InfoSec & Privacy team are responsible for conducting awareness trainings.	Teletrac/Vontier	31-Mar-22
Training & Awareness	Are refresher courses held? If so, please describe the nature of the training given, when it is given, identify who is responsible for carrying out the training and who is directed to attend.	Yes, we have formal awareness training given to all employees of the organization during HR orientation and once in a year as well. Along with annual awareness program, we do conduct quiz and other awareness campaign.	Teletrac/Vontier	31-Mar-22

Training & Awareness	Are staff aware that unlawful access to and/or disclosure of personal data is prohibited? Describe how this is communicated and enforced.	Yes Employees are aware of the action, this is communicated via training	Teletrac/Vontier	31-Mar-22
Training & Awareness	Do you impose training requirements on subcontractors / sub-processors that access Restricted Data? If so, please describe the nature of the training given, when it is given and identify who is responsible for carrying out the training.	During due-diligence and TPRM, we do check subcontractor's employee awareness program	Teletrac/Vontier	31-Mar-22
Training & Awareness	Do you keep training records of all such staff training that you undertake? Please provide details.	Yes, attendance and training invite captured as artifact	Teletrac/Vontier	31-Mar-22
Training & Awareness	What measures do you take to ensure the reliability of staff who have access to Restricted Data?	Netradyne implements back ground checks for all staffs. Access are provisioned based on RBAC and Least Privileged. Periodic access reviews are incorporated.	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Has your organization (or a sub-processor you have engaged / are proposing to engage to process Restricted Data) experienced any personal data breach involving personal data within the last 5 years? If yes, please provide a general description of the incident, outcome and any remedial action you have taken in response.	No, Netradyne has not experienced any personal data breach in last five years	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Have you ever been audited, investigated or had other enforcement action taken against you by a data protection authority or other regulator in relation to data or security issues? Please provide details of the issue / incident, outcome and any remedial action you have taken in response.	NO	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Has your organization received any complaints from data subjects in respect of its data processing activities in the last 5 years? If so, please provide a general description of the nature of the complaint, how it was resolved and what (if anything) you did to change your policies and procedures in response.	NO, Netradyne has not received any complaints from data subjects in respect of its data processing activities	Teletrac/Vontier	31-Mar-22
Governance Risk & Compliance	Do you hold a current insurance policy covering cyber risks? If so, please provide details of insurance provider, policy coverage and limits of liability.	Yes. Our Cyber insurance covers these areas – General Aggregate Liability Loss of Digital Assets Network security and Privacy Liability Coverage Electronic media liability	Teletrac/Vontier	31-Mar-22
Netradyne Info	Legal tax name	Netradyne, Inc.	SiteOne	11-Aug-23
Netradyne Info	DBA name	N/A	SiteOne	11-Aug-23
Netradyne Info	DUNS Number	N/A	SiteOne	11-Aug-23
Netradyne Info	Taxpayer Federal ID #	47-4998956	SiteOne	11-Aug-23
Netradyne Info	Address	9171 Towne Centre Dr #110, San Diego, CA 92122	SiteOne	11-Aug-23
Netradyne Info	Main telephone number	1 (833) 476-9663	SiteOne	11-Aug-23
Netradyne Info	Primary Contact name and title	Frank Lancaster, Enterprise Sales Manager	SiteOne	11-Aug-23
Netradyne Info	Primary Contact telephone number	501-554-4670	SiteOne	11-Aug-23
Netradyne Info	Primary Contact email address	frank.lancaster@netradyne.com	SiteOne	11-Aug-23
Netradyne Info	Primary Contact years with company	1 year	SiteOne	11-Aug-23
Netradyne Info	Company website address	https://www.netradyne.com	SiteOne	11-Aug-23
Product Features-HW	Capability to scale video resolution up or down	Netradyne has the ability to provide a limited number of 1080 HD alert videos that are prioritized by risk. Alternatively, we can supply all alert videos at 720p.	SiteOne	11-Aug-23
Product Features-HW	121° semi-wide angle front facing camera	Our forward facing video is as follows: 74 degrees (H) 57 degrees (v) 90 degrees (DI). This has been optimized for Forward collision warning, following distance, and the upcoming pedestrian collision warning.	SiteOne	11-Aug-23
Product Features-HW	Minimum 40 hours of 1080p video storage	Our standard offering provides 100 hours of rolling drive time storage on device.	SiteOne	11-Aug-23
Product Features-HW	Operating temperature -20° to 65° C	Our standard operating temperature is -5 degrees celcius to 55 degrees celcius.	SiteOne	11-Aug-23
Product Features-HW	Automatic over-the-air firmware updates	These are sent as hotfixes and planned releases.	SiteOne	11-Aug-23
Product Features-HW	Install kit includes bracket for mounting to the windshield with industrial-grade adhesive tape	We have two mounting brackets that are specified by vehicle type.	SiteOne	11-Aug-23
Product Features-HW	Inward-facing audio speaker for optional in-cab alerts	This is confirgurable by users with the proper permissions and includes audible tones and verbal cues.	SiteOne	11-Aug-23
Product Features-HW	Inward-facing microphone for optional audio capture	This is disabled by default, but can be enabled by a user with the proper permissions.	SiteOne	11-Aug-23
Product Features-HW	Automatic video footage upload of harsh braking, acceleration, turns, crashes	These are availble for supervisor visibility within the web portal known as IDMS.	SiteOne	11-Aug-23
Product Features-HW	Stores continuous recordings on-camera, available for over-the-air retrieval on demand	These are referred to as Event Access requests within the IDMS portal.	SiteOne	11-Aug-23
Product Features-HW	Ability to store and forward data when outside of cellular coverage	This is standard functionality for the Driveri device.	SiteOne	11-Aug-23
Product Features-HW	Ability to self-install (describe the installation process for your camera hardware)	Our Field Engineering team will assist with installer training and documentation.	SiteOne	11-Aug-23
Product Features-HW	No hard-wiring into vehicle required	Installation methods can utilize the OBD2, JBUS, RP1226 or an add-a-fuse.	SiteOne	11-Aug-23
Product Features-HW	Automatic association of telematics equipped vehicle	This is completed through integration with the telematics provider.	SiteOne	11-Aug-23
Product Features-HW	Real-time vehicle telemetry (position, engine status and diagnostics update continuously, in real-time	This data is provided every 10 seconds. We have plans to release every second GPS updates within the next week.	SiteOne	11-Aug-23

Product Features-HW	High-speed 4G LTE wireless connectivity	Please see the attached technical spec sheets for more information.	SiteOne	11-Aug-23
Product Features-HW	Ability to increase dash cam video storage capacity up to 100 hours	Storage capacity can be increased up to 200 hours.	SiteOne	11-Aug-23
Product Features-HW	Internal 1300mAh battery for fallback power when vehicle is off	Our internal supercapacitor provides additional power when the vehicle experiences a sudden loss of power. Our device has multiple power states for when the vehicle is parked/in on standby to ensure battery health.	SiteOne	11-Aug-23
Product Features-HW	Ability to alert via SMS/email when dash cam is disconnected	This is available within the Device Health dashboard and personal notifications.	SiteOne	11-Aug-23
Product Features-HW	Ability to alert via SMS/email when in-cab camera is obstructed	This is available within the Device Health dashboard and personal notifications.	SiteOne	11-Aug-23
Product Features-HW	Ability to provide audible in-cab alert when camera is obstructed	This is an optional in-cab alert that can be configured by a user with the proper permissions.	SiteOne	11-Aug-23
Product Features-HW	Provide a report on camera health and stability	This is available within the Device Health dashboard.	SiteOne	11-Aug-23
Product Features-HW	Provide a visual report when cameras are misaligned, poorly installed, or obstructed	This is currently available within the Alerts screen to review Obstructed events.	SiteOne	11-Aug-23
Product Features-HW	Automated real-time device health monitoring and reporting	This is core functionality for the Device Health monitoring. A device is flagged if it has not reported within 24 hours.	SiteOne	11-Aug-23
Product Features-HW	Available engine immobilizer	Netradyne welcomes the opportunity to further discuss this with SiteOne.	SiteOne	11-Aug-23
Product Features-HW	Availability for drivers to record and upload footage on-demand	Driver- initiated feature button on the camera that can send a video clip to a driver manager or management team.	SiteOne	11-Aug-23
Product Features-HW	Available NFC card reader	We provide a device called Beacons. Beacons are wireless transmitters that use low-energy Bluetooth technology to send signals to other smart devices that are nearby such as the Driver•i Camera. The purpose of this feature is to associate a Driver to the vehicle during their drive time.	SiteOne	11-Aug-23
Product Features-HW	Available wireless Driver ID token	We provide a device called Beacons. Beacons are wireless transmitters that use low-energy Bluetooth technology to send signals to other smart devices that are nearby such as the Driver•i Camera. The purpose of this feature is to associate a Driver to the vehicle during their drive time.	SiteOne	11-Aug-23
Product Features-HW	Available integrated asset tracking hardware	This is available through our partnership/integration with Geotab.	SiteOne	11-Aug-23
Product Features-HW	Available integrated telematics hardware	This is provided through our Netradyne D-210 device.	SiteOne	11-Aug-23
Product Features-HW	Describe process to integrate additional cameras into your system made by you and by third parties	Netradyne leverages our Driveri D Hub X which provides additional connectivity by leveraging 4-pin aviation plug connectors. The DHub X has it's own internal embedded storage for these additional camera views.	SiteOne	11-Aug-23
Product Features-SW	Fully hosted cloud-based fleet management tool	Our entire stack is hosted by the secure and scalable AWS architecture which are located primarily within US West 1.	SiteOne	11-Aug-23
Product Features-SW	Default retention of all data for lifetime of the account	This is further detailed within the Contract/MSA between the customer and Netradyne.	SiteOne	11-Aug-23
Product Features-SW	Customizable data retention policies	We welcome the opportunity to discuss this with SiteOne. Netradyne has worked in partnership with our customers regarding this in the past.	SiteOne	11-Aug-23
Product Features-SW	Tag-based structure to create hierarchical groups of users and assets to allow for flexible administration of sub-organizations	Netradyne can support this through Groups or organizational hierachy within IDMS.	SiteOne	11-Aug-23
Product Features-SW	Customizable user roles and permissions settings	There are 5+ default user roles and permissions within IDMS. Custom roles can also be created.	SiteOne	11-Aug-23
Product Features-SW	Ability to configure per-vehicle camera settings for audio recording, voice coaching, and AI detection	Configurations can be set at the fleet and per vehicle level.	SiteOne	11-Aug-23
Product Features-SW	Support for SMS, email and webhook alerts	These are set within personal notifications by the user.	SiteOne	11-Aug-23
Product Features-SW	Ability to export reports to .csv	Netradyne has 20+ core reports that can be exported to either PDF or Excel/CSV.	SiteOne	11-Aug-23
Product Features-SW	Ability to brand dashboard by adding custom logo	This is set by the Netradyne Ops team when the account is configured.	SiteOne	11-Aug-23
Product Features-SW	Platform-wide search capability	Users can access modules within IDMS to search by driver, vehicle, etc.	SiteOne	11-Aug-23
Product Features-SW	Mobile Applications	Supplier Detailed Response	SiteOne	11-Aug-23
Product Features-SW	Driver application (iOS and Android)	Netradyne supports a Driver, Supervisor, and Installer mobile applications.	SiteOne	11-Aug-23
Product Features-SW	Fleet management application for managers, admins, installers, mechanics, etc. (iOS and Android)	This app is available on IOS and Android. We can also support MDM solutions.	SiteOne	11-Aug-23
Product Features-SW	Support for real-time two-way messaging between drivers and fleet managers	This is available through Supervisor Notes and Driver feedback.	SiteOne	11-Aug-23
Product Features-SW	Automatic over-the-air upgrades	These are sent as hotfixes and regular releases. No user input required.	SiteOne	11-Aug-23
Product Features-SW	Ability to review harsh event (speeding, harsh turn, harsh acceleration, harsh stop, rolling stops) footage	Supervisors can also provide alert feedback to improve detection models.	SiteOne	11-Aug-23
Product Features-SW	Ability to review a distracted driving event, tailgating event, or near-forward collision footage	All our supported alert types and users can provide alert feedback to improve detection models.	SiteOne	11-Aug-23
Product Features-SW	APIs & Integrations	Supplier Detailed Response	SiteOne	11-Aug-23
Product Features-SW	Support for APIs to pull safety and coaching information from the platform	This is supported through our Coaching Sessions endpoint within our Rest APIs.	SiteOne	11-Aug-23
Product Features-SW	Publicly documented REST-based API	https://developer.netradyne.com/docs/api-documentation/oyuxlbkt02nc7-authentication	SiteOne	11-Aug-23
Product Features-SW	Available integration with Ford Data Services	Netradyne welcomes the opportunity to further discuss this with SiteOne.	SiteOne	11-Aug-23
Product Features-SW	Available integration with Holman	We have had previous discussions with Holman before regarding customer integration requirements. We welcome the opportunity to further discuss this with SiteOne.	SiteOne	11-Aug-23
Product Features-SW	Available integration with Maximo	We welcome the opportunity to further discuss this with SiteOne.	SiteOne	11-Aug-23
Product Features-SW	Available integration with Geotab	Netradyne has an ELD, SSO, and several MyGeotab application level integration with Geotab. We are happy to further discuss this in future conversations.	SiteOne	11-Aug-23
Product Features-SW	Available integration with DispatchTrack	We welcome the opportunity to further discuss this with SiteOne.	SiteOne	11-Aug-23
Product Features-SW	Extended marketplace of 3rd party applications	https://www.netradyne.com/integrations	SiteOne	11-Aug-23
Product Utility	Harsh Event Detection	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to detect harsh events (harsh turn, harsh acceleration, harsh brake, crash)	This is based upon specified G-force thresholds.	SiteOne	11-Aug-23
Product Utility	Ability to playback footage of all cameras	Supported by IDMS' Alert Video player.	SiteOne	11-Aug-23
Product Utility	Ability to detect unbuckled seat belt & support in-cab audible alerts	This is known as Seatbelt compliance within IDMS.	SiteOne	11-Aug-23
Product Utility	Ability to configure harsh event sensitivity based on vehicle type	This is configurable by the Netradyne Ops and Solution Engineering teams.	SiteOne	11-Aug-23

Product Utility	Provide data overlay with videos	Annotations and metadata provide rich context to risk detections that include telematics data and objection detection insights.	SiteOne	11-Aug-23
Product Utility	Provide driver training materials for in-cab alerts and how the system works	This is provided by our Customer Success team.	SiteOne	11-Aug-23
Product Utility	AI Event Detection	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to detect distracted driving, follow-distance violations, rolling stops, and near collisions using AI	All are supported by the Netradyne device and are fully supported by AI models on the device (edge computing). No human review is required/needed.	SiteOne	11-Aug-23
Product Utility	Ability to use proactive, in-cab alerts to improve driver safety	Netradyne supports 25+ internal (driver behavior) and external alerts that can be configured to include in-cab alerts.	SiteOne	11-Aug-23
Product Utility	Real-time detection of follow-distance violations, inattentive driving, forward collision warning, mobile usage, eating, drinking, and no seatbelt	Netradyne supports all of the following and provides additional context and causality of these events types through our sub alert categories.	SiteOne	11-Aug-23
Product Utility	Ability to warn the driver multiple times of safety issues before raising awareness to the dashboard	Netradyne refers to this as our self-coaching workflow which empowers driver and allows supervisors to configure their dashboard alert settings (video upload thresholds).	SiteOne	11-Aug-23
Product Utility	Safety event footage automatically uploaded to a dashboard	This is based on the risk severity and threshold configurations of the fleet.	SiteOne	11-Aug-23
Product Utility	Describe how you use AI/ML to interpret video content	Our solution is powered by over 32 billion minutes of analyzed drive time that leverages computer vision to visually detect high risk driving behaviors such as distraction, tailgating (following distance), stop sign violation, rolling stops, and near collisions. The Driveri solution analyzes every second of every driving mile. This allows Driveri Device to analyze and index driver and external factors/behaviors to identify and warn a driver of poetntial risks before they impact a driver or a third-party. Advanced AI is consistent; the same algorithm is used for the same time frame,compared to human reviews with natural error. Driveri uses the power of AI to gain full visibility into every incident; it provides actionable data to automatically coach and improve safety performance across any fleet, developing proactive drivers and futureproofing your safety program. We utilize Machine Learning to continually improve this process of image acquisition, image processing, and object detection over time.	SiteOne	11-Aug-23
Product Utility	Identify and report distracted driving without a critical event	The IDMS portal allows users to review specific event videos, view trends via Dashboard, and look at data over time via reports.	SiteOne	11-Aug-23
Product Utility	Provide data overlay with videos	Annotations and metadata provide rich context to risk detections that include telematics data and objection detection insights.	SiteOne	11-Aug-23
Product Utility	Speeding Detection	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to detect when driver is above speed limit for an extended period of time	Neteradyne visually detects over 15 different speed sign variations and leverages Netradyne and third-party map data to provide unprecedented accuracy.	SiteOne	11-Aug-23
Product Utility	Ability to configure thresholds for alerts based on speeding severity and duration	These are set by a user with th proper permissions.	SiteOne	11-Aug-23
Product Utility	Ability to support audible in-cab alert for speeding	This in-cab alert is fully supported.	SiteOne	11-Aug-23
Product Utility	Ability to update speed limit through a map interface	This is performed by our Operations team. Neteradyne visually detects over 15 different speed sign variations and leverages Netradyne and third-party map data to provide unprecedented accuracy.	SiteOne	11-Aug-23
Product Utility	Coaching Workflow	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to preview safety event footage in a consolidated page to determine coaching need	This can be performed on an individual driver page or through the Managed Coaching dashboard.	SiteOne	11-Aug-23
Product Utility	Ability to provide automatic coaching assignments	This is supported with our Recommend Coaching workflow and is based on Group and Hierarchy specification.	SiteOne	11-Aug-23
Product Utility	Ability to automatically share video events with drivers in a dedicated driver portal	Alerts can be shared with the Drivers to their mobile app.	SiteOne	11-Aug-23
Product Utility	Ability to aggregate similar types of safety events into one coaching queue	This is core functionality of IDMS.	SiteOne	11-Aug-23
Product Utility	Ability to mark safety events as positive reinforcement	Supervisors have the option to convert event videos to DriverStars which recongnize and reward drivers for safe driving behaviors. DriverStars are also automatically detected for situational and durational driving tendencies.	SiteOne	11-Aug-23
Product Utility	Ability to tag admins to coach on safety events	Netradyne welcomes the opportunity to further discuss this coaching workflow with SiteOne.	SiteOne	11-Aug-23
Product Utility	Provides coaching summary report to drive accountability with coaching efforts - includes average time to coach	This is available within our Managed Coaching Sessions report.	SiteOne	11-Aug-23
Product Utility	Ability to auto-assign coaches to safety event, and notify them via email.	Netradyne welcomes the opportunity to further discuss this coaching workflow with SiteOne.	SiteOne	11-Aug-23
Product Utility	Ability to report metrics on coaching effectiveness, based on repeat behaviors of coached events.	This is available within our Managed Coaching Sessions report.	SiteOne	11-Aug-23
Product Utility	Video Retrieval	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to monitor & report on safe/efficient driving behaviors (Idle time, stop time, breaking, acceleration, speeding, cornering / swerving, high torque, over speed, green band, cruise control activation, anticipation	This is covered within our Fleet Tracking and Alert Decoration feature sets.	SiteOne	11-Aug-23
Product Utility	Ability for video to be downloaded directly from the platform	Videos are downloaded as MP4 files.	SiteOne	11-Aug-23
Product Utility	How long is retrieved video kept on the platform?	90 days plus current month	SiteOne	11-Aug-23
Product Utility	What is the average delay between a video request to the time it is available?	a few minutes.	SiteOne	11-Aug-23
Product Utility	Ability for video to be retrieved directly from the dashboard without customer support	This is performed by any user with the proper permissions.	SiteOne	11-Aug-23
Product Utility	Provide the minimum and maximum time ranges for which video can be retrieved?	90 days plus current month	SiteOne	11-Aug-23
Product Utility	Ability for camera to record video footage when vehicle is idling	The Neteradyne device can be configured to continue recording for 15 minutes to 10+ hours without vehicle movement.	SiteOne	11-Aug-23
Product Utility	List all telematics data points that are captured with video	Location, speed, RPM, throttle, brack pedal position, ABS, cruise control, blinker. Odometer can be pulled through a seprate report.	SiteOne	11-Aug-23
Product Utility	Is your system dependent on a 3rd party provider for uploading videos?		SiteOne	11-Aug-23
Product Utility	Support for automatic upload of safety events	This is set by SiteOne superusers and their thresholds for dashboard alerts.	SiteOne	11-Aug-23

Product Utility	List types of safety events the system automatically uploads video for?	Speeding, distraction, stop sign, traffic light, drowsy, High G, and many more	SiteOne	11-Aug-23
Product Utility	How long are safety event videos kept on the platform?	90 days	SiteOne	11-Aug-23
Product Utility	Can video be purged from platform? Describe details	You would need to request in writing to our team.	SiteOne	11-Aug-23
Product Utility	GPS Tracking	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Capture location of event in real-time	Location is available and is updated every 10 seconds.	SiteOne	11-Aug-23
Product Utility	Can location of safety event to visualized on a map and during a trip?	This is available within the metdata section of the Alert Video player.	SiteOne	11-Aug-23
Product Utility	Ability to view all assets and vehicles within a time range, date, and address	This is supported through our Fleet Tracking module.	SiteOne	11-Aug-23
Product Utility	Ability to create custom geofences by selecting custom areas on map?	This is supported through our Fleet Tracking module.	SiteOne	11-Aug-23
Product Utility	Support for time-on-site reporting	This is currently planned for 1H 2024. Netradyne welcomes the opportunity to further discuss this with SiteOne to potentially modify the current timelines.	SiteOne	11-Aug-23
Product Utility	Support for trip history and view dashcam footage of trip	This is supported through our Fleet Tracking module.	SiteOne	11-Aug-23
Product Utility	Support for route-planning and optimization	This is covered within our partnership/integration with Geotab.	SiteOne	11-Aug-23
Product Utility	Support for real-time dispatch of closest vehicle	This is covered within our partnership/integration with Geotab.	SiteOne	11-Aug-23
Product Utility	Ability to determine if fleet vehicles were near a location at a historical point in time	This is supported through our Fleet Tracking and Event Access modules.	SiteOne	11-Aug-23
Product Utility	Support for dispatching driver routes, and updates, in real-time	This is covered within our partnership/integration with Geotab.	SiteOne	11-Aug-23
Product Utility	Reporting on planned vs. actual performance in route execution	This is covered within our partnership/integration with Geotab.	SiteOne	11-Aug-23
Product Utility	Ability to share live location of vehicle. Describe details of this capability	This is covered within our Fleet Tracking module.	SiteOne	11-Aug-23
Product Utility	Video Live Stream	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to offer minimum 5 minutes of live stream	A single individual live stream is limited to 1 minute, afterwards another additional minute and so on can be requested.	SiteOne	11-Aug-23
Product Utility	Ability to offer option for audio capture	This is disabled by default, but can be enabled by a user with the proper permissions.	SiteOne	11-Aug-23
Product Utility	Ability to offer option for road-facing or dual-facing live stream	Currently, we support a single camera view to be streamed. We welcome the opportunity to further discuss this with SiteOne.	SiteOne	11-Aug-23
Product Utility	Safety Scores	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to score drivers on safety	This is supported through Netradyne's GreenZone score which incorporates safe and risk driving behaviors/events.	SiteOne	11-Aug-23
Product Utility	Ability to configure driver safety scoring methodology based on what is important to my organization	Netradyne is currently developing support for a custom fleet score and welcomes the opportunity to discuss this further with SiteOne.	SiteOne	11-Aug-23
Product Utility	Does your tool provide wizard to help me easily and accurately tune driver scoring?	Netradyne is currently developing support for a custom fleet score and welcomes the opportunity to discuss this further with SiteOne.	SiteOne	11-Aug-23
Product Utility	Ability to include defensive driving to positively impact the safety score	These are known as DriverStars and are automatically detected/awarded to drivers based on situational and durational driving actions.	SiteOne	11-Aug-23
Product Utility	Provide driver performance dashboard and reporting	Supported through the Driver Dashboard and Reports Central modules within IDMS.	SiteOne	11-Aug-23
Product Utility	Ability to "Gamify" our safety program to provide a positive incentive for our drivers to be safer and more efficient	Netradyne supports this through our GreenZone scoring and Driver mobile applications.	SiteOne	11-Aug-23
Product Utility	Safety Reports	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Provide a Safety Dashboard that shows how well my organization is doing period over period. This dashboard should easily highlight areas that need attention and provide drill down into detail for actioning.	This is supported through our Driver Dashboard and GreenZone Statistics modules.	SiteOne	11-Aug-23
Product Utility	Provide ability to report on different safety risk factors such as (Speeding, Distracted Driving, Crashes, Harsh Driving, Collision Risks, Traffic Signs & Signals & Policy Violations) and report on these at multiple levels of granulariy such as by vehicle, driver or segmentation and provide drill down for actioning?	This is best provided by our Alerts report and Executive Summary reports. There are 20+ additional reports to be leveraged within IDMS.	SiteOne	11-Aug-23
Product Utility	Provides reports that show count of safety events at aggregate level and per driver or vehicle basis	These reports are available through our Reports Central module.	SiteOne	11-Aug-23
Product Utility	Provide tag-based reports	These reports are available through our Reports Central module and various Dashboards within IDMS.	SiteOne	11-Aug-23
Product Utility	Provide a coaching report showing timeliness of coaching	This is best supplied through our Managed Coaching report.	SiteOne	11-Aug-23
Product Utility	Provide report showing effectiveness of coaching (Ex. repeat behaviors). Does this report provide detail for actioning?	This is best supplied through our Managed Coaching report.	SiteOne	11-Aug-23
Product Utility	Ability to report on Events with Unassigned drivers?	Supported by our Unassigned Drive Time report.	SiteOne	11-Aug-23
Product Utility	Ability to monitor & report on safe/efficient driving behaviors (Idle time, stop time, breaking, acceleration, speeding, cornering / swerving, high torque, over speed, green band, cruise control activation, anticipation)	We currently support much of this through our Vehicle Activity and Driver Statistics reports. Alert Decoration will provide the remaining data points listed.	SiteOne	11-Aug-23
Product Utility	Driver Assignment	Supplier Detailed Response	SiteOne	11-Aug-23
Product Utility	Ability to accurately auto-assign drivers based off facial recognition	We refer to this as Visual Login System.	SiteOne	11-Aug-23
Product Customer Services	Ability to send feedback directly to product development teams	Through your assigned Customer Success Manager.	SiteOne	11-Aug-23
Product Customer Services	Public status page documenting system health and past incidents	Through your assigned Customer Success Manager and our internal Ops teams.	SiteOne	11-Aug-23
Product Customer Services	Ability to subscribe to real-time automatic system health status updates	These are provided as banner annoucements within IDMS and email subscriptions.	SiteOne	11-Aug-23
Product Customer Services	Describe your technical support services	Netradyne provides tiered support; Level 1, 24-hour technical support and Level 2 advanced hardware and software technical support.	SiteOne	11-Aug-23

Product Customer Services	Describe your implementation support services	Multi-faceted approach to implementation including installation and onboarding services,and ongoing program support.Netradyne provides a dedicate team for implementation that includes a field engineer and Customer Success Manager to ensure successful implementation.	SiteOne	11-Aug-23
Product Customer Services	Provide your hardware failure rate	Netradyne's current device failure rate is ~1%.	SiteOne	11-Aug-23
Product Customer Services	Describe your hardware warranty policy and warranty exchange processes	The device is warrantied through the life of the contract.	SiteOne	11-Aug-23
Product Customer Services	Describe how you actively solicit feedback from customers and implement those ideas in future hardware/systems	Netradyne partners with our customer through our Customer Success and Solution Engineering teams. Additionally, we have a Customer Advisory Board that meets on a regular basis.	SiteOne	11-Aug-23
Product Customer Services	Describe how you communicate industry information to your customers	Through our Customer Advisory Services team.	SiteOne	11-Aug-23
Governance Risk & Compliance	SOC2 Type 2 Security Certification	Netradyne has adopted and implemented ISMS controls and our security infrastructure is certified with ISO 27001. Report can be shared under NDA. We have external audits conducted on a annual basis to review our internal controls and maturity in the organization.	SiteOne	11-Aug-23
Cryptographic Controls	All communications secured by SSL with 256-bit AES encryption	In transit - SSL At rest – AES-256 On back up – AES-256	SiteOne	11-Aug-23
Identity & Access Management	Hardware runs digitally signed firmware		SiteOne	11-Aug-23
Identity & Access Management	Support for SSO (Single Sign On)	We use self-managed accounts and we also allow SSO	SiteOne	11-Aug-23
Cryptographic Controls	Data secured via SSL (256-bit, military-grade encryption)	In transit - SSL At rest – AES-256 On back up – AES-256	SiteOne	11-Aug-23
Identity & Access Management	Support for MFA (Multifactor Authentication)	We enforce SaaS users to use a strong password. For REST services usage on IDMS, OIDC based authentication is supported where internal admin roles are equipped with MFA at this point of time. This can be provisioned as per the contract.	SiteOne	11-Aug-23
Governance Risk & Compliance	Does the respondent have an internal audit department that tests IT Controls on a periodic basis?	Yes, we have external certification firm conducted ISO 27001 audit and we are certified on this standard. We have matured information security practices where processes have been defined, associaetd controls are established and assessed periodicaly for continual improvements.	Quanta	3-Mar-23
Service Scope	Please provide a brief description of the technology or services under consideration and the primary functions that they will serve?	Driveri® is the most advanced vision-based driver recognition and fleet safety solution built to reward positive driving behavior and coach those areas in need of improvement. Unlike legacy platforms that rely only on G-force triggers to record video, Driveri captures every minute of every mile to deliver the insights that matter. Netradyne offers a back office application known as "IDMS." This stands for Intelligent Driver Monitoring Solution which empowers managers to recognize driver safety trends, scores, reports, and monitor/log coaching sessions.	Quanta	3-Mar-23
Service Scope	Please detail the nature of data to be transferred to, and stored in, the solution? Is any of the transferred or stored data financial, Human Resource or Health related data? Would the data referred to above fall under any NERC CIP requirements?	Within the IDMS application, users have the option to store Driver name, phone number, email, and license number. While it is reccommended to store a Driver's first and last name, all other fields are optional. The data stored within IDMS is not subject to NERC CIP. Regarding data transfers and encryption procedures: In transit - SSL / TLS 1.2 and above At rest – AES-256 On back up – AES-256 We encrypt all PII data both In-transit and at Rest.	Quanta	3-Mar-23
Service Scope	What type of software is available as an offering, and which one(s) are being provided, as a part of this assessment from these choices ? (e.g. Commercial Off-The-Shelf (COTS), Custom Developed, Cloud, Mobile, Open Source Software)	Driveri is a SaaS solution offering which is hosted on AWS Infrastructure.	Quanta	3-Mar-23
Service Scope	Who are the biggest customers using this particular service/application? How many employees do [the biggest customers using this product] have that where information is hosted?	Our largest customer operates a fleet of over 80,000 vehicles and is well known in the ecommerce/last mile delivery industries.	Quanta	3-Mar-23
Service Scope	Are references available from a few of those companies that have used this application or service(s)?	Netradyne welcomes the opportunity to connect Customer with customers of similar scope and processes.	Quanta	3-Mar-23
Governance Risk & Compliance	Is a SSAE-18 Service and Organizational Controls (SOC 2 Type II) audit performed annually for the company to review internal control processes? Is any other certification held like ISO 27001, SysTrust etc.? Please provide a copy of the report for review. Note: This question is for the primary provider, NOT the third-party cloud provider Or Data Centers.	We have adopted and implemented ISMS controls algined with NIST framework. We have external audits conducted on a annual basis to review our internal controls and maturity in the organization. A	Quanta	3-Mar-23
Governance Risk & Compliance	If SOC 2 Type II report OR ISO 27001 certification is not available to provide, is there a timeline for performing a SOC or ISO review? Please provide a detailed roadmap and expected timeline of obtaining and providing a SOC or ISO attestation.	See above.	Quanta	3-Mar-23

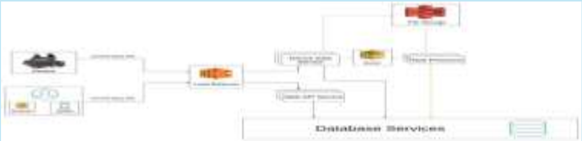
Governance Risk & Compliance	Please provide evidence of mapping of the security controls, architecture, and processes to regulations and/or standards such as COBIT, ISO, NIST 800, CSA etc., both with respect to the product and to the internal security approach.	Netradyne follows standard data protection controls such as Privacy by design, Encryption at rest and in-transit, System Hardening & backups, RBAC, Least Privilege Policy, Logging and Monitoring, Environment segregation and Vulnerability Assessments to identify, prioritize & mitigate any unauthorize system/configuration or data changes. Netradyne also abides by standard privacy controls with respect to standard requirments of data subject, data controller and data processor. The Driverl solution is a SaaS solution offering which is hosted on AWS Infrastructure.Physical security of hosting infrastructure is AWS responsibility. AWS supports security standards and compliance certifications which includes PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements. For more information please refer https://aws.amazon.com/compliance/data-center/controls/	Quanta	3-Mar-23
Vulnerability & Patch Management	Is a third-party hired periodically to perform vulnerability assessment and/or penetration testing? Please provide the frequency of the assessments and a summary report of the results.	External PEN Testing is done yearly by recognized organization following industry standards. We also conduct PEN testing internally on regular basis.	Quanta	3-Mar-23
TPRM	Does the hosting provider perform a SSAE-18 Service and Organizational Controls (SOC 2 type II) audit annually? Does the hosting provider hold any other certifications such as ISO 27001, SysTrust etc. Please provide copy of the report for review. Note: This is for the third-party cloud provider, not the primary provider.	Our hosting provider, AWS, has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014. AWS has also completed SAS70 Type II audit.	Quanta	3-Mar-23
Governance Risk & Compliance	If SOC 1 Type II report is not available to provide, is there a timeline for performing a SOC review? Please provide a detailed roadmap and expected timeline of obtaining and providing a SOC attestation.	Netradyne is not subject to SOC 1.	Quanta	3-Mar-23
Asset Management	Please describe the following technologies used for developing the application and the cloud components and technologies used for providing this service or application: . Programing languages and framework used (Open Source & Proprietary) . Operating System (OS) and Database (DB) . Other components of the technology stack the application is composed of with detail . Cloud Service components used . Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) . Private Cloud, Public Cloud, Community Cloud, Hybrid Cloud	Driveri is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS). Added some of the details below: . Programing languages and framework used (Open Source & Proprietary) --> Java, Python, C++ . Operating System (OS) and Database (DB) --> Linux, Postgres . Other components of the technology stack the application is composed of with detail . Cloud Service components used --> Object storage, Elastic Compute, Key Management Service, Application Load Balancers, Managed DB services, Queue services, Notification services . Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) --> SaaS . Private Cloud, Public Cloud, Community Cloud, Hybrid Cloud --> Public Cloud Logical Diagram:	Quanta	3-Mar-23
Governance Risk & Compliance	Is there an information security (manager) function responsible for security initiatives? Please explain Information Security organizational structure, dedicated functions, the personnel involved, and the reporting structure, organization chart etc.	We have a dedicated Information Security Team for Netradyne accountable for all Security related maturity and control implementation. The team consist of Security Engineers, Analyst, Risk and Compliance personnel reporting to our Information Security Officer.	Quanta	3-Mar-23
Human Risk Management	What are qualifications for security staff? e.g. CIA, CISSP CISA, Work Experience. Are employees required to maintain certifications within security field?	Our Staff qualifications and experiences are from large enterprises and diversified industry background. We have senior professionals with multiple industry certifications from ISC2, ISACA, IAPP, ISO, AICPA etc.	Quanta	3-Mar-23
Human Risk Management	Is background screening and training performed prior to allowing employees, contractors, or consultants access to Scoped Systems and Data?	Yes, we perform background checks on all the new employees. This covers criminal check, education check, employment check. As part of annual security awareness training, employees are made aware of their role in observing and enforcing physical security policies and procedures and reinforcing them when interacting with others in the workplace.Physical access is reviewed on periodic basis.	Quanta	3-Mar-23
TPRM	Does a contract exist with a 3rd party to manage any part of the respondent's security? If so, please list the services which are provided (e.g. vulnerability scanning, firewall or IPS management, security log monitoring)	We use Amazon Inspector and SecurityScorecard.	Quanta	3-Mar-23
Infrastructure Security	Is the network segmented to provide separation between the Internet facing servers and the internal systems? (e.g. Internet-facing servers sit in a DMZ separated from Internet by firewall, other systems such as DEV, QA etc.) Please provide high-level architecture diagram; system and other proprietary information can be redacted.	We have a multi-tenant solution, each customer data is logically separated and secured.	Quanta	3-Mar-23

Infrastructure Security	Are firewalls in use for both internal and external connections? If so, please respond and give details for each bullet and describe how the firewalls are deployed and utilized: . Do the firewalls perform stateful inspection of connections (not a packet filter firewall)? . Are the firewall policies (rule sets) defined to allow only the minimum, required ports and protocols (inbound and outbound) between the network segments listed above? . Are the firewall policies (rule sets) reviewed and verified on an annual basis by someone outside the firewall operations team?	We use AWS Security groups for cloud hosting. For office network Netradyne has Unified Threat Management with inline packet inspection firewall. The company uses cloud-hosted email office365 which comes with bundled security features. There is antimalware installed on all developer's machines and servers. Our Network is partitioned into multiple secure zones and access has been restricted as per IAM policy. We have periodic network configuration reviews performed throughout the year.	Quanta	3-Mar-23
Infrastructure Security	Are network Intrusion Detection and Prevention Systems (IDS/IPS) in use? If so, please respond and give details for each bullet and describe how the firewalls are deployed and utilized: . Are there network Intrusion Detection/Prevention System (IDS/IPS) sensors deployed? . How frequently are the sensors signatures updated? . How often are the IDS/IPS configurations reviewed?	Yes, we use enterprise scale Security Solutions and tools providing Network Security, Firewall, UTM, APT, IDS/IPS protective our systems. The controls are managed and governed by our ISMS policies and guidelines. Yes Meraki AMP (Advance Malware Protection) Sensors signatures updated Hourly IDS/IPS configurations reviewed Quarterly	Quanta	3-Mar-23
Vulnerability & Patch Management	Are vulnerability assessments, scans or penetration tests performed on internal or external networks? If so, please respond and give details as to each bulleted item is performed and describe how the bulleted items are utilized: · Are vulnerability tests (internal/external) performed on all systems at least annually?	We test applications against OWASP Top Ten vulnerabilities. We also perform penetration testing on web applications once in a quarter. We have appropriate entry and exit processes to ensure only authorized users have access to our systems at any given time. We review other processes on an ongoing basis from security perspective. External PEN Testing is done yearly by recognized organization following industry standards. We also conduct PEN testing internally on regular basis.	Quanta	3-Mar-23
Audit, Logging & Monitoring	Is security monitoring and alerting performed using a centralized Security Information and Event Management (SIEM) solution? If so, please respond and give details for each bullet as to how security monitoring and alerting is triggered and how the following components are designed and executed: . Security monitoring and alerting functions for the network infrastructure and applications . Components (list) that are included in SIEM monitoring including network, servers, databases, firewalls, web application firewalls, Access/Identity Management solutions etc. . Are automated correlation of the logs collected from various devices performed? . Are there automated alerts from this automated log correlation? . Are logs being monitored in real-time or periodically? . Are logs monitored for security policy violations and intrusion attempts?	We have centralized log monitoring and SIEM solutions implemented to collect, monitor all security related events are captured are correlated, triaged, and addressed appropriatey and governed by Security Incident response and Management process. Rely on application audit logging and AWS cloud watch logging to detect issues. This is done periodically. All Cloud and application components are included in the monitoring.	Quanta	3-Mar-23
Infrastructure Security	What other security protection mechanisms are used?	We use various tools to proactively detect vulnerabilties across endpoints, infrastructure and application across netradyne and run scans to detect issues. This scan runs automatically several times in a day. In our AWS hosted environment, Firewalls and Security Groups are configured properly to permit only the allowed acceses.	Quanta	3-Mar-23
Infrastructure Security	Will the solution require any persistent connections to the Customer network? For example, services running on the Customer network, site-to-site tunnels, VPN client connections, etc.	Users will access the Netradyne SaaS application through their web browser or IOS/Android mobile app.	Quanta	3-Mar-23
Security Incident Management	Are there documented and implemented security incident response procedures?	Security events are handled by IT or DevOps team as appropriate. DevOps team works with AWS team to close gaps where needed. IT team reviews the incident and makes required changes in configurations or announces and enforces a new policy if needed.	Quanta	3-Mar-23
Security Incident Management	How quickly are potential or confirmed security incidents reported to the customer with respect to detection and if monitoring provides 24 x 7 coverage?	This occurs in real-time. Outage notifications/security issue detection go out to affected customers via push notification as well as email.	Quanta	3-Mar-23
Asset Management	Please describe The location of the data center(s); If the data centers are co-loco or IaaS	Netradyne solution stack is hosted on AWS datacenters within the USA.	Quanta	3-Mar-23

Physical & Environmental Security	Describe the physical security controls present in the building/data center that contains Scoped Systems and Data (e.g. cameras, access card readers, access logs)	➢Periodic BCP-Fire drills convened without fail and employees are trained to manage such unforeseen conditions ➢Access to physical premises are restricted using access card. Offices are segregated internally into different zones/wing and access to those areas are provided to only associated personnel. for example, Server room can be only accessible by few handful of IT Admin personnel usin their access cards. ➢Physical premises are equipped with security, reception desk, CCTVs, security awareness posters etc. ➢Workstations are locked at the operating system level whenever unattended to prevent unauthorized access to workstations and the company network. ➢Printers and fax machines are cleared of confidential information both during work hours and after hours. Printouts are picked up promptly. ➢Doors with external access are never be propped open unless supervised maintenance work requiring unobstructed room access is underway. ➢Doors marked for Emergency Use are not used for non-emergency purposes. ➢All cabinets, drawers, credenzas, etc. containing confidential information are locked after hours of if left unattended over a period of time, such as during a meeting or lunch. ➢All paper trash is to be properly disposed of or shredded. Shred bins are placed throughout office locations to facilitate secured disposal of confidential documents. ➢CCTV cameras are installed to record activity at office entry/exit points and doorways that permit access to interior secured rooms. Access to video recording data is restricted to authorized personnel and is used only for the purposes of security enforcement and monitoring.	Quanta	3-Mar-23
Physical & Environmental Security	Is all access to the hosting facility/data center restricted to authorized personnel and logged?	Access is restricted only to authorized personnel and is logged.	Quanta	3-Mar-23
Physical & Environmental Security	Describe the environmental controls present in the building/data center that contains Scoped Systems and Data (e.g. power surge protection, temperature control, fire suppression, water/flood detection)	All facilities are equipped with adequate environmental controls to maintain systems and data. These include fire suppression, uninterrupted power service (UPS) power backup, air conditioning, elevated floors, etc.	Quanta	3-Mar-23
Identity & Access Management	Describe the authentication mechanisms natively supported by the applications and products. · Integration with, existing customer-based Single Sign On (SSO) solutions · Identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users. · Option 2-Factor authentication (digital certs, smart tokens, SMS verification code, etc.) for user access.	The Netradyne IDMS application requires unique user credentials with a strong password. All credentials are encrypted and hashed. DriverI IDMS solution has its own authentication server where the users are authenticated. It supports SSO based on OpenID Connect (OIDC). Access to the backend database is not allowed. Users will access the Netradyne SaaS application through their web browser/mobile using Https REST services	Quanta	3-Mar-23
Identity & Access Management	Does the application allow for configuring user password parameters (e.g., length, composition, expiration, history, etc.) If so, please provide default values and configurable limits:	We enforce SaaS users to use a strong password. For certain privilege roles, we enforce two factor authentication. For applications and services used by employees and contractors we have set strong password policy. Additionally, we have enabled Two-Factor authentication if supported by the service being used (e.g. AWS, Github).	Quanta	3-Mar-23
Cryptographic Controls	When user credentials are stored in the application, are passwords stored as plain text, encrypted or as hash values?	A majority of application (IDMS) data is stored within AWS. Credentials are stored in encrypted, Hashed and Salted format in DB.	Quanta	3-Mar-23
Identity & Access Management	Please explain security architecture of the application used to manage end user access permissions. For example, Is there the ability to define and manage role based security? Are there options to assign access permissions to individual IDs? Please provide Sample reports, Administration manual or other documentation that explains the permissions available and configuration steps. · Are there pre-defined roles or will roles have to be developed during implementation?	The Solution has predefined ROLES for access level controls: 1. Tenant Super User: Users with this role are likely the owner of the user account. They can perform all the actions that are allowed for a customer in Netradyne Portal. 2.Tenant Safety Manager: A Tenant Safety manager can manage drivers, coach drivers, and generally have access to all safety-related data relating to the Driver•i® system. 3. Safety Coordinator I: Users with this role can perform all functions that a Safety Manager can perform, except for specific admin functions. 4. Safety Coordinator II: Users with this role can perform all functions that a Safety Coordinator I can perform, in addition to specific admin functions. 5. Auditor: Users with this role can view, request, and share alerts/videos as well as view alert-related statistics. Only Tenant Super User and Tenant Safety Manager roles can add users to the Auditor role. 6. Operations Coordinator: Users with this role can manage following operational aspects of the Fleet include device and driver management.	Quanta	3-Mar-23
Identity & Access Management	Are there any approval processes supported by the application (i.e., Manager approvals, PO Approvals, Timesheet approvals, AP Invoice approvals, Supervisor approvals, etc.)? If yes, What approval processes are supported by the app? Are there defined role/permissions for approving items? Is there a matrix or approval workflow in the application for managing approval routes? What role/permissions does the user need for creating and/or modifying approval matrix/routes? Please provide screenshot of the web app and/or local application approval screen, approval request email and approval matrix/routes configurations. Does application positively validate users during approval workflow (protects other users from approving anyone's workflow).	1. Tenant Super User: Users with this role are likely the owner of the user account. They can perform all the actions that are allowed for a customer in Netradyne Portal. 2.Tenant Safety Manager: A Tenant Safety manager can manage drivers, coach drivers, and generally have access to all safety-related data relating to the Driver•i® system. 3. Safety Coordinator I: Users with this role can perform all functions that a Safety Manager can perform, except for specific admin functions. 4. Safety Coordinator II: Users with this role can perform all functions that a Safety Coordinator I can perform, in addition to specific admin functions. 5. Auditor: Users with this role can view, request, and share alerts/videos as well as view alert-related statistics. Only Tenant Super User and Tenant Safety Manager roles can add users to the Auditor role. 6. Operations Coordinator: Users with this role can manage following operational aspects of the Fleet include device and driver management.	Quanta	3-Mar-23

Identity & Access Management	Will end users have access to the database directly for running reports or using third-party tools? · If so, please explain the access control mechanism in place to restrict users making any changes to the data.	Users can run individual reports around their own fleet or segment but are unable to modify or change the reports. All uses have varios acces roles and permissipon but no outside user or customer can augment internal database structure. Users can pull reports directly from the IDMS platform that pertain to their own safety and personal metrics. 1.Tenant Super User: Users with this role are likely the owner of the user account. They can perform all the actions that are allowed for a customer in Netradyne Portal. 2.Tenant Safety Manager: A Tenant Safety manager can manage drivers, coach drivers, and generally have access to all safety-related data relating to the Driver•i® system. 3. Safety Coordinator I: Users with this role can perform all functions that a Safety Manager can perform, except for specific admin functions. 4. Safety Coordinator II: Users with this role can perform all functions that a Safety Coordinator I can perform, in addition to specific admin functions. 5. Auditor: Users with this role can view, request, and share alerts/videos as well as view alert-related statistics. Only Tenant Super User and Tenant Safety Manager roles can add users to the Auditor role. 6. Operations Coordinator: Users with this role can manage following operational aspects of the Fleet include device and driver management.	Quanta	3-Mar-23
Identity & Access Management	Is access to application code/executables restricted? If only compiled executables are provided, is access to those executables limited to IT Application Administrators? For Example, do end users need access rights to the share on server where application code or other system configuration files reside? If yes, please explain the nature of access needed and mitigating controls in place for this access.	All design and code changes in the system are reviewed and tested from security perspective. Multi customer data is stored in the shared database and shared server. Appropriate security checks are applied to ensure data is accessed only by authorized users.	Quanta	3-Mar-23
Identity & Access Management	Is strong authentication enforced (complex passwords, one-time passwords, biometrics) to the all networking equipment (e.g. firewalls, IPS sensors, routers, switches) and servers/clients? Please specify the password and lockout policies.	Single sign on and 2FA are implemented; The Netradyne IDMS application requires unique user credentials with a strong password. All credentials are encrypted and hashed. DriverI IDMS solution has its own authentication server where the users are authenticated. It supports SSO based on OpenID Connect (OIDC). Access to the backend database is not allowed. Users will access the Netradyne SaaS application through their web browser/mobile using Https REST services. Password Policy: •The password must contain at least 8 characters and no more than 32 characters. •The password must not contain first-name, last-name, or username. •Weak passwords are not allowed. •The new password cannot be the same as the previous three passwords.	Quanta	3-Mar-23
Identity & Access Management	For non-terminal access to the firewalls, IPS sensors, routers, and switches are the authentication credentials encrypted (i.e. utilizes ssh instead of telnet)?	We are not using outdated/un-secure protocols (e.g. TELNET)	Quanta	3-Mar-23
Identity & Access Management	Is there an appropriate review process with management approvals prior to permissions being granted? Are all permissions granted on a least privilege required basis?	We have a centralized (IT team) employee exit process which ensure all the access are revoked on exit. Access level is reviewed whenever an employee role is changed which has been quite infrequent. We have similar process for contractors to ensure access is revoked at the time of termination of contract.	Quanta	3-Mar-23
Identity & Access Management	Is all system (server, networking infrastructure, and network access) removed immediately when an employee is terminated or resigns?	We have a centralized (IT team) employee exit process which ensure all the access are revoked on exit. Access level is reviewed whenever an employee role is changed which has been quite infrequent. We have similar process for contractors to ensure access is revoked at the time of termination of contract. Our Identity and Access Management procedures are governed by principle of least privileged and the same is facilitated by timeboud provisioning, de-provisioning and periodic access reviews of each account.	Quanta	3-Mar-23
Identity & Access Management	Are any accounts (local system or domain) required to be created or leveraged within the Customer network/environment?	Netradyne provides a SaaS baseed solution.	Quanta	3-Mar-23
Identity & Access Management	Are staff required to use two factor authentication to remotely access the production cloud environment containing Scoped Data? · If so, please describe the performance of the two factor authentication.	All systems require single sign on and authentication 2FA (users only have access to their IDMS infastructure)	Quanta	3-Mar-23
TPRM	Please explain the need for and controls involved in the accessing of user files or data by the vendor/service provider.	Required personnel from Netradyne, to be able to support the customer. In addition, there is a very small random sample of alerts that are reviewed by labellers (sub-contractors) which help us improve product quality.	Quanta	3-Mar-23
DevSecOps	Is there a formal Software Development Life Cycle (SDLC) process? Are there documented change control procedures in place that are enforced on all production environments?	Yes, all codes are QA'ed and reviewed before deploying in production using GitHub. All design and code changes in the system are reviewed and tested from security perspective.	Quanta	3-Mar-23
Change & Configuration Management	Are all changes thoroughly tested prior to application to the production environment? · Please explain the testing approach.	All systems and services offered to external customers go through a rigerous QA process nothing is released in Beta and all releases need to meet a minumum of 98% accuracy to be released	Quanta	3-Mar-23
DevSecOps	Describe how security is built into the organization's software development life cycle (SDLC) processes and how application vulnerabilities are mitigated (e.g., SQL Injection or Cross-Site Scripting for web applications, buffer overflows for some compiled applications, and so on)	We adhered to standard SDLC practices and align with DevSecOps requiements which cater the need of security by design, Threat modelling and Secure architecture, code reviews, code commit and release management, Pentest, logging and monitoring of all changes. Access to Code repos are restricted to authorised personnel only.	Quanta	3-Mar-23
DevSecOps	Do you perform Dynamic Analysis Security Testing (DAST) or Static Analysis Security Testing (SAST)? If so, please provide details.	We adhered to standard SDLC practices and align with DevSecOps requiements which cater the need of security by design, Threat modelling and Secure architecture, code reviews, code commit and release management, Pentest, logging and monitoring of all changes.Access to Code repos are restricted to authorised personnel only.	Quanta	3-Mar-23
TPRM	Is any development or support being subcontracted out or planned for the future or provided by offshore resources? Please provide details	Netradyne has in house and contracted resources for development and support. All contracted parties have agreements in place.	Quanta	3-Mar-23
TPRM	How is offshore resource access managed? IS SOD in place to ensure code development is appropriate?	SOP and SOD are in place for all contractors.	Quanta	3-Mar-23

Identity & Access Management	Do offshore Developers or Support resources have access to production data?	The resources have limited and access to production data on need basis.	Quanta	3-Mar-23
Infrastructure Security	Is the service/application provided on shared servers (application or database/data storage)?	Our SaaS solution hosted on AWS Infra is natively multi-tenant, we have common database, each tenant data is segregated using the tenant id. Tenant specific sensitive data is encrypted using unique tenant encryption key.	Quanta	3-Mar-23
Infrastructure Security	Describe the security controls present that prevent one client from compromising another client in a resource pooled environment	Data on device and AWS S3 cloud storage is stored encrypted. Sensitive and PII information in database is stored encrypted. On device we use AES-128 algorithm for data encryption. On cloud we use AES-GCM with 256-bit encryption key. We are using envelope encryption and master key is stored in AWS KMS system.	Quanta	3-Mar-23
Infrastructure Security	Describe the data segmentation and separation capability between clients that is provided	Our SaaS solution hosted on AWS Infra is natively multi-tenant, we have common database, each tenant data is segregated using the tenant id. Tenant specific sensitive data is encrypted using unique tenant encryption key.	Quanta	3-Mar-23
Cryptographic Controls	Will scoped data be encrypted in transit or rest? If so, please describe in detail how each of the following items has been implemented:	We have AES 256 bit encryption for data at rest and backups. We use SSL/TLS for data in transit.	Quanta	3-Mar-23
Cryptographic Controls	Data In-transit encryption for Scoped Data	SSL/TLS	Quanta	3-Mar-23
Cryptographic Controls	Data at-rest encryption for Scoped Data	AES 256	Quanta	3-Mar-23
Cryptographic Controls	Encryption algorithm and strength of the encryption keys (AES 256 bit, AES 128, 3DES 128 bit, etc.)	AES 256	Quanta	3-Mar-23
Cryptographic Controls	Key rotation schedule / frequency and if it can be done at customer request	Master key is rotated on annual basis. Currently we don't have provision to perform the rotation on customer request.	Quanta	3-Mar-23
BCP & DR	What is the frequency and location of the backup or replication of Scoped Systems and Data?	DriverI offering is SaaS solution hosted on Auto scalable, robust and redundant AWS Infrastruture. Netradyne backup DB data. We have all our data backed up regularly on AWS S3 which provides a 99.5% availability and the 99.999999999% durability.	Quanta	3-Mar-23
BCP & DR	How long are backup copies retained by default? Please specify Daily, Weekly, Monthly and Yearly retention that will allow point in time restoration of data with default settings. For Example, Data is retained for 5 years and point in time recovery at any point-in time is available.	Data can be kept or deleted post account closure based on agreed data retention policy with client. Our data retention policy is 90 days for video and 12 months for data points. Netradyne take database backups every 4 hours, and retain them for 4 days (we can do point-in-time-recovery to any point in the last 4 days.) Data retention for raw payloads is governed by the video and non-video DRP (data-retention-policy) that is a part of customer agreements.	Quanta	3-Mar-23
BCP & DR	How frequently are backups or replication tested? When was the last test performed? Was it successful?	Alerts are set for backup failure, if any. Failed back ups are monitored and mitigated. DB backups are successfully tested every day using automation.	Quanta	3-Mar-23
BCP & DR	Are backups performed password protected and/or encrypted in-transit/transport (In case of tapes) and storage?	DB backups are performed using EBS snapshots, so there is no data replication used for this. EBS snapshots are encrypted.	Quanta	3-Mar-23
BCP & DR	If data replication is used, is the data encrypted during transport and at-rest?	DB backups are performed using EBS snapshots, so there is no data replication used for this. EBS snapshots are encrypted.	Quanta	3-Mar-23
BCP & DR	Is there a Disaster Recovery Plan (DRP) in place? If so, please respond and give details for Protections are in place for disasters or localized outages, Frequency and success/failure of the DRP testing in the last few cycles etc.	DRP is defined, tested and established for Netradyne	Quanta	3-Mar-23
Data Security/Privacy	If the contract relationship is severed, are there means to have the client data extracted and sent to the client? ·If so, please provide details on the following bulleted items on data retrieval after contract separation: ·The approach of the data retrieval and delivery ·The period of time allowed time window and approach to destroying the data that is retained at the end of the contract relationship ·The time window of the data retrieval after the expiry of contract	We have AES 256 bit encryption for data at rest and backups. We use SSL/TLS for data in transit. Data can be kept or deleted post account closure based on agreed data retention policy with client.	Quanta	3-Mar-23
Data Security/Privacy	If the data is accidentally lost or breached, what recourse would the client have?	Data on device and AWS S3 cloud storage is stored encrypted and object locks in place.	Quanta	3-Mar-23
Data Security/Privacy	Are the policies in place around the retention and/or purging of customer data? ·Are there provisions for how much or how long data can be retained? ·Please cite the document reference if the answer is yes. ·What is the notification process for pending purges? ·Is there a fee for these services?	our data retention policy is 90 days for video and 12 months for data points.	Quanta	3-Mar-23
TPRM	Are there any dependencies on critical third party service providers? If so, please explain the third-party dependencies and give details in each of the following bulleted items has been implemented and give details:	DriverI offering is SaaS solution hosted on Secure, Auto scalable, robust and redundant AWS Infrastruture. We have established Third-Party Risk Management (TPRM) process to onboard any vendor/contractor.	Quanta	3-Mar-23
Data Security/Privacy	The Scoped Data disclosure policy (with limitations, if any) to third parties	Netradyne contractual agreement with third party will take care of data disclosure aspects	Quanta	3-Mar-23
Data Security/Privacy	The Scoped Data disclosure policy to third parties outside of the U.S.A.	Netradyne contractual agreement with third party will take care of data disclosure aspects	Quanta	3-Mar-23
TPRM	Contractual controls to ensure that Scoped Data shared with third parties is limited to defined parameters for access, use and disclosure; If no such controls exist, please explain the reason	Netradyne has DPA meeting GDPR requirements signed with critical Third Party Partner(s).	Quanta	3-Mar-23
DevSecOps	Is the mobile application being developed in-house or by a third party? If in-house, please specify the SDLC framework being used: . If third-party, please attach or provide the link to the SOC 2 Type II report.	Mobile applications are developed inhouse and follows the standard SDLC practices of design review and code review before pushing to Github.	Quanta	3-Mar-23

Cryptographic Controls	Is scoped data stored on mobile devices, and if so, is the data encrypted? Please explain and give details.	App stores minimal user data. All the Personal Identifiable Information (PII) is encrypted when data is stored. App collects Driveri App usage using a library called Mixpanel. This includes information on- Feature Analytics - How a user is using certain app features App Analytics - How many users are using iOS vs Android, or what is the OS version used etc. Diagnostics - Identifying users impacted by App crashes etc	Quanta	3-Mar-23
Governance Risk & Compliance	Is there a risk management, or compliance department, or other management oversight unit with responsibility for identifying and tracking resolution of outstanding regulatory issues?	Netradyne has established a robust Enterprise Risk Framework that adheres and aligns to leading practices to maintain security, privacy and compliance. •Netradyne has been built on the foundation of ISMS controls to facilitate a secure and trusted operational environment •Netradyne's Information Security Management System (ISMS) is reviewed periodically by an independent firm for ISO 27001 certification •Netradyne's priorities, constraints, risk tolerances, and assumptions are established and recorded in Risk Register and used to support infrastructure, operational and vendor risk decisions. •Netradyne understands the cybersecurity risk to its on-prime as well as cloud hosted operations (including mission, functions, reputation), organizational assets, and individuals. •Netradyne InfoSec team performs periodic risk assessment to identify risks and associated mitigation strategies, including controls. It has a defined and established enterprise Risk Register to list out all the identified vulnerabilities with it's threat landscapes, Prioritize the Risk remediation strategies, communicate to leadership and monitor the same till risk closure.	Quanta	3-Mar-23
Data Security/Privacy	Is there a formal process for reporting and responding to privacy complaints or privacy incidents for Scoped Data? If so, describe the process and give details: . If there is no process please explain why and give details:	Detailed privacy breach response plan includes initial recognition of the privacy incident and a detemination of its severity, including reporting requirements. All privacy complaints and incidents are reviewed by the privacy team and escalated appropriately in coordination with InfoSec	Quanta	3-Mar-23
Data Security/Privacy	Is there a business associate contract in place to address obligations for the privacy and security requirements of the services provided? If so, please explain and give details:	We have subprocessor agreements in place with our main service providers as part of GDPR compliance.	Quanta	3-Mar-23
Data Security/Privacy	How is personnel information protected from release or use for direct marketing or advertising purposes? Please explain and give details: .	Personnel (Driver and other service users?) information is segregated from website visitor and other direct marketing databases. Personnel information is only used to provide the services.	Quanta	3-Mar-23
Security Incident Management	Can Customer staff or certified computer forensic experts as well third party experts to assist in investigations and electronic discovery?	This should be subjected to business requirements and customer agreements	Quanta	3-Mar-23
Data Security/Privacy	How will data be loaded to the application?	Device data, collected by the Driveri and built-in sensors is collected from the Driveri device and transmitted to the Netradyne cloud servers and used to populate the portals. Administrative data such as Drivers/Vehicles/Users is collected from the customer within the web portal, or ported in via APIs utilized by the customer or it's officers. Changes to existing data are able to be sent via the web portal and the mobile application available to drivers and users.	Quanta	3-Mar-23
Cryptographic Controls	Will data be encrypted in transit?	All data in transit is encrypted with SSL/TLS v1.2 industry standard protocols	Quanta	3-Mar-23
DevSecOps	Are APIs available to link to our on-site systems?	API documentation: https://resources.netradyne.com/?user=partner	Quanta	3-Mar-23
Data Security/Privacy	Does the app provide a data import/portability capability or tool? If yes, please identify role/permissions that provides such access; Is this access per module, per table, per function or open for any table. Does the capability or tool allow overwriting existing data? If yes, does the tool provide options to see impact in proof mode, provides log of changes, other protections for maintaining data integrity.	This is allowed depending on function and permission. Each function has a different capability of overwriting versus adding, based on the constraints of that feature. Internal validation is always performed prior to updates. Internal logs are retained, but are not customer facing.	Quanta	3-Mar-23
DevSecOps	What other options are available to integrate with on-site systems.	Continually looking to integrate with additional providers. https://www.netradyne.com/integrations	Quanta	3-Mar-23
Product Customer Services	Does the respondent offer Service Level Agreements (SLA)? If so, please explain the details of the SLA Agreement in each of the following bulleted items and give details: ; If no SLA exists any of the individual bulleted items, please state what alternate agreements or arrangements have been made to satisfy this request: . Please: · Identify the SLAs for the third-party providers · State the services that SLAs address · Identify the penalties or remediation clauses for breaches of availability/continuity within the SLAs	For the IDMS console we have enabled Two-Factor authentication for high privilege roles. Enforcing 2 Factor authentication for customer roles have not been rolled out yet, but this can be added on the roadmap. The product has been designed such that it ca	Quanta	3-Mar-23
Security Architecture	Describe the overall architecture of the system or application. Include diagrams of the network, server and telephony architecture if applicable.		ABC Supply	15-Mar-23

Security Architecture	Describe and diagram all existing and future network connectivity in which Customer Supply data will be transferred or received. (This may include transfers between your company and Customer Supply or your company and other partners.)	Above Architecture diagram is valid here also. Driveri is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS). Added some of the details below: . Programing languages and framework used (Open Source & Proprietary) --> Java, Python, C++ . Operating System (OS) and Database (DB) --> Linux, Postgres . Cloud Service components used --> Object storage, Elastic Compute, Key Management Service, Application Load Balancers, Managed DB services, Queue services, Notification services	ABC Supply	15-Mar-23
Security Architecture	Specific to the service(s) provided, what ports, service and protocol requirements do you have for connections to/from your environment?	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs	ABC Supply	15-Mar-23
Security Architecture	In relation to the network perimeter, do you utilize a multi-tiered DMZ configuration or DMZ architecture? (e.g. web/app and database or web/app/database)	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs, which is the front end of Mutli-Tier architecture, DBs are at back end and only accessible though Netradyne internal web API services to fetch the data for the requests.	ABC Supply	15-Mar-23
Physical & Environmental Security	Do you host all of the system hardware and software? If not, identify by name and address your data center provider.	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs	ABC Supply	15-Mar-23
Physical & Environmental Security	Describe the physical security of your data center or hosting provider's data center.	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure.Physical security of hosting infrastructure is AWS responsibility. AWS supports security standards and compliance certifications which includes PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements. For more information please refer https://aws.amazon.com/compliance/data-center/controls/	ABC Supply	15-Mar-23
Governance Risk & Compliance	Does your organization have a formal Information Security, Compliance, and Risk Management Program(s)? If so, describe the program(s), how often policies/procedures/controls are reviewed, and the accountability structure.	Netradyne has established a robust Enterprise Risk Framework that adheres and aligns to leading practices to maintain security, privacy and compliance. •Netradyne has been built on the foundation of ISMS controls to facilitate a secure and trusted operational environment •Netradyne's Information Security Management System (ISMS) is reviewed periodically (Annual) by an independent firm for ISO 27001 certification •Netradyne's priorities, constraints, risk tolerances, and assumptions are established and recorded in Risk Register and used to support infrastructure, operational and vendor risk decisions. •Netradyne understands the cybersecurity risk to its on-prime as well as cloud hosted operations (including mission, functions, reputation), organizational assets, and individuals. Accountability lies with the senior management and they acknowldged their roles and responsibilities with respect to Information Security. •Netradyne InfoSec team performs periodic risk assessment to identify risks and associated mitigation strategies, including controls. It has a defined and established enterprise Risk Register to list out all the identified vulnerabilities with it's threat landscapes, Prioritize the Risk remediation strategies, communicate to leadership and monitor the same till risk closure. All outputs from risk register is leverage to review and refine the existing policies and procedures on annual basis.	ABC Supply	15-Mar-23
Training & Awareness	Describe security awareness and training programs.	Netradyne employees undergo extensive training programs covering technical/core, business, and soft skills, enabling client readiness from day one. Netradyne's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements	ABC Supply	15-Mar-23
Identity & Access Management	Describe how separation of duties is achieved in order to isolate security roles and responsibilities.	Segregation of duties is clearly defined, assigned, and documented in access control list of Netradyne. All privileged activities are accompanied with MFA and properly monitored. Non-repudiation is in place for audit and accountability purpose.	ABC Supply	15-Mar-23
Governance Risk & Compliance	Has your company successfully completed a “SAS 70 Type II” or “ISO 27001” or “SSAE 16 Type II” audit? If so, by whom? Please share the results.	We have adopted and implemented ISMS controls and our security infrastructure is certified with ISO 27001 : 2013. Report can be shared under NDA. We have external audits conducted on a annual basis to review our internal controls and maturity in the organization. Attached certification details for reference ISO 27001 - https://gmsintercert.com/verify/single-cert-verify.php?cRegName=ISMS2020025	ABC Supply	15-Mar-23
BCP & DR	Describe your fault tolereance and system redundancies in the event of failure.	DriverI offering is SaaS solution hosted on Auto scalable, robust and redundant AWS Infrastruture. Netradyne backup DB data. We have all our data backed up regularly on AWS S3 which provides a 99.99% availability and the 99.999999999% durability.	ABC Supply	15-Mar-23
BCP & DR	Do you maintain and regularly practice disaster recovery and business continuity plans and procedures? Describe the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).	We have all our data backed up regularly on AWS S3 which provides a 99.99% availability and the 99.999999999% durability. Data can be kept or deleted post account closure based on agreed data retention policy with client. Our data retention policy is 90 days for video and 12 months for data points. Netradyne take database backups every 4 hours, and retain them for 4 days (we can do point-in-time-recovery to any point in the last 4 days.) Data retention for raw payloads is governed by the video and non-video DRP (data-retention-policy) that is a part of customer agreements.	ABC Supply	15-Mar-23
BCP & DR	How often are the backup and restore procedures tested, reviewed, and modified?	Alerts are set for backup failure, if any. Failed back ups are monitored and mitigated. Disaster Recovery Planning is defined, tested and established for Netradyne and happened on annual basis.	ABC Supply	15-Mar-23
BCP & DR	Is client data separated on the backup media? If so, describe procedures for segregating backups by customer on separate media.	Our SaaS solution hosted on AWS Infra is natively multi-tenant, we have common database, each tenant data is segregated using the tenant id. Tenant specific sensitive data is encrypted using unique tenant encryption key. DB backups are performed using EBS snapshots and its separated for each client. EBS snapshots are encrypted.	ABC Supply	15-Mar-23
BCP & DR	Describe the encryption method used for backup media. If backup media is not currently encrypted, explain.	DB backups are performed using EBS snapshots and its encrypted using AES 256.	ABC Supply	15-Mar-23

BCP & DR	Does your organization have an alternate site location for data center recovery purposes? If so, where is your alternate site located? What is the approximate distance between your production (primary) site and alternate (secondary) site?	DriverI offering is SaaS solution hosted on Auto scalable, robust and redundant AWS Infrastruture. Netradyne backup DB data. We have all our data backed up regularly on AWS S3 which provides a 99.99% availability and the 99.999999999% durability.	ABC Supply	15-Mar-23
DevSecOps	How is information security incorporated into the software design process?	We adhered to standard SDLC practices and align with DevSecOps requiements which cater the need of security by design, Threat modelling and Secure architecture, code reviews, code commit and release management, Pentest, logging and monitoring of all changes.Access to Code repos are restricted to authorised personnel only.	ABC Supply	15-Mar-23
Infrastructure Security	Describe the methodology and controls used to separate client data?⍰	Our SaaS solution hosted on AWS Infra is natively multi-tenant, we have common database, each tenant data is segregated using the tenant id. Tenant specific sensitive data is encrypted using unique tenant encryption key. We segregate one customer data from other customers using customer unique identifier. We utilize Authentication and Authorization to prevent a customer from accessing another customer's data.	ABC Supply	15-Mar-23
Infrastructure Security	Describe how test, development, and production environments are separated. Is any production data used in a non-production environment?	Netradyne has separate accounts for Development, Test, QA, Preproduction, Production. Access to implement changes to the production environment(s) and other infrastructure components is appropriately restricted through role-based access controls.	ABC Supply	15-Mar-23
Identity & Access Management	Describe how user access is controlled at your organization. What credentials are required to access a company's system?	DriverI IDMS solution has its own authentication server where the users are authenticated. It supports SSO based on OpenID Connect (OIDC). For the IDMS console we have enabled Two-Factor authentication for high privilege roles. We have Role Based Access control (RBAC) defined which follows the least privilege and Need to know priniciples. In that way we are limiting the client data access to very limited set of people only for troubleshoot or debugging purpose. We have set data retention policy of different kind of data.	ABC Supply	15-Mar-23
Identity & Access Management	What controls are in place for privileged access and accounts (e.g. root, administrator)?	For the IDMS console we have enabled Two-Factor authentication for high privilege roles. Enforcing 2 Factor authentication for customer roles have not been rolled out yet, but this can be added on the roadmap. The product has been designed such that it can be extended to support 2 factor authentication for any role in future. However, so far, it has been lower priority to strike the right balance between convenience and security.	ABC Supply	15-Mar-23
Infrastructure Security	Do you utilize an intrusion detection or intrusion prevention system at the application, host, or network level to protect your environment? Describe tools/methodologies in place.	Yes, we use enterprise scale Security Solutions and tools providing Network Security, Firewall, UTM, APT, IDS/IPS protective our systems. The controls are managed and governed by our ISMS policies and guidelines. Meraki AMP (Advance Malware Protection) deployed as an IDS/IPS where Sensors signatures updated Hourly & IDS/IPS configurations reviewed Quarterly	ABC Supply	15-Mar-23
Vulnerability & Patch Management	Do you regularly perform vulnerability scans of networks and applications? Describe the frequency and scope of scanning as well as the tools used to perform scanning.	Netradyne has defined and established Patch & Vulnerability Management Process and control implementations. We test applications against OWASP Top Ten vulnerabilities. We also perform penetration testing on web applications once in a quarter. We have appropriate entry and exit processes to ensure only authorized users have access to our systems at any given time. We review other processes on an ongoing basis from security perspective. External PEN Testing is done yearly by recognized organization following industry standards. We also conduct PEN testing internally on regular basis.	ABC Supply	15-Mar-23
Infrastructure Security	Describe virus and malware prevention, detection, and mediation on all devices, including but not limited to: • Application servers • Infrastructure servers • Mail servers • Workstations • Laptops	Yes, we use enterprise scale security solutions and endpoint protection tools (EDR-Crowdstrike) providing anti malware protection along with deployed Firewall, UTM, APT, IDS/IPS. The controls are managed and governed by our ISMS policies and guidelines. Meraki AMP (Advance Malware Protection) is deployed and operational.	ABC Supply	15-Mar-23
Cryptographic Controls	Do you utilize a full disk encryption system for workstations, laptops, and servers?	Yes	ABC Supply	15-Mar-23
Data Security/Privacy	How long does your organization retain data, including logs? How is the data disposed? What steps are taken to ensure that data from obsolete media is unrecoverable?	We have AES 256 bit encryption for data at rest and backups. We use SSL/TLS for data in transit. Data can be kept or deleted post account closure based on agreed data retention policy with client. Our default data retention policy is 90 days for video and 12 months for data points.	ABC Supply	15-Mar-23
Security Incident Management	Does your organization collect, retain, monitor, and alert on logs from security solutions/systems? If so, are these logs managed in a centralized manner using a SIEM?	Yes, we have established a dedicated security operation center and centralised SIEM solution is in place.	ABC Supply	15-Mar-23
Governance Risk & Compliance	How often do you perform third party penetration testing and what tools/vendors are used? Describe the results of such testing and the remediation procedures.	We test applications against OWASP Top Ten vulnerabilities. We also perform penetration testing on web applications once in a quarter. We have appropriate entry and exit processes to ensure only authorized users have access to our systems at any given time. We review other processes on an ongoing basis from security perspective. External PEN Testing is done yearly by recognized organization following industry standards. We also conduct PEN testing internally on regular basis.	ABC Supply	15-Mar-23
Security Incident Management	Does your business have an Incident Response Plan to take responsive actions after a security incident or breach occurs? If yes, please describe the plan.	Yes, Netradyne InfoSec-Security Operation team performs monitoring, including documentation, classification, escalation, coordination and tracking of incidents per documented procedures. -Additional Threat Intel: Netradyne-developed use cases for auto-remediation of most common system misconfigurations -Custom use cases: Additional custom use cases can be implemented for each application/system on boarded -Incident Response Processes: Processes and procedures defined and operationalized for alert categorization and priority, notification trees, escalation paths, and response workflows -Log Centralization: Log centralization capability deployable via automation to aggregate log sources and enable ingestion into SIEM solution -Deployment Templates: Templates and configurations established to expedite deployment of SIEM capabilities	ABC Supply	15-Mar-23
Security Incident Management	Describe any past security breaches of your system and the resulting improvements you have made to prevent future incidents from occuring.	NA, but from process perspective-For enterprise-wide critical severity security incidents, a root cause analysis is conducted and discussed with risk management. Based on the root cause analysis, change requests are prepared and the risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.	ABC Supply	15-Mar-23

Security Incident Management	Describe the process for notifying customers of potential compromise to information and systems.	We offer multiple communication channels to notify customer for any probable downtime, if applicable.	ABC Supply	15-Mar-23
Security Incident Management	Do you take full responsibility if you make a mistake and expose confidential data? For example, if one of your employees sold our information, would you be fully responsible or would that be our liability?	We maintain the required level of security hygiene across our employees & associated third party. Security is a shared responsibilities and accoutability should be discussed and fixed as a contractual requirement.	ABC Supply	15-Mar-23
Data Security/Privacy	Describe privacy and confidentiality statements and practices.	Netradyne's privacy policy is available at https://www.netradyne.com/privacy-policy. For the vast majority of Personal Information processing conducted by Netradyne through the Driver•i device (or related services or accessories), Netradyne is acting as a data processor or service provider on behalf of its business customers, and such processing is carried out in compliance with our legal and contractual obligations with business customers. Our business customer is responsible for complying with laws that may require notice, disclosure or consent related to the transfer of Personal Information to Netradyne. Netradyne enters into agreements with our business customers that legally require Netradyne to protect the Personal Information we receive or are directed to collect and use it only to provide our products and services to the business customer. A very small fraction of data collected through the Driver•i device (or related services and accessories) will enter Netradyne's Training Data for machine learning purposes. For such machine learning activities, and to the extent Netradyne is processing Personal Information, Netradyne is acting as the controller or business of the Personal Information. The Safer Roads and Safer Driving sections of the Privacy Policy (https://www.netradyne.com/privacy-policy) provide information specifically about how Netradyne collects and uses data for training its machine learning models. Netradyne has received Privacy-by-Design certification and is also ISO 27001 certified. Netradyne maintains policies and procedures to safeguard personal data. All privacy complaints and incidents are reviewed by the privacy team and escalated appropriately in coordination with InfoSec.	ABC Supply	15-Mar-23
Cryptographic Controls	Describe cryptographic methods for passwords and data at rest and data in transit. Identify the algorithms utilized including TLS requirements, etc.	We have AES 256 bit encryption for data at rest, backups. We use SSL/TLS for data in transit.	ABC Supply	15-Mar-23
Cryptographic Controls	Do you maintain encryption key management procedures?	Master key is managed and rotated on annual basis.	ABC Supply	15-Mar-23
Vulnerability & Patch Management	Describe your ongoing system maintenance process and responsibilities. Include information regarding bug fixes, security patches, frequency and expected downtime.	Netradyne has deifned and established Patch & Vulnerability Management Process and control implementations. We test applications against OWASP Top Ten vulnerabilities. We also perform penetration testing on web applications once in a quarter. We have appropriate entry and exit processes to ensure only authorized users have access to our systems at any given time. We review other processes on an ongoing basis from security perspective. Security patches are notified as and when released, assessed, prioritized, downloaded, tested and then deployed in control environment as per defined Patch & vulnerability management process. External PEN Testing is done yearly by recognized organization following industry standards. We also conduct PEN testing internally on regular basis.	ABC Supply	15-Mar-23
Infrastructure Security	What components of your infrastructure are dedicated to Customer Supply? What components are shared with other clients?	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs. No any SaaS component is shared with Clients.	ABC Supply	15-Mar-23
Identity & Access Management	Do you support single-sing on (SSO)? Specifically, do you support SAML 2.0 and Okta?	Yes, OIDC based SSO is supported.	ABC Supply	15-Mar-23
Identity & Access Management	What is the account and password maintenance and administration features are available in the application?	Single sign on and 2FA are implemented; The Netradyne IDMS application requires unique user credentials with a strong password. All credentials are encrypted and hashed. DriverI IDMS solution has its own authentication server where the users are authenticated. It supports SSO based on OpenID Connect (OIDC). Access to the backend database is not allowed. Users will access the Netradyne SaaS application through their web browser/mobile using Https REST services. Password Policy: •The password must contain at least 8 characters and no more than 32 characters. •The password must not contain first-name, last-name, or username. •Weak passwords are not allowed. •The new password cannot be the same as the previous three passwords.	ABC Supply	15-Mar-23
Identity & Access Management	Do you support multi-factor authentication?	We enforce SaaS users to use a strong password. For certain privilege roles, we enforce two factor authentication. For applications and services used by employees and contractors we have set strong password policy. Additionally, we have enabled Two-Factor authentication if supported by the service being used (e.g. AWS, Github).	ABC Supply	15-Mar-23

Identity & Access Management	Describe application authorization and access controls that protect the security of data in the system, including system user roles. How is role based security managed in your solution? Describe capabilities to support reporting and viewing of application users and rights. Can your company system administrators access and view Customer data?	A majority of application (IDMS) data is stored within AWS. Credentials are stored in encrypted, Hashed and Salted format in DB. The Solution has predefined ROLES for access level controls: 1. Tenant Super User: Users with this role are likely the owner of the user account. They can perform all the actions that are allowed for a customer in Netradyne Portal. 2.Tenant Safety Manager: A Tenant Safety manager can manage drivers, coach drivers, and generally have access to all safety-related data relating to the Driver•i® system. 3. Safety Coordinator I: Users with this role can perform all functions that a Safety Manager can perform, except for specific admin functions. 4. Safety Coordinator II: Users with this role can perform all functions that a Safety Coordinator I can perform, in addition to specific admin functions. 5. Auditor: Users with this role can view, request, and share alerts/videos as well as view alert-related statistics. Only Tenant Super User and Tenant Safety Manager roles can add users to the Auditor role. 6. Operations Coordinator: Users with this role can manage following operational aspects of the Fleet include device and driver management.	ABC Supply	15-Mar-23
DevSecOps	Do you provide a public API? If so, what API security measures are in place? How does the client administer/request/manage corresponding keys/secrets/credentials?	We have API platform. We authenticate APIs using API tokens which can be generated using client credentials shared with customers.	ABC Supply	15-Mar-23
DevSecOps	What are the planned security features to be released in the application?	We constantly review to improve and mature our security features in the application. This can be discussed part of the contract engagement.	ABC Supply	15-Mar-23
Audit, Logging & Monitoring	Describe your methodology and tools used for monitoring the application and all underlying components including servers and network. What components are not monitored?	Yes, Netradyne InfoSec-Security Operation team performs monitoring, including documentation, classification, escalation, coordination and tracking of incidents per documented procedures. -Additional Threat Intel: Netradyne-developed use cases for auto-remediation of most common system misconfigurations -Custom use cases: Additional custom use cases can be implemented for each application/system on boarded -Incident Response Processes: Processes and procedures defined and operationalized for alert categorization and priority, notification trees, escalation paths, and response workflows -Log Centralization: Log centralization capability deployable via automation to aggregate log sources and enable ingestion into SIEM solution -Deployment Templates: Templates and configurations established to expedite deployment of SIEM capabilities		15-Mar-23
BCP & DR	Describe your methodology for capacity planning and how you leverage operations monitoring results into the process - include your performance/stress testing tools and methodology in your response.	Netradyne system disaster recovery plan and capacity planning is implemented and maintained. We have estimated the log storage space required and our capacity planning is aligned with volume of log data, we are receieving to SIEM for analysis. A Business Impact Assessment (BIA) is performed each fiscal year to identify threats to software, hardware, people, and physical assets	ABC Supply	15-Mar-23
Security Incident Management	Does your application log actions and events? If so, can these logs be exported to a SIEM?	Yes, we have established a dedicated security operation center and centralised SIEM solution is in place.	ABC Supply	15-Mar-23
TPRM	Describe methodology for sending data to 3rd parties external to your company; include discussion on media, transmission process and the encryption, shipping and handling for both electronic and non-electronic media.	External parties/vendors are subjected to a risk evaluation and are monitored on a go-forward basis according to the risk rating. Vendor/Third party compliance requirements, service levels, privacy, and confidentiality requirements are written into the contract with that vendor as necessary based on the service provided.	ABC Supply	15-Mar-23
TPRM	Is data stored, sent to, or accessed from any Third Party or Subcontracted Vendor location? Do you send data or allow any work functions to any non-U.S. Locations? If so please list location.	Engineering support activities are provided by Netradyne India. In addition, Netradyne engages other third parties for some services - AWS for datahosting, Concentrix (India) for customer support and eLancer (India) for data labelling. Wherever required, Netradyne conductsTransfer Impact Assessment (TIA) and enters into Data Processing Agreements (DPAs) with third parties.	ABC Supply	15-Mar-23
Change & Configuration Management	What are your scheduled maintenance / change windows?	We are constantly improving our systems and making changes on need basis. Usually the planned changes are deployed every 2 weeks. Changes may get deployed on need basis outside the schedule.	ABC Supply	15-Mar-23
Change & Configuration Management	Describe the process for scheduled changes and unscheduled changes. Describe the notification process, both internally and to clients, for scheduled and unscheduled changes. Include normal timeframes for notification to clients.	Any customer impacting changes are notified via Whats New section in the dashboard.	ABC Supply	15-Mar-23
Identity & Access Management	Are adequate access controls implemented to access information systems in your environment?	ND uses Azure AD for centralize Access Management. Access to ND resources are restricted to appropriate personnel via Active Directory groups based on job responsibilities	JIO IRM	5-Aug-24
Identity & Access Management	Are access logs enabled and monitored regularly?	All Access/System Logs are enabled , ingested to ND Security Operation Centre (SOC), analyzed & monitored for any anomaly. Netradyne' s practices for continuous logging and monitoring are aligned with leading practices Activity performed on cloud environment resources is logged, monitored and alerted on based on a defined ruleset	JIO IRM	5-Aug-24
Identity & Access Management	Do your perform periodic access review ensuring- 1) Timely removal of ids which are no longer required 2) Disabling of default IDs. 3) Disabling dormant/inactive accounts	ND Perform periodic User Access Reviews of Users and Associated Group(s) for both aspects, access, and permissions. ND Maintain and update security group user memberships ND Add, remove, disable user accounts based on procedures and processes defined within Netradyne Information Security Policy and Procedure	JIO IRM	5-Aug-24
Identity & Access Management	Do you have an Identity and Access Management (IDAM) system in place to enable both role-based access and context-based entitlement to data?	ND uses Azure AD for centralize Access Management. Access to ND resources are restricted to appropriate personnel via Active Directory groups based on job responsibilities & entitlements	JIO IRM	5-Aug-24
Identity & Access Management	Do you use a Secure channel (VPN, Https, etc) to provide access to your cloud service infrastructure & applications?	In order to connect to Netradyne systems users either authenticate through a VPN (Virtual Private Network) which requires MFA (multi-factor authentication) or be connected to the Netradyne corporate network	JIO IRM	5-Aug-24
Identity & Access Management	Are strong and complex passwords enabled for accessing the System and application accounts? (Includes Min length, complexity, Password History, Password age,)	ND follows the Password complexities and password parameters are in conformity with Information Security policies and standards	JIO IRM	5-Aug-24

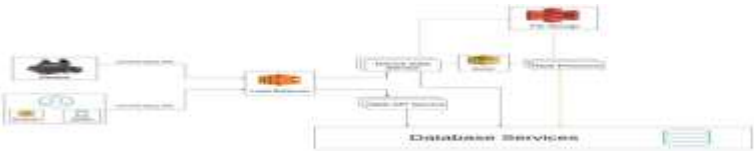
Identity & Access Management	Is 2 factor authentication enabled for administrative accounts? Do you use a separate system such as Privileged Identity/Access Management system to connect to systems to carry out administrative activities?	Yes, MFA is enabled for administrative accounts and getting managed through Azure AD and conditional policies. Administrative activity performed on Cloud resources is logged, monitored and alerted based on defined ruleset.	JIO IRM	5-Aug-24
DevSecOps	Do you design, develop, deploy and test application and APIs in accordance to leading industry standards?	Yes, Secure Software Development Life Cycle has been defined and Implemented at Netradyne based on DevSecOps Methodology.	JIO IRM	5-Aug-24
DevSecOps	Does the CSP ensure that applications undergo Application Security testing that include source code and dynamic analysis against applications hosted in the cloud.	Yes, Code reviews, VAPTs and Testing are established norms at Netradyne. Netradyne uses SonarQube, Burp Suite and Nessus as enablers.	JIO IRM	5-Aug-24
DevSecOps	Do you expose your API's which can we consumed by the tenant to implement tenant specific security policies (to support integration with Cloud Access Security Broker)	NA	JIO IRM	5-Aug-24
Governance Risk & Compliance	Do you allow tenants/ customers to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Under NDA. Netradyne ISO 27001:2022 Certificates can be shared	JIO IRM	5-Aug-24
Governance Risk & Compliance	Do you train your employees regularly on Information Security Awareness and their responsibilities on customer data protection?	Netradyne's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements	JIO IRM	5-Aug-24
Governance Risk & Compliance	Are all personnel in your company required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	Yes, It is required to sign the NDA/Confidentiality agreement	JIO IRM	5-Aug-24
Governance Risk & Compliance	Do you provide tenant with a role definition document clarifying your administrative responsibilities versus those of the tenant?	Yes, we do have that capability and clarification. The Solution has predefined ROLES for access level controls: 1. Tenant Super User: Users with this role are likely the owner of the user account. They can perform all the actions that are allowed for a customer in Netradyne Portal. 2.Tenant Safety Manager: A Tenant Safety manager can manage drivers, coach drivers, and generally have access to all safety-related data relating to the Driver•i® system. 3. Safety Coordinator I: Users with this role can perform all functions that a Safety Manager can perform, except for specific admin functions. 4. Safety Coordinator II: Users with this role can perform all functions that a Safety Coordinator I can perform, in addition to specific admin functions. 5. Auditor: Users with this role can view, request, and share alerts/videos as well as view alert-related statistics. Only Tenant Super User and Tenant Safety Manager roles can add users to the Auditor role. 6. Operations Coordinator: Users with this role can manage following operational aspects of the Fleet include device and driver management.	JIO IRM	5-Aug-24
Governance Risk & Compliance	Does your SLA terms/ contracts include 'Right to Audit' clause?	Instead, customer can review our security certifications and report under signed NDA. Netradyne solution is a SaaS offering which is hosted on secure, highly available & scalable AWS (Amazon Web Services) Infrastructure. Netradyne adopt industry best security practices and is certified with ISO 27001:2022 and 27701:2019 recognitions on annual basis. Apart from external certification audit, the Netradyne InfoSec team involved in periodic assessments, audits, VAPTs and vulnerability scans to improve and mature the overall security posture including Data, Endpoint, Cloud Infrastructure and Network.	JIO IRM	5-Aug-24
BCP & DR	Do you provide disaster recovery capability?	Netradyne solution is a SaaS offering which is hosted on secure, highly available & scalable AWS (Amazon Web Services) Infrastructure. Netradyne system disaster recovery plan is implemented and maintained for its systems and infrastructure. BCP plans are in place to support continued operations of Netradyne Managed Services.	JIO IRM	5-Aug-24
BCP & DR	Does your Business Continuity plan include RTO & RPO? Are business continuity plans are tested at planned intervals to ensure business continuity plans are effective?	Recovery Time Objectives (RTOSs) and Recovery Point Objectives (RPOS) are established and monitored based on Customer's requirements as defined in SLAs	JIO IRM	5-Aug-24
BCP & DR	Have you implemented backup or restoration mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements? Do you test your backup or redundancy mechanisms at least annually?	Yes, Netradyne solution is a SaaS offering which is hosted on secure, highly available & scalable AWS (Amazon Web Services) Infrastructure. Netradyne has implemented backup and restoration mechanism as per industry and regulatory expectation to fulfilled the agreed SLAs requirements. BCP/DR drills are conducted periodically to test the redundancy, failover and restoration to normalcy.	JIO IRM	5-Aug-24
Change & Configuration Management	Do you follow change management process as per industry standards for System, Application/ Code changes?	Yes, Netradyne has the established procedure for System change request, change review, Change Planning, Approvals, Implementation and Closure in controlled & secure environment	JIO IRM	5-Aug-24
Data Security/Privacy	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	This was discussed in the call and Niraj has said that it is not so relevant as: 1) Sensitivity of captured data 2) Stricter controlled implemented for Data Security and Privacy at ND managed AWS environment. 3) IF requires, DPA (Data Processor Agreement) can be signed. All data is stored on datacenters in the US. Data may be accessed by Netradyne's staff and service providers globally to provide services to the customers.	JIO IRM	5-Aug-24
Data Security/Privacy	Do you have technical control capabilities to enforce tenant specific data retention policies?	Yes, We do have these capabilities as per business requirements and agreed contractual agreement. Netradyne Information Security Policy and Procedure	JIO IRM	5-Aug-24
Data Security/Privacy	Do you have a documented procedure for responding to requests for tenant data from governments, law enforcement agencies or third parties?	Yes, we do have such documented procedures and our dedicated Data Privacy Officer and Data Privacy team in collaboration with Legal team will take care of any such request.	JIO IRM	5-Aug-24
Data Security/Privacy	Is your Privacy Policy aligned with the Global privacy laws?	Yes, Netradyne strives to comply with applicable privacy laws and regulatory obligations. Towards that end, Netradyne reviews its privacy policy periodically.	JIO IRM	5-Aug-24
Data Security/Privacy	Do you provide options for data portability post contract termination?	Generally, most of the data remains on the device and is overwritten (every 100-200 hours based on device configuration). Data that is uploaded to the cloud is deleted based on the agreed data retention period (DRP). A small fraction of the data may be deidentified or anonymized (for product improvement, new product development etc.). Such data may not be available to fulfill data-portability requests. However, if data portability is a major requirement for the customer, the details (of such a feature/solution) may have to be discussed with Netradyne product and engineering teams during contract finalization	JIO IRM	5-Aug-24
Cryptographic Controls	Do you have key management policies binding keys to identifiable owners?	Yes, ND do have key management policies defined and implemented using AWS KMS (Key Management System)	JIO IRM	5-Aug-24

Cryptographic Controls	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes, ND do have encryption at rest using AES 256.	JIO IRM	5-Aug-24
Cryptographic Controls	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Yes, ND do have key management policies defined and implemented using AWS KMS (Key Management System)	JIO IRM	5-Aug-24
Cryptographic Controls	Do you provide strong encryption methodologies to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes, ND do have strong key encryption methodologies used while data in transit & rest. ND use secure TLS 1.2+ for such transfer and AES 256 while data at rest.	JIO IRM	5-Aug-24
Security Incident Management	Are systems in place to monitor privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes, ND have defined process and procedures to monitor and respond to privacy breaches and notify the relevant stakeholders withing the stipulated time.	JIO IRM	5-Aug-24
Infrastructure Security	Do you conduct penetration tests of your cloud service infrastructure including by a third party on a periodic basis?	Internal and External VAPTs are conducted periodically on ND Infrastructure to detect new and unremediated vulnerabilities.	JIO IRM	5-Aug-24
Infrastructure Security	Do you have separate Non-production & Production environment?	Yes, The production environment is logically segregated from the non-production environments.	JIO IRM	5-Aug-24
Infrastructure Security	Do you have segregation in place for application components (App, DB etc.) and follows a three tier architecture	Yes, ND follows the multi-tier and multi- cluster architecture to embed robust security in the design itself.	JIO IRM	5-Aug-24
Infrastructure Security	Are the cloud's internal and public/DMZ segments separated using different VLANs or Firewalls?	Yes, these capabilities are enabled using AWS Infrastructure and tools	JIO IRM	5-Aug-24
Infrastructure Security	Is the communication between the customers device/interface and the cloud applications encrypted using SSL/TLS encryption?	Yes, it is encrypted using Transport Layer Encryption (TLS)	JIO IRM	5-Aug-24
Infrastructure Security	Do you use secure protocols for accessing applications or systems? And insecure protocols such as FTP, telnet, IMAP, POP3 etc. are not used.	Yes, As per ND Information Security Policy and Procedure, any legacy or insecure protocols shall not be used. The same is getting monitored using Microsoft Defender XDR, Crowdstrike EDR and Crowdstrike CSPM for any anomaly and remediations.	JIO IRM	5-Aug-24
Infrastructure Security	Do you have strong controls to prevent advanced malware entering your network?	Yes, As per ND Information Security Policy and Procedure, antimalware solutions are in place using Microsoft Defender XDR, Crowdstrike EDR and Crowdstrike CSPM to detect any anomaly, monitor and ensure the remediations.	JIO IRM	5-Aug-24
Infrastructure Security	Is time synchronization on the cloud servers done through the central time servers(NTP) only?	Yes, we do have NTP in place as per standard AWS configuration setup.	JIO IRM	5-Aug-24
Infrastructure Security	Are the Infrastructure components hardened and only required services should be available to support the application stack.	Secure systems configuration standards/hardening baseline are defined for endpoint, cloud infra and OS. The same are getting reviewed, monitor for any changes.	JIO IRM	5-Aug-24
Infrastructure Security	Are the security patches applied to the virtual machines, hypervisors and applications periodically?	Patch & Vulnerability management (PVM) process has been defined and established to detect any vulnerability/patch; These security patches/remediations are tested, validated and deployed to the affected system within the stipulated timeline based on analyzed severity.	JIO IRM	5-Aug-24
Infrastructure Security	Does the CSP ensure that once the contract is over or terminated, the data in the CSP infrastructure will be disposed off completely in a secure way (degaussing or cryptographic wiping to avoid unauthorized disclosure of data?	Yes, this has been defined and established as per AWS standard contracts	JIO IRM	5-Aug-24
Infrastructure Security	Do you maintain effective Isolation and workload Security between tenant?	Netradyne follows secure log storage where encryption, role based authorization, network security controls is in place. Our solution is natively multi-tenant, we have common database, each tenant data is logically segregated using the tenant id. Tenant specific sensitive data is encrypted using unique tenant encryption key.	JIO IRM	5-Aug-24
Audit, Logging & Monitoring	Are applications hosted in your infrastructure protected by a Web Application Firewall? Are network monitoring tools in place to monitor the network level threats?	Yes, ND managed AWS Infra is protected using WAF, AWS VPC, AWS Security Groups. All Ingress and Egress activities are monitored using AWS native tools (such as Cloud trail, Guard duty, AWS security Hub, Cloud watch etc.) alongside Data Dog, Crowdstrike CSPM and all these logs are ingested to Netradyne centralize security operation center (SOC) for detecting any anomaly and provide the remediations.	JIO IRM	5-Aug-24
Audit, Logging & Monitoring	Are the logging facilities and log information protected against tampering and unauthorized access? Do you review audit logs for Root/ Administrative access on all systems in Virtualized environment?	Yes, Netradyne follows secure log storage and access to that is provided to only specific people based on job responsibility. These accesses are monitored and flagged for any suspicious activity.	JIO IRM	5-Aug-24
Audit, Logging & Monitoring	Do you monitor your cloud infrastructure continuously for cyber threats? Do you have a mechanism/process to report tenants in case of a suspected breach?	Yes, we have a centralized Security Operation Centre (SOC) & Site Reliability Engineers (SRE) Team to monitor our cloud infra, application and customer related metrics. We do have a defined procedure in place to notify the suspected breach to relevant stakeholders within the stipulated timeline	JIO IRM	5-Aug-24
Audit, Logging & Monitoring	Do you have the capability to provide logs to the tenant in case of a security breach	ND has technical capability to provide the customer specific logs in case of any reported breach, if needed. *Subjective to engagement terms and legal clearance	JIO IRM	5-Aug-24
Data Security/Privacy	What are the datasecurity measures your organization adopts for storing, handling, processing for / on behalf of Navistar	"Netradyne's privacy policy is available at https://www.netradyne.com/privacy-policy For the vast majority of Personal Information processing conducted by Netradyne through the Driver•i device (or related services or accessories), Netradyne is acting as a data processor or service provider on behalf of its business customers, and such processing is carried out in compliance with our legal and contractual obligations with business customers. Our business customer is responsible for complying with laws that may require notice, disclosure or consent related to the transfer of Personal Information to Netradyne. Netradyne enters into agreements with our business customers that legally require Netradyne to protect the Personal Information we receive or are directed to collect and use it only to provide our products and services to the business customer. A very small fraction of data collected through the Driver•i device (or related services and accessories) will enter Netradyne's Training Data for machine learning purposes. For such machine learning activities, and to the extent Netradyne is processing Personal Information, Netradyne is acting as the controller or business of the Personal Information. The Safer Roads and Safer Driving sections of the Privacy Policy (https://www.netradyne.com/privacy-policy) provide information specifically about how Netradyne collects and uses data for training its machine learning models.	NaviStar	12-Aug-24

Data Security/Privacy	What (type) data your organization stores, handles, process for / on behalf of Navistar	The Driveri device fitted on customer vehicles captures video of the driver, the road and the surrounding environment along with inertial data (accelerometer and gyroscope data) and geolocation data. Most of the recorded data remains on the device and is overwritten with new data-stream as the device memory becomes full. Less than 1% of video data might be uploaded to a cloud server as part of the services provided to customers. Safety events are detected based on processing of video and sensor data on the Driver•i device. Inward camera video recordings are used to detect safety events such as distracted driving or wearing a seatbelt. Recordings of drivers, passengers, or other Personal Information (such as may be visible on name tags) may be contained in these inward camera video recordings. Outward camera video recordings are used to detect safety events such as coming to a complete stop at an applicable stop sign. Processing of outward camera data results in the detection of cars, motorcycles, bicycles, etc. with their individual position and movement in relation to the Driver•i-equipped vehicle as well as the position and movement of pedestrians. Recordings of individual road users, license plates or other Personal Information may be contained in these video recordings. Safety event data may be used by our customers for, among other reasons, driver commendation or training purposes, and for managing the relationship with the driver. Please see this list of events that may be captured, collected, stored or processed along with supporting video. High G Driver Initiated Low Impact Potential Collision Traffic Light Violation Sign Violation U Tunr Hard Braking Hard Turn Hard Acceleration Driver Distraction Following Distance Speeding Violations Seatbelt Compliance Camera Obstruction Driver Drowsiness Weaving Railroad Crossing Collision Warning	NaviStar	4-Sep-24
Data Security/Privacy	How do you separate Navistar's data from other customers' data?	We implement strict data segregation protocols to ensure customer data is isolated from other data. This includes logical separation and associated access control to prevent unauthorized access and ensure data integrity. Our solution is natively multi-tenant, each tenant data is logically segregated using the tenant id. Tenant specific sensitive data is encrypted using unique tenant encryption key.	NaviStar	12-Aug-24
Data Security/Privacy	Where do you store Navistar data? Region / Datacenter location etc.	AWS US West	NaviStar	12-Aug-24
Data Security/Privacy	Is the data encrypted at-rest?	We employ encryption methods such as AES-256 to protect data at rest. Our encryption keys are managed securely using key management systems, and we regularly review and update our encryption policies to align with industry best practices.	NaviStar	12-Aug-24
Data Security/Privacy	What is the encryption strength? Provide details	We employ encryption methods such as AES-256 to protect data at rest.	NaviStar	12-Aug-24
Data Security/Privacy	Do we have option to manage the encryption keys for our data? Please explain.	We have key management policies defined and implemented using AWS KMS (Key Management System) for Netradyne managed environment. Keys are rotated based on defined intervals.	NaviStar	12-Aug-24
Data Security/Privacy	What is your data retention policy?	Data can be kept or deleted post account closure based on agreed data retention policy with client. Our data retention policy is 90 days for video and 12 months for data points. Netradyne take database backups every 4 hours, and retain them for 4 days (we can do point-in-time-recovery to any point in the last 4 days.) Data retention for raw payloads is governed by the video and non-video DRP (data-retention-policy) that is a part of customer agreements.	NaviStar	12-Aug-24
Data Security/Privacy	Is the data encrypted in-transit?	We use TLS/SSL encryption for data in transit to secure communications between systems. Additionally, we employ VPNs and secure tunneling protocols for internal data transfers to further protect data from interception and unauthorized access.	NaviStar	12-Aug-24
Data Security/Privacy	Do you support TLS 1.2 or above?	Yes, We do leverage TLS 1.2 or above for secure communication channels.	NaviStar	12-Aug-24
Data Security/Privacy	Have you disabled deprecated TLS versions?	Yes	NaviStar	12-Aug-24
Data Security/Privacy	What is the minimum TLS version supported?	TLS 1.2 and above	NaviStar	12-Aug-24
Data Security/Privacy	What mechanisms are used to load data from Navistar to your service? Example - SFTP, API, streaming, HTTPS transfer etc. *This question is applicable to Initial load, real-time and batch process.*	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs, which is the front end of Multi-Tier architecture, DBs are at back end and only accessible though Netradyne internal web API services to fetch the data for the requests.	NaviStar	12-Aug-24
Data Security/Privacy	Does the camera on the vehicle directly send data to the backend? If so, how?	Yes via wireless 5G/LTE network provider e.g. TMobile and follows Netradyne's data transfers and encryption procedures: In transit - SSL / TLS 1.2 and above At rest – AES-256 On back up – AES-256 On device - AES-256 algorithm for data encryption.	NaviStar	4-Sep-24

Data Security/Privacy	How do you identify and prevent data exfiltration from your environment? Provide details for both live and backup data.	Data exfiltration risks are identified and proactively managed using following security controls: 1. Encryption at rest and in transit 2. Environment and Resource segregation 2. Usage of secure and latest communication protocol 4. 24X7 monitoring of application and underlying infrastructure with real time alerting and analysis at Netradyne Security Operation Centre. 5. Secure Data Backup 6. Granular Access Control, following need to know and least privilege principals. 7. Implementation of robust data security/privacy measures and controls across Netradyne.	NaviStar	12-Aug-24
Physical & Environmental Security	Is the data center managed by a third party? Provide details.	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. Physical & infra security of hosting infrastructure is AWS responsibility. AWS supports security standards and compliance certifications which includes PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements. For more information please refer https://aws.amazon.com/compliance/data-center/controls/	NaviStar	12-Aug-24
Physical & Environmental Security	Is access to critical assets restricted and monitored 24x7? Provide details	Yes, Access to critical assets &underlying infrastructure are monitored on 24X7 basis with real time alerting and analysis at Netradyne Security Operation Centre (SOC). User access rights and permissions are managed through a role-based access control (RBAC) system. Access is granted based on the principle of least privilege, ensuring users have only the access necessary to perform their job functions. Access reviews and audits are conducted regularly.	NaviStar	12-Aug-24
Governance Risk & Compliance	Do you have SSAE 18 - SOC2 Type 2 report?	On SOC2, we have not gone through the certification yet but our existing controls maturity and security certifications aptly covers the Customer expectations on Information Security front. We have stringent levels of protection to secure our product(s) and underlying infrastructure. Netradyne adopt industry best security practices and is certified with ISO 27001:2022; 27701:2019 & HIPAA recognitions. The same can be shared under NDA. Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management.	NaviStar	12-Aug-24
Governance Risk & Compliance	If the answer to previous question is YES, Can you share the SOC2 Type 2 report?	Netradyne adopt industry best security practices and is certified with ISO 27001:2022; 27701:2019 recognitions. The same can be shared under NDA.	NaviStar	12-Aug-24
Vulnerability & Patch Management	How often do you scan for vulnerabilities on your network and applications?	Netradyne has defined and established Patch & Vulnerability Management Process and control implementations. Our infrastructure, platform and other systems are getting scanned and monitor on continuous basis using Security Operation Centre and Tools like, Vulcan, Crowdstrike CSPM, AWS Native tools (such as Guard Duty, Cloud Trail, Cloud Watch, Amazon Inspector etc.). We test applications against OWASP Top Ten vulnerabilities. External PEN Testing is done yearly by recognized organization following industry standards. We also conduct PEN testing internally on regular basis.	NaviStar	12-Aug-24
Vulnerability & Patch Management	What is your vulnerability remediation / patching policy?	Netradyne has defined and established Patch & Vulnerability Management Process and control implementations. We revied the PVM process, identified vulnerabilities and patch status with various teams on monthly basis. All the vulnerability remediations and patch deployments are tested, implemented within the defined timeline based on severity and validated with pre and post patch reports.	NaviStar	12-Aug-24
Vulnerability & Patch Management	Do you allow Navistar to conduct an external vulnerability assessment on your network?	It will be an unnecessary duplication. We have already employed external independent security firm to do the external Vulnerability Assessment on Netradyne system and if requires, the report can be shared if requires under NDA.	NaviStar	12-Aug-24
Vulnerability & Patch Management	Do you allow Navistar to conduct a penetration test on your application?	It will be an unnecessary duplication. We have already employed external independent security firm to do the external PenTest on Netradyne system and if requires, the report can be shared under NDA.	NaviStar	12-Aug-24
Vulnerability & Patch Management	Have you subscribed to any third party security scoring services?	We have a recently concluded third party (CyberGRX) security scoring comprehensive report available and the same can be shared under NDA.	NaviStar	12-Aug-24
Vulnerability & Patch Management	If the answer to previous question (Third Party Security Scoring Services Subscription) is YES, can you provide the service name and current score?	**CyberGRX Third Party Risk Assessment:** Strategic-5 out of 5 Operational-4.83 out of 5 Core-5 out of 5 Management-5 out of 5 Privacy-4.83 out of 5	NaviStar	12-Aug-24
Identity & Access Management	Do you support SAML 2.0 federated Single Sign-On (SSO)?	No	NaviStar	12-Aug-24
Identity & Access Management	Do you support Oauth 2.0 / OpenID Connect Single Sign-On (SSO)?	Yes, depending on the agreed terms and conditions	NaviStar	12-Aug-24
Identity & Access Management	Do you support any other federation standards? Provide details	NA	NaviStar	12-Aug-24
Identity & Access Management	Do you need local login for Administration IDs? (This is to bypass SSO for administration purposes)	NA	NaviStar	12-Aug-24
Identity & Access Management	If the answer to previous question is YES, please provide security controls for those IDs	NA	NaviStar	12-Aug-24
Identity & Access Management	Once SSO is enabled, do you have option to turn off local logins?	NA	NaviStar	12-Aug-24
Identity & Access Management	How do you secure the local user IDs and access credentials?	NA	NaviStar	12-Aug-24
Identity & Access Management	How do you handle user turnover (provisioning and deprovisioning accounts)?	NA	NaviStar	12-Aug-24

Identity & Access Management	Can you support multifactor authentication?	We have enabled Two-Factor authentication for various services like Office 365, AWS console, GIT, Sentry for all the employees. For IDMS console we have enabled Two-Factor authentication for high privilege roles only. Employees working remotely need to login to our VPN using IT issued credentials. We have different levels of access via VPN, and access is provided on need-basis	NaviStar	12-Aug-24
Identity & Access Management	Do you perform background checks on all relevant personnel? Provide details.	Yes, we do background checks. Netradyne ensure that all employees, contractors, and third-party personnel who have access to sensitive information or critical systems are thoroughly vetted before being granted access.	NaviStar	12-Aug-24
Identity & Access Management	Do the developers have access to the production environment?	Yes	NaviStar	12-Aug-24
Identity & Access Management	Do you document your employee access to customer data?	Yes, roles has been defined and permissions have been assigned accordingly.	NaviStar	12-Aug-24
Identity & Access Management	Do you have an approval workflow before getting access to the customer data?	Yes, we do have as per Netradyne defined Identity and Access Management policy, which takes care of overall account Lifecyle security (consists screening, onboarding, provisioning, management, offboarding and de-provisioning of accounts)	NaviStar	12-Aug-24
Identity & Access Management	How do you ensure that access to shared logs and resources won't reveal sensitive information about Navistar?	Netradyne has received Privacy-by-Design certification and is also ISO 27001 certified. Netradyne maintains policies and procedures to safeguard personal data. All privacy complaints and incidents are reviewed by the privacy team and escalated appropriately in coordination with InfoSec.	NaviStar	12-Aug-24
DevSecOps	Do you follow OWASP or any other standard guidelines for application development?	Netradyne has defined and established Patch & Vulnerability Management Process and control implementations. We test applications against OWASP Top Ten vulnerabilities. We also perform penetration testing on web applications once in a quarter. We have appropriate entry and exit processes to ensure only authorized users have access to our systems at any given time. We review other processes on an ongoing basis from security perspective. External PEN Testing is done yearly by recognized organization following industry standards. We also conduct PEN testing internally on regular basis.	NaviStar	12-Aug-24
DevSecOps	Do you have a formal SDLC program? Please explain.	We adhere to standard SDLC practices and align with DevSecOps requirements which cater the need of security by design, Threat modelling and Secure architecture, code reviews, code commit and release management, Pentest, logging and monitoring of all changes. Access to code repositories are restricted to authorized personnel only.	NaviStar	12-Aug-24
DevSecOps	Do you follow DevSecOps process? Provide details	We adhere to standard SDLC practices and align with DevSecOps requirements which cater the need of security by design, Threat modelling and Secure architecture, code reviews, code commit and release management, Pentest, logging and monitoring of all changes. Access to code repositories are restricted to authorized personnel only.	NaviStar	12-Aug-24
DevSecOps	Do you scan, test and certify outsourced, packaged and third party components used in your service?	Yes	NaviStar	12-Aug-24
DevSecOps	What application security measures (if any) do you use in your production environment? (Example - application firewall, authentication gateway, audit logs etc.)	Yes. We use AWS Security groups for cloud hosting. For office network Netradyne has Unified Threat Management with inline packet inspection firewall.	NaviStar	12-Aug-24
DevSecOps	Do you support role based authorization?	Yes	NaviStar	12-Aug-24
DevSecOps	If the answer to above question is YES, can you consume role memberships through security assertion tokens?	No	NaviStar	12-Aug-24
DevSecOps	Do you support Oauth 2.0 for API security?	Yes	NaviStar	12-Aug-24
DevSecOps	If answer to above question is YES, do you accept OAUTH tokens from an external provider?	Yes	NaviStar	12-Aug-24
DevSecOps	Does your application integrate or use third party AI enabled assistants (example - Open AI Chat GPT, Google Bard and others) or use AI assistants?	Yes, we provide Safety Manager Assistant is an innovative chat assistant that is specifically designed for Safety Managers. It is a powerful tool that provides real-time support by instantly analyzing extensive amounts of Fleet and driver data. This intelligent virtual assistant harnesses advanced AI technology to deliver accurate and timely information, thereby enabling Safety Managers to proactively address potential issues and make informed decisions on the spot. The Assistant also incorporates Driver Data information and will enable the user to start asking driver and alert questions such as	NaviStar	12-Aug-24
DevSecOps	How do you protect certificates and credentials that are being used in your cloud applications?	We use Authentication and Authorization to control data access from external interfaces.	NaviStar	12-Aug-24
Security Incident Management	Do you have a formal incident response process? Provide details	Yes, Netradyne InfoSec-Security Operation team performs monitoring, including documentation, classification, escalation, coordination and tracking of incidents per documented procedures. -Additional Threat Intel: Netradyne-developed use cases for auto-remediation of most common system misconfigurations -Custom use cases: Additional custom use cases can be implemented for each application/system on boarded -Incident Response Processes: Processes and procedures defined and operationalized for alert categorization and priority, notification trees, escalation paths, and response workflows -Log Centralization: Log centralization capability deployable via automation to aggregate log sources and enable ingestion into SIEM solution -Deployment Templates: Templates and configurations established to expedite deployment of SIEM capabilities	NaviStar	12-Aug-24
Security Incident Management	Can you transfer security event logs pertaining to Navistar data to Navistar SIEM solution?	Possible, depending on the agreed terms and conditions	NaviStar	12-Aug-24
Security Incident Management	In case of a data breach, within what time period will Navistar be notified?	We have 'Data Breach Response and Notification procedure' policy in place. Netradyne standard notification time is 72 Hrs.	NaviStar	12-Aug-24
Infrastructure Security	Do we need to allow any ports other than port 443 (HTTPS) from Navistar network to your systems?	NA, unless there is a customer specific requirement and agreed in contract.	NaviStar	12-Aug-24

Infrastructure Security	Do we need to allow any incoming traffic from your network to Navistar?	 Architecture Overview of Driveri solution is provided for understanding. DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs.	NaviStar	12-Aug-24
Infrastructure Security	Do we need a VPN connection to your network?	DriverI is a SaaS solution offering which is hosted on AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs.	NaviStar	12-Aug-24
BCP & DR	Do you provide high availability? Please explain	We use AWS which provides highly stringent data reliability and service availability SLAs.	NaviStar	12-Aug-24
BCP & DR	What uptime guarantee in the SLA you will provide to Navistar?	SLA is 99%. In reality, our uptime has been close to 99.7% this year	NaviStar	12-Aug-24
BCP & DR	Do you have disaster recovery and/or business continuity planning documents?	We use AWS which provides highly stringent data reliability and service availability SLAs. DriverI offering is SaaS solution hosted on Auto scalable, robust and redundant AWS Infrastructure. Netradyne backup DB data.	NaviStar	12-Aug-24
BCP & DR	If answer to previous question is YES, can we review them?	NETRADYNE systems are hosted on AWS infrastructure which supports high availability. Infrastructure resiliency is provided by AWS. AWS supports security standards and compliance certifications which includes PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements. For more information please refer https://aws.amazon.com/compliance/data-center/controls/	NaviStar	12-Aug-24
BCP & DR	What is your Recovery Point Objective (RPO) and Recovery Time Objective (RTO)?	Recovery Time Objectives (RTOSs) and Recovery Point Objectives (RPOS) are established and monitored based on Customer's requirements as defined in SLAs (By Default its aligned with SLA of 99%).	NaviStar	12-Aug-24
BCP & DR	Where are your recovery data centers located?	Our entire stack is hosted by the secure and scalable AWS architecture which are located primarily within US West 1.	NaviStar	12-Aug-24
Data Security/Privacy	What Personally Identifiable Information (PII) or Protected Health Information (PHI) do you collect, if any?	Within the Driver.i application, users have the option to store Driver name, phone number, email, and license number. While it is recommended to store a Driver's first and last name, all other fields are optional. Further, the Driver.i device fitted on customer vehicles capture driver photographs and video, geolocation of the vehicle, alerts generated, timestamps. GreenZone scores are generated as a function of certain alerts that are generated. The data stored within IDMS is not subject to NERC CIP.	NaviStar	12-Aug-24
Data Security/Privacy	How do you secure the PII/PHI data?	Netradyne has stringent levels of protection to secure our product(s), Data (Including PII, PHI) and underlying infrastructure. Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST SP 800-53 and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management. Netradyne is also certified with ISO 27001:2022, 27701:2019 Standards & HIPAA regulations. The same can be shared under NDA. Netradyne has ability to: 1. Discover and Classify sensitive data and apply stringent and customized security controls. 2. Map Data and Permissions to maintain the RBAC, Need to Know and Least Privilege Principals. 3. Manage prudent access control across the organization resources. 4. Monitor data, file activities and user behavior in its security operation center and provide the proactive remediations. 5. In summary, perimeter and boundary level NGFW are installed which filters the traffic. WAF is also equipped along with IPS/IDS. Netradyne uses enterprise scale Security Solutions and tools providing RBAC & Least Privilege, Network Security, Firewall, UTM, APT, IDS/IPS to protect the systems. It has AES 256-bit encryption for data at rest and backups. It uses SSL/TLS 1.2+ for data in transit	NaviStar	12-Aug-24
Data Security/Privacy	How long will the PII/PHI be stored?	Most of the data that is collected remains on the Netradyne Driver.i device and is overwritten once the device storage is full. The data on the device may be retained for up to 200 hours depending on the model and configuration of the Driver.i device. A limited amount of data (<1%) is uploaded to the cloud. For the data uploaded on the cloud- - Video data uploaded is available 90-days plus the current month - Non-Video data is available for 12 months plus the current month Subject to legal and contractual permissions, Netradyne may retain a very small subset of data uploaded to the cloud in deidentified or anonymized form to improve/develop existing or new products/services.	NaviStar	12-Aug-24
Data Security/Privacy	How do you identify where PII/PHI data is stored in case Navistar needs to respond to individuals "right to know" or delete data "right to forget" requests?	Driver details (including driving session details) are stored within the IDMS system. Netradyne has a process to assist customers in responding to DSARs (Data Subject Access Requests). While customers are primarily responsible for responding to data subject requests (for access, deletion etc.), Netradyne has well defined workflows to locate relevant data and act as per customer instructions.	NaviStar	12-Aug-24
Data Security/Privacy	How do you ensure that sensitive data (e.g., PII, SSN, payment card number) is properly masked in all non-production environments?	Deidentified data is used for training ML models	NaviStar	12-Aug-24
Data Security/Privacy	What type of privacy awareness training do you provide to individuals that have access to or handle PII/PHI data?	We use KnowBe4 security awareness and training platform to provide ongoing awareness and training to employees on various aspect which includes information security and data privacy. Along with annual awareness program, we do conduct quiz and other awareness campaigns.	NaviStar	12-Aug-24
Data Security/Privacy	Under what conditions might third parties, including government agencies, have access to Navistar data?	Netradyne shares some data with its service providers in the context of providing services to its customers. Netradyne has appropriate contractual arrangements with these service providers. More information is provided here- https://www.netradyne.com/privacy-policy#:~:text=Us%E2%80%9D%20below.- ,How%20We%20Disclose%20your%20Personal%20Information,-We%20do%20not	NaviStar	12-Aug-24

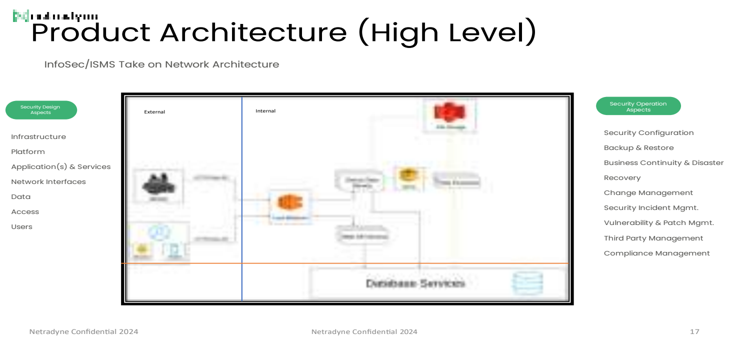
Data Security/Privacy	How do you maintain compliance with existing and upcoming privacy laws and regulations?	Netradyne's privacy team keeps track of existing and upcoming privacy laws and regulations. Netradyne also provides a short overview of biometric laws to assist customers in their compliance efforts- https://www.netradyne.com/biometric-data-processing-regulatory-overview. Our policies and procedures are periodically updated to ensure compliance with existing laws and regulations.	NaviStar	12-Aug-24
Audit, Logging & Monitoring	Can you accommodate a timely forensic investigation? (e.g., eDiscovery)	Yes, we have capability to support investigation with logs and data, subjected to business requirements and customer agreements	NaviStar	12-Aug-24
Audit, Logging & Monitoring	How long do you keep logs and audit trails?	Our default log retention period is 12 months. Data (including logs) can be kept or deleted post account closure based on agreed data retention policy with client.	NaviStar	12-Aug-24
Audit, Logging & Monitoring	Do we have visibility to the logs?	Netradyne has technical capability to provide the customer specific logs in case of any reported breach, if needed. *Subjective to engagement terms and legal clearance	NaviStar	12-Aug-24
Audit, Logging & Monitoring	Can you send the logs to our log aggregation (SIEM) solution?	NA, Netradyne has established a dedicated security operation center and centralized SIEM solution is in place. Netradyne managed AWS Infra is protected using WAF, AWS VPC, AWS Security Groups. All Ingress and Egress activities are monitored using AWS native tools (such as Cloud trail, Guard duty, AWS security Hub, Cloud watch etc.) alongside Data Dog, Crowdstrike CSPM and all these logs are ingested to Netradyne centralize security operation center (SOC) for detecting any anomaly and provide the remediations.	NaviStar	12-Aug-24
Audit, Logging & Monitoring	Do you provide an interface to Cloud Access Security Broker (CASB)?	NA, Netradyne DriverI solution does not have any such requirement for customer(s).	NaviStar	12-Aug-24
Audit, Logging & Monitoring	Can you show evidence of tamper-proofing for logs and audit trails?	Yes, Log centralization capability deployable via automation to aggregate log sources and enable ingestion into Netradyne SIEM solution. Netradyne follows secure log storage and access to that is provided to only specific people based on job responsibility. These accesses are monitored and flagged for any suspicious activity.	NaviStar	12-Aug-24
Governance Risk & Compliance	Are you ISO-27001:2013 compliant?	We have stringent levels of protection to secure our product(s) and underlying infrastructure. Netradyne adopt industry best security practices and is certified with ISO 27001:2022 and 27701:2019 recognitions. The same can be shared under NDA. Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management.	NaviStar	12-Aug-24
Governance Risk & Compliance	GDPR-Is your application compliant for any of the following? If so, please include details or compliance plans: (please indicate if item does not pertain to your business)	Yes	NaviStar	12-Aug-24
Governance Risk & Compliance	CCPA-Is your application compliant for any of the following? If so, please include details or compliance plans: (please indicate if item does not pertain to your business)	Netradyne has the alignment. California specific privacy rights accorded to consumers as well as our commitments are detailed in our Privacy Policy- https://www.netradyne.com/privacy-policy. Further, we have stringent levels of protection to secure our product(s), Data and underlying infrastructure. Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST SP 800-53 and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management.	NaviStar	12-Aug-24
Governance Risk & Compliance	HIPAA-Is your application compliant for any of the following? If so, please include details or compliance plans: (please indicate if item does not pertain to your business)	Yes	NaviStar	12-Aug-24
Governance Risk & Compliance	PCI-Is your application compliant for any of the following? If so, please include details or compliance plans: (please indicate if item does not pertain to your business)	NA, Our DriverI Infra and Platform does not have any PCI data. Physical security of hosting infrastructure is AWS responsibility. AWS supports security standards and compliance certifications which includes PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements. For more information please refer https://aws.amazon.com/compliance/data-center/controls/	NaviStar	12-Aug-24
Governance Risk & Compliance	ITAR -Is your application compliant for any of the following? If so, please include details or compliance plans: (please indicate if item does not pertain to your business)	NA However, Netradyne has the alignment. We have stringent levels of protection to secure our product(s), Data and underlying infrastructure. Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST SP 800-53 and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management. Netradyne is also certified with ISO 27001:2022, 27701:2019 Standards & HIPAA regulations. The same can be shared under NDA. Netradyne has ability to: 1. Discover and Classify sensitive data and apply stringent and customized security controls. 2. Map Data and Permissions to maintain the RBAC, Need to Know and Least Privilege Principals. 3. Manage prudent access control across the organization resources. 4. Monitor data, file activities and user behavior in its security operation center and provide the proactive remediations. 5. In summary, perimeter and boundary level NGFW are installed which filters the traffic. WAF is also equipped along with IPS/IDS. Netradyne uses enterprise scale Security Solutions and tools providing RBAC & Least Privilege, Network Security, Firewall, UTM, APT, IDS/IPS to protect the systems. It has AES 256-bit encryption for data at rest and backups. It uses SSL/TLS 1.2+ for data in transit	NaviStar	12-Aug-24

Identity & Access Management	When setting up a user in Netradyne dashboard we have the ability to allow user to use the app. At that time, if we opt for having the user log in select a password – what are the requirements? For example, 7 characters, 1 capital, 1 special character. Also, are there any rules around password needs to change after a period of time?	•The Netradyne IDMS application requires unique user credentials with a strong password. All credentials are encrypted and hashed. DriverI IDMS solution has its own authentication server where the users are authenticated. It supports SSO based on OpenID Connect (OIDC). In case Customer opt for SSO (off course depends on business agreement and additional cost, if any), they can control their own tenant authentication with their password policies including enforced rotation. Users will access the Netradyne SaaS application through their web browser/mobile using Https REST services. •Default Password parameters are in conformity with Netradyne Information Security Password Policies and Standards: •The password must contain at least 8 characters and shall follow the complexities (like inclusion of upper case, lower case, numbers & special symbols) •The password must not contain first-name, last-name, or username. •Passwords History Restriction is maintained •Not be a dictionary word or proper name. •Restrict sequential and repetitive characters (e.g., 12345 or aaaaaa). •Not be the same as the User ID. •Not be displayed when entered. •IDMS users can change their password at regular intervals, but it is not enforced.	Weyerhaeuser	20-Sep-24
Audit, Logging & Monitoring	Traceability: For example, if a user in the system makes change such as create or delete a user, does the application have the ability for you to view the logs and see who made the change, what action was performed, and when? If yes, how long are these logs saved in the system?	Yes, Netradyne does have these capabilities of log enablement and supporting non-repudiations. These log data is securely stored/archived and retained for 12 months.	Weyerhaeuser	20-Sep-24
Audit, Logging & Monitoring	Logging/monitoring: for the items you listed about that are traceable, at what level are they detailed for example: user who made the action, the action that the user took, the time which the action occurred, the IP address and/or device that that change occurred from, city/country that the change occurred from, application/module that the change occurred in, etc.	Yes, we do have these capabilities and through application/File/DB logs we can monitor/determine all the required details (such as User details, Activities details, Time stamp, IP Adress, City/Country, Application/Service Traces etc.)	Weyerhaeuser	20-Sep-24
Governance Risk & Compliance	Can you check whether your app has a SOC 2 Certificate? I think we did not think it was which is why we had you complete the SIG questionnaire but want to cross check.	•On SOC2, we have not gone through the certification yet but our existing controls maturity and security certifications aptly covers the Customer expectations on Information Security front. We have stringent levels of protection to secure our product(s) and underlying infrastructure. Netradyne adopts industry best security practices and is certified with ISO 27001:2022 and 27701:2019 recognitions. The same has already been shared. (A copy attached with this mail- Netradyne Inc- ISMS - 2024.pdf) •Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management.	Weyerhaeuser	20-Sep-24
BCP & DR	Do you have a disaster recovery plan? How does that incorporate not only bringing back up your Web/App but also bringing back customer data?	•Yes, Netradyne system Disaster Recovery Plan is established, implemented and maintained for its products, systems and infrastructure. BCP plans are in place to support continued operations of Netradyne Managed Services. BCP/DR drills are conducted periodically to test the redundancy, failover and restoration to normalcy. •AWS DriverI offering is a SaaS solution hosted on Auto scalable, robust and redundant AWS Infrastructure which provides highly stringent data reliability and service availability SLAs. Netradyne backup DB data, codes and system configurations which will help in bringing back up our services as well as customer data. Netradyne has implemented backup and restoration mechanism as per industry and regulatory expectation to fulfilled the agreed SLAs requirements.	Weyerhaeuser	20-Sep-24
Artificial Intelligence Management System (AI/ML)	1.1 Name of AI project (Single selection allowed)	Risk Engineering | 301	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	1.2 Third Party Name *	Netradyne, Inc.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	1.3 Provide a detailed description of the business use case *	Netradyne provides driveri devices that are powered with Netradyne's proprietary AI technology to detect certain road and driving conditions to ensure safer roads. This includes analyzing driving sessions and generating alerts when unsafe driving behavior (such as distracted driving, not wearing seatbelt, drowsiness, etc.) is detected.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	1.4 What is the AI component you are exploring? (Multiple selections allowed) (Allows other) *	Computer Vision (non-generative) Facial Recognition Facial recognition applies only when the customer has chosen to use the Visual Login Service (VLS) feature.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	1.5 Does your solution use Generative AI? (Single selection allowed) *	No	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	1.6 As part of the services being provided to Zurich, are you providing a solution which includes, embed, link to AI, or data derived from AI based on the OECD definition of AI? (Single selection allowed) (Justification allowed) (Justification required) *	Yes	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	1.7 Please provide a brief explanation of how your solution uses or incorporates AI and the techniques used? *	The Driveri device fitted on customer vehicles captures the driver, the road, the surrounding environment, geolocation and inertial data. Real-time video streams are analyzed, using computer vision and deep learning, to detect certain driving events (such as traffic-sign violation, not wearing seatbelt, distracted driving etc.).	Zurich NA	30-Sep-24

Artificial Intelligence Management System (AI/ML)	1.8 Do you provide any notification to the end user that they are interacting with an AI solution? (Single selection allowed) (Justification allowed) (Justification required) *	No Netradyne requires its customers to provde legally required notices to their drivers. Netradyne does provide information relating to the use of data for machine learning purposes in its privacy notice.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.1 What is the source data you are using to train your models? *	Data for developing the algorithm is sourced directly from driveri devices deployed on customers' vehicles (under appropriate contractual arrangement) or test vehicles deployed by Netrdyne.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.2 Is any Zurich data being used to train the models? (Single selection allowed) (Justification allowed) (Justification required) *	Yes Zurich data may be used to retrain Netradyne's AI models. This is required to improve the accuracy of the models.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.3 If the Zurich data contains PII, will the model be trained on the PII? (Single selection allowed) *	No The training data is deidentified such that the driver and customer identifiers are removed from the training data set.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.4 Please provide explanation. *	The training data set is deidentified.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.5 Can you ensure that Zurich data is not being saved? (Single selection allowed) (Justification allowed) (Justification required) *	No This question is not very clear. Netradyne stores and processes certain customer data for a defined data retention period (DRP) to provide the agreed services. In the context of model training, if Zurich's data is not to be used, the ML models' accuracy may deteriorate or the model may continue to repeat errors for longer than they normally would.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.6 Can you ensure that Zurich data is not being used to retrain any models? (Single selection allowed) (Justification allowed) (Justification required) *	Yes If Zurich prohibits Netradyne from using its data for retraining the models, the models may continue to make certain errors for longer than they would otherwise.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.7 If someone requested their information be deleted from the model, how would that be handled and what impact would that have on this product? *	Individual drivers may request Netradyne to stop training its models based on their images, subject to applicable laws. If a driver chooses to opt-out of Training Data, newly collected images collected during driving sessions associated with the driver will not be selected as Training Data. As a result, on-device processing may continue to make certain errors for longer than it would otherwise. Images of the driver that have already been selected as Training Data prior to the opt-out request may continue to be used as Training Data as the deidentification process and related privacy protections are designed such that Training Data images are effectively unsearchable.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	2.8 Was permission obtained from any individuals whose voice, image, writing, art, and/or likeness was used in the training of the model (at any stage)? (Single selection allowed) (Justification allowed) (Justification required) *	Yes Netradyne requires its customers to obtain necessary permissions from their drivers so that their data can be processed by Netradyne. To assist customers with obtaining drivers' consent, Netradyne provides a sample consent forms on its website- consent for in-cab safety features (https://www.netradyne.com/sample-consent-form-in-cab-safety-features) and consent for visual login service (https://www.netradyne.com/sample-consent-form-visual-login-system).	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	3.1 Will the model be hosted on the Zurich network? (Single selection allowed) (Justification allowed) (Justification required) *	No Most of the models are deployed on the edge (hosted on driveri devices fitted on customer vehicles). The VLS model and the blurring models are hosted on AWS cloud managed by Netradyne.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	3.2 Is the model hosted within the continental United States? (Single selection allowed) (Justification allowed) (Justification required) *	Yes Most of the models are hosted on the driveri devices that are fitted on customer vehicles. The VLS model and the blurring models are hosted on AWS servers (in the US) managed by Netradyne.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	3.3 If the model breaks (i.e. is unresponsive, producing unusual results, etc.) what operations are impacted? *	The model might not produce expected outcomes resulting in inaccurate alerts or no alerts being generated.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	3.4 How will return of services be handled until it resumes normal function? *	If an on-device model crashes/hangs, there are mechanisms to automatically detect the anomaly and restart the inference service to restore normal operation. Typically, such restoration can happen within a very short period of time (within a minute). Such issues are limited to the individual device running the model (not the entire network). There are mechanisms, including auto-scaling groups, to provision computing resources as required.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	4.1 What is the expertise of your employees developing and monitoring the solution? *	Different AI models corresponding to different safety features are developed, trained, and monitored by dedicated Developers. Many of the Developers have PhD degrees or other advanced degrees and/or multiple years of experience in developing, training, and testing AI models.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	4.2 Describe the annotation process used for the training and validation of the model? *	Human labelers review data to annotate videos with labels that are relevant to the AI system being built or improved. Quality Assurance of labels is performed by the feature developer. The feature developer is also responsible for the labelling instructions and may refine or update labelling instructions in response to QA activity.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	4.3 Please provide who performed the annotation and how the QA was performed. *	The labelers add relevant labels to the video frames based on instructionsprovided by the developers. The current process of labeling also involves a team of reviewers who review the labels for correctness.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	4.4 Has algorithmic failure or prohibition been considered in your business resilience plans? *	Certain features may be disabled till the causes of the failure are identified and rectified. Note that alerts related models are mostly deployed to edge devices and not on a centralized server and issues with individual devices are unlikely to impact the business as a whole. Further, there is a robust model testing and evaluation process in place for continuous monitoring.	Zurich NA	30-Sep-24

Artificial Intelligence Management System (AI/ML)	4.5 Has the algorithm/system been tested for fairness and absence of bias using data appropriate to the market and regulatory environment in which the solution will be deployed? (Single selection allowed) (Justification allowed) (Justification required) *	Yes Netradyne primarily tracks bias in source data by testing the outputs of the AI model during model development and training and then adding more data and/or reviewing data quality for any issues that are surfaced. After deployment, Netradyne has a model evaluation and retraining process in place to improve model performance over time. A formal bias study for drowsiness detection model did not reveal statistically significant differences across different demographic groups. Periodic bias studies are planned for high-risk AI systems to detect/monitor potential bias in model outputs to ensure that precision metrics are fair with respect to identifiable groups that may be small relative to the overall population of data subjects.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	4.6 Do you have a model monitoring plan? (Single selection allowed) (Justification allowed) (Justification required) *	Yes Netradyne conducts regular monitoring of key KPIs/metrics (alert rate, precision, false-positive rate) against set target thresholds. KPIs include ongoing tests to gauge if sensitive attributes, such as race or gender, might be implicit factors to the model outputs.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	5.1 What guardrails are in place to prevent adversarial attacks? *	Since most of the models are deployed on the edge, circumstaces within the vehicles may be a source of adversarial attack. Some adversarial techniques such as physical obstructions, camouflage or intentional distractions intended to introduce perturbations in the model input data can be well detected and tolerated by Netradyne's models. The models have been trained with with enough context data for dealing with certain kinds of adversarial attacks. Further, the model outputs may be audited by a human-in-the-loop for quality control purposes.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	5.2 Can a user opt-out of tracking and/or receiving recommendation? (Single selection allowed) (Justification allowed) (Justification required) *	No Certain alerts can be suppressed for a fleet, but the same cannot be done at individual driver level. Drivers may opt out of allowing their data for ML training purposes as described in resonse to 2.7.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	5.3 Has your solution undergone any external AI audit/assessment? (Single selection allowed) (Justification allowed) (Justification required) *	No Netradyne has a roadmap planned for its AI Governance program that includes audit readiness to achieve compliance with AI related industry standards and applicable regulations.	Zurich NA	30-Sep-24
Artificial Intelligence Management System (AI/ML)	5.4 Do you have an Ethical/Responsible AI policy? (Single selection allowed) (Justification allowed) (Justification required) *	Yes The ResponsibleAI policy draft is under review internally and has not yet been approved for publication. Draft policy may be shown virually over a call, subject to a prior non-disclosure agreement (NDA).	Zurich NA	30-Sep-24
Application & Interface Security	Please provide a general overview of what your add-in does.	Netradyne has multiple add-ins, individually enabled in Geotab and in Netradyne. 1. Driver Assignment. Netradyne pulls drive time for each vehicle from the Driver Change API every 15 minutes to import into Netradyne. This is used to assign drivers to vehicles for the duration they are driving. 2. Maps page add in. Alerts from the past 24 hours are presented as an add-in inline on the Geotab map. A right-hand menu is available to show summary information about all alerts, which also functions as a filter, and also allows users to view a help article about the add-ins. The alerts show as green icons on the map. When selected, they allow users to view the video that is present for that alert. 3. Trips page add in. Similarly to the Maps page add in, the alerts are visibile for a selected trip. This goes back as far as our alerts are present in our system, typically 4 months. 4. Netradyne iframe + SSO. A Netradyne left-hand menu page is available for users to open the Netradyne application within Geotab. SSO is simulated by having the user login once, then persists the open session with the Geotab session.	GeoTab EU & UK	1-Oct-24

Product Security	**Netradyne offerings (Product + IDMS Platform) shall be free from any kind of malware &**	Netradyne security controls are managed and governed by Netradyne ISMS policies and guidelines and it also aligned with NIST and CIS Critical Security controls requirements related to Data Protection/privacy, Identity & Access, DevSecOps, Vigilance, Resilience, Network & Infrastructure Security, Risk and Compliance Management. We have stringent levels of protection to secure our product(s) and underlying infrastructure. Let’s understand the Product architecture at high level and how it is being used from the customer side to use the service offerings (read, analyze, copy or download the recorded data/reports/inference or events) what all interfaces & Security design/operation aspects are there and what way it is made available to respective customers:Netradyne adopt industry best security practices and is certified with ISO 27001:2022 and 27701:2019 recognitions. The same can be shared under NDA (snippets are attached above). Our solution is a SaaS offering which is hosted on secure, highly available & scalable AWS Infrastructure. User Interface is accessible through browser and mobile application (Supported on Android & iOS) using Https REST APIs, which is the front end of Multi-Tier architecture, DBs are at back end and only accessible though Netradyne internal web API services to fetch the data for the requests.	GeoTab EU & UK	27-Nov-24
Product Security	**Downloading or copying any data from IDMS/device shall not introduce any malware into the customer network/system**	Same as above	GeoTab EU & UK	27-Nov-24
Product Security	**Netradyne offering shall not contain any triggering factor which can make it unavailable or inoperable after a certain period of time or usage**	Netradyne does not deploy such tactics and practices. Netradyne is very fair and transparent in its service commitment and SLAs and its security posture supports the SLA requirements. Netradyne understands the critical nature of information security requirements and are committed to maintain the highest standards. We appreciate customer diligence in reviewing our security posture, and we look forward to addressing any concerns or additional requirements they may have. Our goal is to establish a partnership built on trust and confidence.	GeoTab EU & UK	27-Nov-24



Product Architecture (High Level)

InfoSec/ISMS Take on Network Architecture

Security Design Aspects

- Infrastructure
- Platform
- Application(s) & Services
- Network Interfaces
- Data
- Access
- Users

Security Operation Aspects

- Security Configuration
- Backup & Restore
- Business Continuity & Disaster
- Recovery
- Change Management
- Security Incident Mgmt.
- Vulnerability & Patch Mgmt.
- Third Party Management
- Compliance Management

Netradyne Confidential 2024 Netradyne Confidential 2024 17