A-LIGN

OnSolve, LLC

Type 2 SOC 3

2022

ONSOLVE™

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2022 to December 31, 2022

Table of Contents

SECTION 1

ASSERTION OF ONSOLVE, LLC MANAGEMENT

ASSERTION OF ONSOLVE, LLC MANAGEMENT

January 19,2023

We are responsible for designing, implementing, operating, and maintaining effective controls within OnSolve, LLC's ('OnSolve' or 'the Company') OnSolve and MIR3 Platform Services System throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that OnSolve's service commitments and system requirements relevant to Security and Availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "OnSolve, LLC's Description of Its OnSolve and MIR3 Platform Services System throughout the period January 1, 2022 to December 31, 2022" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that OnSolve's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). OnSolve's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "OnSolve, LLC's Description of Its OnSolve and MIR3 Platform Services System throughout the period January 1, 2022 to December 31, 2022".

OnSolve uses Amazon Web Services ('AWS') for cloud hosting services and Equinix and Flexential to provide colocation services (collectively, 'the subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OnSolve, to achieve OnSolve's service commitments and system requirements based on the applicable trust services criteria. The description presents OnSolve's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OnSolve's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve OnSolve's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of OnSolve's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2022 to December 31, 2022 to provide reasonable assurance that OnSolve's service commitments and system requirements were achieved based on the applicable trust services criteria.

John Herbst
Chief Legal Officer
OnSolve, LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To OnSolve, LLC:

Scope

We have examined OnSolve, LLC's ('OnSolve' or 'the Company') accompanying description of OnSolve and MIR3 Platform Services System titled "OnSolve, LLC's Description of Its OnSolve and MIR3 Platform Services System throughout the period January 1, 2022 to December 31, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that OnSolve's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

OnSolve uses AWS for cloud hosting services and Equinix and Flexential to provide colocation services (collectively, 'the subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OnSolve, to achieve OnSolve's service commitments and system requirements based on the applicable trust services criteria. The description presents OnSolve's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OnSolve's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OnSolve, to achieve OnSolve's service commitments and system requirements based on the applicable trust services criteria. The description presents OnSolve's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of OnSolve's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

OnSolve is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that OnSolve's service commitments and system requirements were achieved. OnSolve has provided the accompanying assertion titled "Assertion of OnSolve, LLC Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. OnSolve is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within OnSolve's OnSolve and MIR3 Platform Services System were suitably designed and operating effectively throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that OnSolve's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on OnSolve's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of OnSolve, user entities of OnSolve's OnSolve and MIR3 Platform Services during some or all of the period January 1, 2022 to December 31, 2022, business partners of OnSolve subject to risks arising from interactions with the OnSolve and MIR3 Platform Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
January 19, 2023

SECTION 3

ONSOLVE, LLC'S DESCRIPTION OF ITS ONSOLVE AND MIR3 PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2022 TO DECEMBER 31, 2022

OVERVIEW OF OPERATIONS

Company Background

OnSolve is a global provider of software-as-a-service (SaaS)-based critical communication solutions for enterprise, small and midsize business (SMB), and government customers. The OnSolve and MIR3 Platform for Critical Event Management (CEM) is a cloud-based software communications platform that provides seamless and easy-to-deploy solutions for the exchange of critical information among organizations, their people, devices, and external entities with use cases designed to save lives, enhance revenue and reduce costs. More information can be found on the Company's website at www.OnSolve.com.

Description of Services Provided

The OnSolve and MIR3 Platform are flexible and reliable mass notification and business continuity solutions. The solutions allow organizations to send important mass notifications or alerts to any number of people, at once, allowing for immediate, individual responses with an automatic audit trail. The OnSolve and MIR3 Platform allow for text-based and voice messages to be sent to cell phones, home phones, work phones, satellite phones, e-mail, pagers, fax machines, and more. Additionally, both solutions allow for two-way communication in messages. This allows for the dynamic flow of information in the event of an emergency or important event.

OnSolve and MIR3 Platform are comprised of systems and infrastructure needed to allow organizations to communicate with a large group of individuals quickly and efficiently. When used in crisis response, the system allows for organizations to pinpoint and respond to threats that impact their people, places, and property - quickly, accurately, and reliably.

OnSolve and MIR3 Platform:

- Leverages AI-Powered Risk Intelligence - Filters through massive amounts of data sources to detect and assess critical events and speed up crisis reporting and response times. Customers can see, understand, and escalate relevant information and filter out the noise of irrelevant data
- Drives Seamless Critical Communications - Ensure employee safety and business continuity, swift disaster recovery and more through reliable communication. Maintain contact data seamlessly by integrating with existing business systems to streamline processes
- Delivers Adaptable Incident Management - Turn static emergency response plans into interactive mobile guides for rapid collaboration between customers and individuals. Real-time monitoring and reporting allow you to respond and hone procedures on the fly as the recovery unfolds

The core of the OnSolve and MIR3 Platform is a SaaS solution hosted in the AWS US East/West cloud environment.

Principal Service Commitments and System Requirements

OnSolve designs its processes and procedures related to the OnSolve and MIR3 Platform to meet its objectives for its emergency notification services. Those objectives are based on the service commitments that OnSolve makes to user entities, the laws and regulations that govern the provision of emergency notification services, and the financial, operational, and compliance requirements that OnSolve has established for the services. The emergency notification services of OnSolve are subject to the security and privacy relevant standards and regulations, including international and U. S. state privacy security laws and regulations in the jurisdictions in which OnSolve operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) within each customer's agreement. Security commitments are standardized and include, but are not limited to, the following:

- Security concepts within the OnSolve and MIR3 Platform are fundamentally designed to permit authorized access and visibility to data and system resources and ensure the data is protected from unauthorized changes
- Availability principles within the OnSolve and MIR3 Platform are fundamentally designed to permit authorized users' access to the system resources when they need access while preventing unauthorized users from accessing the system or interfering with authorized users from accessing the systems

OnSolve establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in OnSolve's system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the OnSolve and MIR3 Platform.

Components of the System

Infrastructure

The primary infrastructure used to support the OnSolve and MIR3 Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Function and Purpose**
Packer Ubuntu 18.04 Server	Ubuntu 18.04	Application hosting

Software

The primary software used to provide the OnSolve and MIR3 Platform Services System includes the following:

Primary Software		
Software	**Operating System**	**Function and Purpose**
MongoDB Database	Ubuntu 18.04	Data storage and Management
Redis Database		
Cassandra Database		
MySQL Database		
Kubernetes Worker / Control Plane		Container management
Kubernetes Orchestration		
Kubernetes Worker / Control Plane		
Ansible Orchestration		Container deployment
accountexpiration-app		Micro service Application

Primary Software		
Software	**Operating System**	**Function and Purpose**
announcementservice-app	Kubernetes-Hosted Container	
auditlogservice-app		
cascades-app		
cassandra-identityconfigurational-migration		
contactfileparserservice-app		
customfieldservice-app		
weathernotificationgateway-api		
eventsentry-app		
developerportal-app		
feedsservice-app		
filestorageservice-app		
franconia-app		
identityservice-identityuserserver		
katmai-eventprocessor		
tahoe-app		
yosemite-app		
denaliapi-app		
Microsoft Active Directory (AD)	Windows	Directory service for Windows domain networks

People

The Company's organization provides for the segregation of responsibilities into the following areas:

Executive Management

OnSolve's Executive Management team provides strategic support for the overall organization including ensuring resources for the effective development, operations, and support of the products. Executive Management is directly responsible for the relationship with OnSolve's leadership and private equity partner.

Human Resources

OnSolve's Human Resources Department is responsible for day-to-day employment issues for the Company including employee benefits for the organization. The HR department manages the employee lifecycle from candidates for employment, through the background check process, and employment status processes such as annual reviews, job changes, and disciplinary actions until termination of employment. HR also ensures that the Company's policies, including those contained in the Company Handbook, are being met and that the Company complies with human resources and employment-related laws and regulations.

Finance

The Finance Department is responsible for maintaining the Company's financial records per applicable accounting policies, laws, rules, and regulations. The Finance Department runs the monthly, quarterly, and annual financial reporting processes for the organization. The Finance Department is responsible for ensuring that OnSolve's finance and control functions result in the preparation and disclosure of financial data that fairly presents OnSolve's financial position, results of operations, and cash flows by generally accepted accounting principles.

Legal

The Legal Department is responsible for managing the legal affairs of the Company, which covers areas such as contract and supplier negotiations, legal and regulatory compliance, privacy compliance, intellectual property work, litigation matters, and corporate governance. The Legal department also helps coordinate activities with OnSolve's Board of Directors and related compliance and governance activities.

The Security and Compliance team is responsible for establishing and maintaining administrative processes, policies, and procedures for OnSolve. This includes the processes, policies, and procedures that apply to the application and infrastructure. The Security and Compliance team assists in ensuring that procedures used by teams are in harmony with data security and data privacy policies. The team manages security-specific tools and oversees security features of the operational tools in support of the environment. The Security and Compliance team also manages data privacy, disaster recovery, and business continuity activities and conducts the Risk Assessments associated with the Risk Management process, policies, and procedures.

Marketing

The Marketing Department manages marketing communications for the Company globally through its branding, advertising, public relations, web, and online presence, educational initiatives, events, relationship marketing, and internal communications functions. Marketing also assists the Sales group in developing and executing marketing strategies to enhance global brand awareness and the sales and lead pipelines.

Sales, Account Management and Customer Care

This Department is responsible for presenting appropriate information to potential new customers and ensuring current customers receive appropriate information to satisfy their due diligence requirements, as well as day-to-day customer support. Customers are assigned an Account Manager with the objectives to engage regularly with the customer to ensure a high level of satisfaction, proactively pursue customer renewals, seed new business ideas, collaborate to solve business problems, and upsell new applications. Customers are also assigned a Customer Relationship Manager with technical objectives to ensure high degrees of success with the implementation of the application, training within the product, and support services to ensure the most effective use of the product. The Account Manager and Customer Relationship Manager roles coordinate with customers to manage any complaints customers may have about the product, or about OnSolve resources.

Internal Processes

This Department manages the tools and resources used by OnSolve employees. These include the various ticket tracking tools such as Service Now and Jira, as well as customer relationship management tools such as NetSuite and Salesforce.

Technology

The Technology Department includes corporate technology and production operations; including product management, application engineering, and Database Operations.

Corporation Information Technology (CorpIT) is responsible for the day-to-day functioning of OnSolve employees' workstations and the servers or cloud services that support the organization. These include information repositories such as SharePoint and Confluence as well as e-mail communications in Office 365.

The Production Operations team (ProdOps) is responsible for the servers that support the OnSolve and MIR3 Platform to ensure it is available and in line with customer SLAs. This team includes the Network Operations Center (NOC), System Engineers, and Site Reliability Engineers (SRE) as well as the DevOps roles, which are responsible for deploying the applications after successfully passing Quality Control. This team has access to the servers that support the application and databases but does not have direct access to the databases, or the data within them.

Product Management is responsible for the strategic direction of the products developed by OnSolve. This team works closely with customers to understand features that are desirable and works to ensure the applications are developed with the end user in mind.

Application Engineering is responsible for creating the applications and services at the heart of the OnSolve and MIR3 Platform, through in-house coding to ensure the feature functionality of the application. The team also performs Quality Control testing and presents deployable packages to DevOps to deploy into production.

The Database Operations team is responsible for the databases. This team ensures the availability and efficient functioning of the databases and has access to data.

Data

OnSolve acts only as the data processor for customer data. OnSolve has a responsibility to ensure customer data is managed, processed, and stored following the relevant data protection regulations, and security standards and with specific requirements formally established in customer agreements. Customer data is provided to OnSolve from each customer, and that data is utilized by OnSolve in delivering OnSolve and MIR3 Platform. Customers have full control over the data they share, and each customer data set is unique. Customers are responsible for loading data into the OnSolve and MIR3 Platform and the Platform makes no changes to the data other than checking for integrity for purposes of ingestion. The OnSolve and MIR3 Platform require such data necessary to contact an individual and deliver the customers' alert message to each recipient. System-generated data includes system usage reports.

Processes, Policies and Procedures

OnSolve has implemented formal corporate policies relevant to both administrative and operational controls. Control policies are formalized in process, policy, and procedure documents. These documents are updated annually, and appropriate personnel is notified of the update and the location of the document for their reference. Each document has a classification marking that describes the sensitivity of the information in the document including the acceptable audience for the document. Each process, policy, and procedure have unique sections concerning the document topic, and documents have common sections that cover the purpose, scope, and statement of commitment, as well as exception and exemption options. The teams are expected to adhere to the OnSolve process, policies, and procedures and the document describes disciplinary actions that will occur for failures to follow control policies.

Physical Security

The OnSolve and MIR3 Platform are hosted by AWS, Equinix, and Flexential. They are responsible for the physical security controls for OnSolve and MIR3 Platform Services as part of their cloud hosting or colocation services.

Logical Access

Logical access controls are utilized to restrict access to OnSolve's network at the operating system, application, and database levels. OnSolve employees are given access to the corporate domain only.

Access to the domains that support the OnSolve and MIR3 Platform is restricted to members of the Production Operations and Database teams. The OnSolve and MIR3 Platform are composed of various systems that allow the processing of customers' on-demand alerts and responses. Customers use the OnSolve Platform Customer Web Portal for uploading and managing their data. A limited number of OnSolve employees in the Customer Relationship Management team have access to the OnSolve and MIR3 Platform using the Support Web Portal.

External points of connectivity are protected by a firewall. Firewall hardening standards are based on relevant applicable technical specifications and these are compared against product and industry-recommended practices and updated. External access to nonpublic systems is restricted through the use of user authentication and message encryption systems using a Virtual Private Network (VPN) and multi-factor authentication.

Standards exist for infrastructure and software hardening and configuration that include requirements for the implementation of access control software. Standardized AWS Security Groups define which privileges are available to each user or system account. The principle of least privilege is utilized throughout the platform.

Computer Operations - Backups

To ensure production data is available for restoration in the event of a normal production system failure or disaster, a backup and archiving schedule for Production data has been implemented. In addition, formal policies and procedures have been established to cover the OnSolve and MIR3 Platform data backup and recovery procedures.

For internal file servers, the Corporate IT team performs daily backups of the key systems. Data restores are performed on those key systems on a staggered basis in line with OnSolve and MIR3 Platform Operating Procedures.

OnSolve and MIR3 Platform Databases are backed up via real-time replication between the AWS East and West availability zones.

AWS Telemetry provides the Production Operations teams with detailed reports on successful and failed jobs, missed files, status, and run times if any. Backups are captured electronically, and no physical media is created or retained for these processes. In addition, access to administer the backup schedules is restricted to authorized members of the Production Operations and Database teams only.

Computer Operations - Availability

OnSolve uses AWS Availability zones for its Production Operations to ensure the ability to resume operations at a redundant site in the event of the loss of the primary site.

Infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.

Availability zones are geographically disbursed currently in the United States.

AWS is responsible for managing its environmental controls and OnSolve reviews the effectiveness of these controls via its third-party and contractual management process. The environmental protection systems in place include:

- Cooling systems

- Battery and fuel generator backup in the event of power failure
- Redundant communications lines
- Smoke detectors
- Fire protection system such as a dry pipe sprinkler
- At least annual maintenance and regular testing on these systems

Should any of these systems fail, and cause an outage in the OnSolve environment, a member of the The Third-Party Data Center Operations team will alert the OnSolve NOC team. The NOC team is available on a 24x7 basis. The NOC team follows a playbook with appropriate instructions including escalation to the appropriate Production Operations team.

Incident Response and Event Monitoring

Incident response procedures exist for each of the areas to ensure issues are identified, reported, and responded to effectively and timely. The incident response plan includes steps for categorizing incidents, containment of incidents, incident eradication, incident recovery, and incident follow-up.

OnSolve monitors environments for events that could lead to security events. Security logs are managed and sent to a central repository where they are correlated and reviewed for issues. Defined alerts are sent to the NOC, who follows a playbook and escalates to Security Engineering as needed. Security events are formally reviewed by the System Engineering team every week.

Risks Assessment procedures are in place to assure that management is aware of possible impacts on the environment. These risk items are a focal point for monitoring events.

Change Control

OnSolve has implemented a change management process that includes managing changes to the OnSolve Platform, MIR3, and any systems or software that support the applications as well as to any Corporate environments.

The patch management process is performed to ensure that both the corporate environments and the production environment are maintained to the standards recommended by each vendor. Patching of systems is performed following the manufacturer's patch release schedules such as Microsoft's Patch Tuesday.

Patches and other changes are reviewed, implemented in the testing environment, and approved before being deployed in each environment.

Changes to the application are presented through the ticketing systems and may be requested from multiple sources including customer enhancement requests, defects identified from various testing sources, and feature functionality changes identified by Product Management. Additionally, Security Testing and scanning will identify security changes that are necessary for the systems.

Each of these changes is incorporated into the System Development Life Cycle. A more formalized and automated Continuous Integration and Continuous Delivery (CI/CD) strategy is in the process of being rolled into the change processes.

Security Testing and Scanning included in the SDLC include Static Application Vulnerability Testing (SAST), Composite Analysis (CA), Dynamic Application Vulnerability Testing (DAST), and Manual Pen Testing. Internal Vulnerability Testing is also performed on the operating system, network, and application layer. Finding from these tests are recorded in the ticket tracking tools and managed through the standard change management processes.

Changes flow through the Quality Control process and are approved before being provided to the DevOps team for deployment into the production environments.

Separate environments are used for development, testing, and production. Only approved personnel can perform changes in each of the environments.

Data Communications

Data transmitted over a public network is encrypted using advanced encryption standards. IPSec VPNs are used between sites for inter-site transmissions. Network traffic is managed with layers of firewalls which are also configured with intrusion protection system (IPS) and intrusion detection system (IDS) functionality. Microsoft Windows-based systems have antivirus software installed and are scanned regularly. Systems are monitored for various activities and logs are correlated and stored in a Security Incident and Event Management tool.

Access to the system is controlled and restricted to defined users based on their job duties. Approval for access must be approved through the Chief Technology Officer (CTO).

Boundaries of the System

The scope of this report includes the OnSolve and MIR3 Platform Services System performed at the Ormond Beach, Florida; Dayton, Ohio; and Alpharetta, Georgia facilities.

This report does not include the cloud hosting services by AWS or the colocation services provided by Equinix and Flexential at multiple US facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common / Security and Availability criterion were applicable to the OnSolve and MIR3 Platform Services System.

Subservice Organizations

AWS provides cloud hosting services and Equinix and Flexential provide colocation services. AWS, Equinix, and Flexential are responsible for the physical and environmental security of the facilities.

Subservice Description of Services

AWS provides cloud hosting services and Equinix and Flexential provide co-location services.

Complementary Subservice Organization Controls

OnSolve's services are designed with the assumption that certain controls will be implemented by the subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to OnSolve's services to be solely achieved by OnSolve control procedures. Accordingly, the subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of OnSolve.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4, CC7.2	Physical access to facilities housing the production servers is the responsibility of the third-party data center, AWS.
		Recovery Key materials used for disaster recovery processes by Key Management Service (KMS) are physically secured offline so that no single AWS employee can gain access to the key material.
		Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
		Physical access to the data center is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor being deactivated.
		Physical access to the data center is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to the server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to the server locations are managed by electronic access control device.
		Electronic intrusion detection system are installed within data server locations to monitor, detect and automatically alert personnel of security incident.
Availability	A1.2	Amazon-owned data centers are protected by fire and detection suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and system monitor and control air temperature and humidity at appropriate levels.
		Uninterruptable power supply units provide backup power in the event of an electrical failure in Amazon owned data center.
		Amazon owned data centers have generators to provide backup power in case of electrical failure.
		Contractors are in place with the third-party location service providers which include provisions to provide fire suppression systems, air conditioning, to maintain appropriate atmospheric conditions, uninterruptable power supply, and redundant power supplies.

The following subservice organization controls have been implemented by Equinix and included in this report to provide additional assurance that the trust services criteria are met:

Subservice Organization - Equinix		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4, CC7.2	Physical access control systems are in place to restrict access to and within the corporate facility and data center housing the facilities, backup media, and other system components such as firewall, routers, and servers to properly authorized individuals.
		Procedures exist and are followed to established and make changes to physical access privileges for customers.
		Security personnel review a government issued ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to the facility.
		Procedures exist and are followed to establish and make changes to physical access privileges for employees.
Availability	A1.2	Fire detection and suppression equipment is in place at each facility.
		Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly.
		Power management equipment is in place for each facility.
		Scheduled maintenance procedures are performed to test and confirm the operation of the power management systems.
		Air conditioning and ventilation equipment is in place at each facility to ensure that humidity levels and the required temperature are maintained.
		Scheduled maintenance procedures are performed to ensure that the Heating, Ventination, and Air Conditioning (HVAC) equipment and temperature and water detection sensors are working properly.
		Internal and external monitoring of environmental systems activity is performed through the use of Building Management Systems (BMS) and 24x7 monitoring by facility engineers.
		Emergency procedures are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

The following subservice organization controls have been implemented by Flexential and included in this report to provide additional assurance that the trust services criteria are met:

Subservice Organization - Flexential		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4, CC7.2	Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access: • Access card and PIN at building entrances • Access card and biometric scan at data center entrances
		Visitors are required to sign-in with onsite security personnel prior to entering the data centers.
		Data center visitors are required to be accompanied and supervised by an authorized Flexential employee or client escort.
		Visitors are required to wear a visitor badge while visiting the data centers.
		Client equipment is maintained in lockable cages or racks within the data centers.
		There are no exterior facing windows in the walls of the areas where client production servers are located.
		Documented security procedures are in place to govern vendor access to the data centers, and include, but are not limited to, the following: • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging
		Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.
		The Director of Compliance reviews user account access of terminated employees on a quarterly basis.
		A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.
Availability	A1.2	Documented policies and procedures are in place to govern environmental security practices and responses to certain environmental security events.
		The data centers are protected by the following fire detection and suppression controls: • Audible and visual fire alarms • Pre-action dry-pipe water sprinklers and/or agent-based fire suppression system • Fire and smoke detectors • Hand-held fire extinguishers

Subservice Organization - Flexential		
Category	**Criteria**	**Control**
		Management obtains inspection reports to ensure that third-party specialists inspect the fire detection and suppression systems on an annual basis.
		The data centers are equipped with multiple air conditioning units to regulate temperature and humidity.
		Management obtains inspection reports to ensure that third-party specialists inspect the air conditioning units on a quarterly basis.
		The data centers are equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak.
		The data centers are connected to multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage.
		Management obtains inspection reports and/or invoices to ensure that third-party specialists inspect the UPS systems on a quarterly basis.
		The data centers are equipped with fueled electric power generators to provide backup power in the event of a power outage.
		Management contracts with third-party specialists to inspect the fueled electric power generators on a quarterly basis and the inspection report is retained as evidence of completion.
		Management obtains inspection reports to ensure that generators are load tested on a quarterly basis.
		Environmental monitoring systems are utilized to monitor the environmental systems and conditions within the data centers including, but not limited to, the following: • Fire alarm status and suppression systems • Temperature • Humidity and air quality • Power levels and availability
		The environmental monitoring application is configured to notify operations personnel via on-screen and/or e-mail alert notifications if certain predefined thresholds are exceeded on monitored systems.
		For subscribing customers, disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

COMPLEMENTARY USER ENTITY CONTROLS

OnSolve's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to OnSolve's services to be solely achieved by OnSolve control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of OnSolve.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to OnSolve.
2. User entities are responsible for notifying OnSolve of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of OnSolve services by their personnel.
5. User entities are responsible for developing disaster recovery and business continuity plans that address the inability to access or utilize OnSolve services.
6. User entities are responsible for providing OnSolve with a list to notify for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying OnSolve of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.