OnSolve, LLC

MIR3-Send Word Now (SWN) System Services

Type 2 SOC 3

2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2020 To December 31, 2020

Table of Contents

SECTION 1

ASSERTION OF ONSOLVE, LLC MANAGEMENT

ASSERTION OF ONSOLVE, LLC MANAGEMENT

February 26, 2021

We are responsible for designing, implementing, operating, and maintaining effective controls within OnSolve, LLC's ('OnSolve' or 'the Company') MIR3 and Send Word Now (SWN) Application and Infrastructure Services System throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that OnSolve's service commitments and system requirements relevant to Security and Availability were achieved. Our description of the boundaries of the system is presented below in "OnSolve, LLC's Description of Its MIR3 and Send Word Now (SWN) Application and Infrastructure Services System throughout the period January 1, 2020 to December 31, 2020" 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, 2020 to December 31, 2020, 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, Confidentiality, Processing Integrity 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 MIR3 and Send Word Now (SWN) Application and Infrastructure Services System throughout the period January 1, 2020 to December 31, 2020".

OnSolve uses Equinix, Inc. ('Equinix'), Digital Realty Trust, Inc ('DRT'), and Flexential Corp. ('Flexential') to provide data center hosting 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, 2020 to December 31, 2020 to provide reasonable assurance that OnSolve's service commitments and system requirements were achieved based on the applicable trust services criteria.

Cheryl Carmel
VP Security & Compliance
OnSolve, LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: OnSolve, LLC

Scope

We have examined OnSolve's accompanying description of its MIR3 and Send Word Now (SWN) Application and Infrastructure Services System titled "OnSolve, LLC's Description of Its MIR3 and Send Word Now (SWN) Application and Infrastructure Services System throughout the period January 1, 2020 to December 31, 2020" (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, 2020 to December 31, 2020, 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 Equinix, DRT, and Flexential to provide data center hosting services. 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.

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 MIR3 and Send Word Now (SWN) Application and Infrastructure Services System were suitably designed and operating effectively throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that OnSolve, LLC'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 MIR3 and Send Word Now (SWN) Application and Infrastructure Services System during some or all of the period January 1, 2020 to December 31, 2020, business partners of OnSolve subject to risks arising from interactions with the MIR3 and Send Word Now (SWN) Application and Infrastructure Services System, 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
February 26, 2021

SECTION 3

ONSOLVE, LLC'S DESCRIPTION OF ITS MIR3 AND SEND WORD NOW (SWN) APPLICATION AND INFRASTRUCTURE SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2020 TO DECEMBER 31, 2020

OVERVIEW OF OPERATIONS

Company Background

OnSolve, LLC is a global provider of SaaS-based critical communication solutions for enterprise, small and midsize business (SMB), and government customers. The company's cloud-based software communications platform 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

OnSolve has two main applications that are used for the MIR3 and Send Word Now Application and Infrastructure Services:

SWN

SWN's Alert Notification Services, Incident Management Services, and other related services that are part of the system enable organizations to quickly, securely, and reliably distribute critical information to large numbers of people on virtually any device and on virtually any network. In the event of an emergency or other time-sensitive event, text-based and voice messages (using text-to-speech technology) are simultaneously delivered to individuals via cell phone, home phone, work phone, satellite phone, e-mail, pager, BlackBerry PIN, and more.

MIR3

MIR3 is a mass notification and business continuity solution. The MIR3 solution allows for organizations to send important mass notifications or alerts to any number of people, at once, allow for immediate, individual responses with an automatic audit trail. Similar to SWN, MIR3 allows for text-based and voice messages to be sent to cell phone, home phones, work phones, satellite phones, e-mail, pagers, BlackBerry PINS, and more. Additionally, the MIR3 solution allows for two-way communication in messages. This allows for the dynamic flow of information in the event of an emergency or important event.

Principal Service Commitments and System Requirements

OnSolve designs its processes and procedures related to MIR3 and SWN 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 as 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 customers agreement. Security commitments are standardized and include, but are not limited to, the following:

- Security concepts within MIR3 and SWN 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 MIR3 and SWN 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 authorized users form 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 MIR3 and SWN systems. Summaries of OnSolve policies and procedures are provided to customers in the MIR3 or SWN Specific Hosted Services Security Measures document.

Components of the System

Infrastructure

Primary infrastructure used to support OnSolve's MIR3 and SWN Application and Infrastructure Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Function and Purpose**
MIR3		
Watchguard	Firewall	Firewall to filter in/outbound IP traffic in Production network
BigIP F5	Load Balancer	Load Balancer to distribute web requests to redundant backend servers for various services and applications
HP Proliant	Servers	Server hardware for web, and database
SuperMicro	Servers	Server hardware for web, and database
Cisco Catalyst	Switch	Switch to connect physical devices to Production Network
Network	Windows Active Directory	Network
Production Server	Linux CentOS	Operating System
Production Server	Linux RedHat	Operating System
Production Server	Linux Ubuntu	Operating System
Production Server	Oracle	Database Management System

Primary Infrastructure		
Hardware	**Type**	**Function and Purpose**
SWN		
BigIP F5	Load Balancer	Load Balancer to distribute web requests to redundant backend servers for various services and applications
HP Proliant	Servers	Server hardware for web, and database
Dell PowerEdge	Servers	Server hardware for web, and database
Sansay	VOIP Session Boarder Controllers (SBC)	VOIP Session Boarder Controllers (SBC) used for routing SIP and Media to/from downstream carriers
Production Server	Microsoft Server 2012 R2	Operating System
Production Database	Microsoft SQL Server 2012 Enterprise	Database Management System

Software

Primary software used to provide OnSolve's MIR3 and SWN Application and Infrastructure Services System includes the following:

Primary Software		
Software	**Operating System**	**Function and Purpose**
MIR3 Application	Linux	Primary alert notification system/software
SWN Application	Linux and Windows	Primary alert notification system/software
PRTG	SaaS	Network Monitor
VMware ESXI	Hypervisor	Virtualization software
Solarwinds	SaaS	Network Monitor
SOPHOS	SaaS	Antivirus

Security Software	
Tripwire Log Center	Log Correlation and Security Event and Incident Management
Tenable.io	Internal vulnerability management
SOPHOS	Antivirus, web filtering
Rapid7 Insight AppSec	Dynamic Application Security Testing
Veracode, Sourceclear	Static Application Security Testing, Composite Analysis
Portswigger BurpSuite	Internal Penetration Testing
KnowBe4	Security Awareness, Training and Education and Phishing exercises
MetaNetworks	VPN

People

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

Executive Management

OnSolve's Executive Management team provide 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 Board of Director 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 employments, through the background check process, employment status processes such as annual reviews, job change 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 all human resources and employment related laws and regulations.

Finance

The Finance Department is responsible for maintaining the Company's financial records in accordance with applicable accounting policies, laws, rules, and regulations. The Finance Department runs the monthly, quarterly, and annual financial reporting process for the organization. The Finance Department is responsible for ensuring that OnSolve's finance and control functions result in preparation and disclosure of financial data that fairly present OnSolve's financial position, results of operations, and cash flows in accordance with 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 all activities with OnSolve's Board of Directors and related compliance and governance activities.

The Security and Compliance team is responsible for establishing and maintaining all administrative process, policies, and procedures for OnSolve. This includes the processes, policies and procedures that apply to the application and infrastructure. The Security and Privacy team assists in the ensuring that procedures used by all 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. Security and Privacy team also manages the 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 to ensure 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 objectives to engage regularly with the customer to ensure high level of satisfaction, proactively pursue customer renewals, and 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 implementation of the application, training within the product and all support services to ensure most effective use of the product. The Account Manager and Customer Relationship Manager roles coordinate with customers to manage any complaints customers may have within 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; includes product management, application engineering and Database Operations. OnSolve's Security and Privacy department is also part of the Technology Department.

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.

Production Operations team is responsible for the servers that support MIR3 and SWN application being available at all times. This team includes the Network Operations Center (NOC), System Engineers and Site Reliability Engineers (SRE) as well as the DevOps role, which is responsible for deploying the applications after successfully passing Quality Control. This team has access to the servers that support the application and databases, but do not have direct access to the databases.

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 to create the application through coding and acquisition of code to ensure the feature functionality of the application. The team also performs Quality Control testing and presents installable packages to DevOps to deploy into production.

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

Data

OnSolve is the data processor for customer data. They hold the responsibility to ensure customer data is managed, processed, and stored in accordance with the relevant data protection regulations, 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 its MIR3 and SWN Application and Infrastructure Services System. Customers have full control over the data they share, and each customers' data set are unique. The system requires 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 are 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 all documents have common sections that cover the purpose, scope and statement of commitment, as well as exception and exemption options. All teams are expected to adhere to OnSolve process, policies and procedures and the document describes disciplinary actions that will occur for failures to follow control policies.

Physical Security

The MIR3 and SWN application and supporting infrastructure is hosted by Equinix, DRT and Flexential. They are responsible for the physical security controls for the MIR3 and SWN application as part of their data center hosting services.

Logical Access

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

Access to the domains that support MIR3 or SWN production systems is restricted to members of the Production Operations and Database teams. The MIR3 and SWN platform is composed of various systems that allow processing of customers' on-demand alerts and responses. Customers and internal users do not actually log in to the MIR3 and SWN platform. Customers use the service via the MIR3 and SWN Customer Web Portal. A limited number of OnSolve employees in the Customer Relationship Management team have access to the MIR3 or SWN system 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 periodically. 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 implementation of access control software. Standardized access control lists define which privileges are available to each user or system account. Principle of least privilege is utilized throughout the platforms.

Computer Operations - Backups

To ensure corporate data and production data is available for restoration in the event of a normal production system failure or disaster, a backup and archiving schedule for vital applications and data has been implemented. In addition, formal policies and procedures have been established to cover the Company's 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 annually.

For customer production servers, the Production Operations team performs backups for MIR3 and SWN in their respected environments.

MIR3 Oracle database is backup is completed in the primary environment, encrypted and transferred to the secondary site where the backup is mounted to ensure full functionality of the database. In addition, MIR3 data is replicated in real-time to a tertiary site.

SWN's SQL database is log shipped of data to network-attached storage (NAS) devices located in the primary co-location facilities on a five-minute delay. A daily full backup of the database is sent to NAS devices located at the SWN backups secondary site. In addition, SWN performs real-time replication of production SQL server databases to disaster recovery SQL databases located at the SWN secondary site. The SQL database replication is monitored by the database administrator (DBA) group on a real-time basis.

Backups and archiving are performed utilizing native and third-party backup utilities that provide the Corporate IT and Production Operations teams with detailed reports on successful and failed jobs, missed files, status, and run times. The backup status detailed reports are reviewed by the Corporate IT and Production Operations teams on a real-time basis and exceptions are addressed in a timely manner. All 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 a multi-location strategy for its Production Operations to ensure the ability to resume operations at a redundant site in the event of loss of the primary site.

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

Multiple Third-Party Data Centers are contracted for co-location facilities to house OnSolve contracted cage areas. These data centers are geographically disbursed throughout the United States as well as internationally.

Each Third-Party Data Center is responsible to manage their environmental controls and OnSolve reviews the effectiveness of these control in the annual third-party due diligence processes. The environmental protection systems in place include the following:

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

Should any of these systems fail, and cause an outage in the OnSolve environment, a member of the Third-Party Data Center Operations team will alert the OnSolve Network Operations Center (NOC) team. The NOC team is available on a 24x7 basis. 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 incident, 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 on a weekly basis.

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

Change Control

OnSolve has implemented a change management process that include managing changes to the MIR3 and SWN applications 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 all systems is performed following manufacturer's patch release schedules such as Microsoft's Patch Tuesday.

Patches and other changes are reviewed, implemented in the testing environment, and approved prior to 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 request, defects identified from various testing sources, 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 are 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.

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

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

Data Communications

All data transmitted over 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. All Microsoft Windows-based systems have antivirus software installed and are scanned regularly. Systems are monitored for various activity and logs are correlated and stored in a Security Incident and Event Management tool.

All access to the system is controlled and restricted to defined users based upon their job duties. Approval for access must be approved through the CTO.

Boundaries of the System

The scope of this report includes the MIR3 and SWN Application and Infrastructure Services System performed in the Albany, New York; Boston, Massachusetts; Ormond Beach, Florida; and San Diego, California facilities.

This report does not include the data center hosting services by Equinix, DRT and Flexential at the multiple location facilities.

Changes to the System in the Last 12 Months

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

Criteria Not Applicable to the System

All Common and Availability criteria were applicable to the OnSolve MIR3 and SWN Application and Infrastructure Services System.

Subservice Organizations

Subservice Description of Services

Equinix, DRT and Flexential provide data center hosting services.

Complementary Subservice Organization Controls

OnSolve's services are designed with the assumption that certain controls will be implemented by 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, 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 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**	**Applicable Controls**
Common Criteria/Security	CC6.4	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 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 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 DRT and included in this report to provide additional assurance that the trust services criteria are met:

Subservice Organization - DRT		
Category	**Criteria**	**Applicable Controls**
Common Criteria/Security	CC6.4	Physical access controls are in place to restrict access to and within the data center facilities.
		Physical access requests are documented and require the approval of the site manager.

Subservice Organization - DRT		
Category	**Criteria**	**Applicable Controls**
		A review of Digital Reality employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, notified, and removed.
		A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Reality employee and contractor terminations within one business day of termination.
		Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day.
		Surveillance cameras are in place to monitor and record access to and within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
		Digital surveillance systems are configured to retain video footage for the data centers for a minimum of 90 days.
Availability	A1.2	BMS applications are configured to monitor environmental systems and physical access systems and alert IT personnel when predefined thresholds have been met.
		The data centers are equipped with the following environmental protection equipment: • Fire detection and • suppression equipment • UPS systems • Generators • CRAC/CRAH units
		Management retains the inspection report received from third-party specialists evidencing completion of inspection and maintenance of the following according to a predefined schedule: • Fire detection and • suppression equipment • UPS systems • Generators • CRAC/CRAH units
		Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring.

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**	**Applicable Controls**
Common Criteria/Security	CC6.4	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**	**Applicable Controls**
		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's.

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 own 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 their own 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.