Dynamic Signal, Inc.
Type 2 SOC 3
2021

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 16, 2020 to July 15, 2021

Table of Contents

SECTION 1

ASSERTION OF DYNAMIC SIGNAL, INC. MANAGEMENT

ASSERTION OF DYNAMIC SIGNAL, INC. MANAGEMENT

August 12, 2021

We are responsible for designing, implementing, operating, and maintaining effective controls within Dynamic Signal, Inc.'s ('Dynamic Signal' or 'the Company') Employee Communication and Engagement Platform Services System throughout the period July 16, 2020 to July 15, 2021, to provide reasonable assurance that Dynamic Signal's service commitments and system requirements relevant to Criteria, Availability and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Dynamic Signal, Inc.'s Description of Its Employee Communication and Engagement Platform Services System throughout the period July 16, 2020 to July 15, 2021" 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 July 16, 2020 to July 15, 2021, to provide reasonable assurance that Dynamic Signal's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (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*). Dynamic Signal'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 "Dynamic Signal, Inc.'s Description of Its Employee Communication and Engagement Platform Services System throughout the period July 16, 2020 to July 15, 2021".

Dynamic Signal uses EdgeConneX and Interxion to provide colocation and managed hosting/IaaS services (collectively, 'subservice organizations'). The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Dynamic Signal, to achieve Dynamic Signal's service commitments and system requirements based on the applicable trust services criteria. The description presents Dynamic Signal's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Dynamic Signal'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 Dynamic Signal'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 Dynamic Signal'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 July 16, 2020 to July 15, 2021 to provide reasonable assurance that Dynamic Signal's service commitments and system requirements were achieved based on the applicable trust services criteria.

James Peterson
Director of Information Security
Dynamic Signal, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Dynamic Signal, Inc.:

Scope

We have examined Dynamic Signal, Inc.'s accompanying description of Employee Communication and Engagement Platform Services System titled "Dynamic Signal, Inc.'s Description of Its Employee Communication and Engagement Platform Services System throughout the period July 16, 2020 to July 15, 2021" (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 July 16, 2020 to July 15, 2021, to provide reasonable assurance that Dynamic Signal's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (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*).

Dynamic Signal uses EdgeConneX and Interxion to provide colocation and managed hosting/IaaS services. The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Dynamic Signal, to achieve Dynamic Signal's service commitments and system requirements based on the applicable trust services criteria. The description presents Dynamic Signal's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Dynamic Signal'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 organizations controls.

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

Dynamic Signal 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 Dynamic Signal's service commitments and system requirements were achieved. Dynamic Signal has provided the accompanying assertion titled "Assertion of Dynamic Signal, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Dynamic Signal 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 Dynamic Signal's Employee Communication and Engagement Platform Services System were suitably designed and operating effectively throughout the period July 16, 2020 to July 15, 2021, to provide reasonable assurance that Dynamic Signal'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 Dynamic Signal'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 Dynamic Signal, user entities of Dynamic Signal's Employee Communication and Engagement Platform Services during some or all of the period July 16, 2020 to July 15, 2021, business partners of Dynamic Signal subject to risks arising from interactions with the Employee Communication and Engagement Platform Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organizations 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
August 12, 2021

SECTION 3

DYNAMIC SIGNAL, INC.'S DESCRIPTION OF ITS EMPLOYEE COMMUNICATION AND ENGAGEMENT PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 16, 2020 TO JULY 15, 2021

OVERVIEW OF OPERATIONS

Company Background

Founded in November 2010 by Russ Fradin, Steve Heyman and Jim Larrison, Dynamic Signal is an Employee Communication and Engagement Platform, headquartered in Silicon Valley, with offices in London, New York, Chicago, and Seattle.

Focused on providing the market's most comprehensive and scalable Employee Communication and Engagement platform, Dynamic Signal's technology allows organizations to drive improvement in critical business metrics such as decreased attrition, improved employee experience, lower total cost of ownership, increased earned media value, and increased productivity.

These solutions are delivered via a value creation life cycle services model, designed to ensure excellence in strategic planning, execution, deployment, and customer satisfaction.

Dynamic Signal is the Official Salesforce.com Partner for Social, a Top 20 Preferred Microsoft Collaboration Partner, and an approved offering for Cisco. The company's platform also integrates with existing enterprise systems such as Microsoft's SharePoint and Active Directory, Adobe Marketing Suite, Workday, Oracle HCM, Salesforce, Slack, Yammer and more.

An industry agnostic technology platform, Dynamic Signal serves almost every vertical including Financial Services, Healthcare, Manufacturing, Business Services, Telecommunications, Advertising, Retail, Educational institutions, and Government agencies.

Used by more than 300 enterprise customers, across 100 countries, in 14 languages, Dynamic Signal's mission is to modernize how companies engage and connect with their employees by communicating with them the way they prefer.

Description of Services Provided

Dynamic Signal is a SaaS platform that facilitates companies communicate with their employees. Dynamic Signal is a communication platform that provides service such as:

- Workforce Communication
- Employee Advocacy
- Mobile Intranet

Dynamic Signal platform delivers content to their customer's distributed workforce by using these core capabilities:

- Content Personalization:
    - Reduce communication noise for employees by delivering relevant content based on job function, location, department, or any other custom attribute. Give employees the option to subscribe to specific areas of interest. Auto-subscribe employees to important content categories. Engage global workforce by communicating in their preferred languages
- Broadcasting:
    - Distribute information across any device and communication channel. Broadcast content via native app, e-mail, push notifications, SMS, intranets, and collaboration tools like Slack, Yammer and Chatter. Request acknowledgments to confirm that urgent messages are received. Quickly re-broadcast to employees who missed the original message
- Social Sharing:
    - Provide company-approved stories and news that employees can easily post to their social media networks such as Facebook, Twitter, and LinkedIn. Control the message with suggested share text, hashtags, @mentions, and disclosures. Extend the reach of marketing campaigns while helping employees build their own brands

- Reporting:
    - Measure and analyze with real-time metrics. Complete visibility into adoption rates, participation, content views, reads, shares, clicks, social reactions, impressions, reach, and more. Monitor program performance with simple-to-use dashboards and graphical reports. Easily export data for further analysis
- Video:
    - Record in-app videos or upload content to show rather than tell. Deliver executive announcements, important news, and employee recognition that are authentic, resonate, and get the attention of busy employees
- Newsletters:
    - Create custom newsletters designed for mobile viewers. Highlight existing content and important company information that's tailored for every employee. Use the drag-and-drop editor to build and rearrange mobile-friendly layouts. No HTML experience required
- Survey:
    - Create and distribute mobile-friendly surveys or online polls to targeted groups. Design surveys combining different types of questions including multiple choice, ranking, rating, Net-Promoter Score, and open response. Make surveys or polls known or anonymous. Easily review results with graphical displays. Export responses for more analysis
- Permissions:
    - Set unique manager permissions and privileges to support the needs of large, complex organizations. Robust permission options ensure program managers have the proper access and control for their roles
- Messaging:
    - Seamlessly integrate with existing business tools and systems. Meet clients' unique needs with APIs that integrate with intranets, collaboration tools, and systems of records. Create and manage member profiles. Source content and employee information. Broadcast to third-party channels. All at enterprise scale

Principal Service Commitments and System Requirements

Dynamic Signal designed and built their principal services to meet Customer Success and delivery objectives.

Those objectives are based on the service commitments that Dynamic Signal makes to customers, the laws and regulations that govern the provision services, and the financial, operational, and compliance requirements that Dynamic Signal has established for the services:

- Onboarding Customers - The Customer Success Team is dedicated to supporting and partnering with their customers to help their programs achieve success. During the implementation phase, the relevant teams will undergo a comprehensive training from a dedicated Customer Success Team. learn the ins-and-outs of the platform, develop an efficient workflow for managing content, have any opportunity to ask the right questions and gain insight on useful ways of tracking program success over time
- Customer Support- In addition to dedicated resources, customers also have access to dedicated 24/7 Support through e-mail and a self-service 'Knowledge Base' with many best practices, recommendations, and customer examples
- Security commitments - Dynamic Signal's security commitments are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security principles within the platform designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role

Components of the System

Infrastructure

Primary infrastructure used to provide Dynamic Signal's Employee Communication and Engagement Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Supermicro	Server	Servers to run databases, services, websites, etc.
Cisco	Network Switch	Network switch
Juniper	Firewall	Restrict access to and from the systems
PaloAlto	Firewall	Restrict access to and from the systems

Software

Primary software used to provide Dynamic Signal's Employee Communication and Engagement Platform Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
PostgreSQL	Centos	Database server
Redis	Centos	Cache server
RabbitMq	Centos	Queue server
Docker	Centos	Host containers/microservices
Nginx	Centos	Proxy/secure sockets layer (SSL) termination
Windows	Windows	Host IIS sites and custom services

People

Dynamic Signal consist of the personnel involved in the governance, operation, and use of the system:

- Engineering - Responsible for the development, testing, deployment, and maintenance of new code for Dynamic Signal production applications. Engineering consists of multiple global teams with specific assignments including Quality Assurance, Product Development, and Sustaining
- Technical Operations - Responsible for making hardware, network, and server configuration changes within the Dynamic Signal Production Network. Additionally, responsible for granting logical access to the systems within the Dynamic Signal Production Network, performing quarterly reviews of access to those systems, and revoking logical access rights upon user termination. Operations manages the Denial-of-Service (DDOS) protections, and is responsible for overall system availability, including system redundancy, system logging and monitoring, backup and recovery, and capacity planning. Operations works closely with Security to patch discovered system vulnerabilities. Operations consists of multiple teams with specific assignments including System Operations, Cloud Operations, Infra Operations, Core Operations, Shared Services Operations, Data Operations, Network Operations, Data Center Operations, Database Management, and DevOps

- Information Technology (IT) - Responsible for managing corporate computing devices (laptops/endpoints), business applications, supporting toolsets, and employee and contractor identities. IT grants access to SaaS applications and to systems within the corporate network, and manages this access using Single sign-on (SSO), Active Directory (AD), People Operations (HR) management and Virtual Private
- Networking virtual private network (VPN) technologies and terminates access when applicable
- Information Security - Responsible for security governance, security monitoring, vulnerability scanning, network and application layer penetration testing, security awareness, incident response, security architecture, and compliance oversight
- HR - Responsible for onboarding new personnel, defining the role/position of new hires, performing background checks, and facilitating the employee termination process
- Facilities - Responsible for managing physical security and granting physical access to Dynamic Signal corporate offices
- Customer Support - Responsible for managing customer interactions via e-mail, chat, social media and over the phone. The team files and resolves customer inquiries and issues regarding Dynamic Signal plans, training, and other technical issues related to the software. Customer Support is responsible to communicate information to customers regarding new issues and/or developments, changes in processing schedules, system enhancements, new product features and updates, security incidents, and other relevant information
- Legal - Responsible for setting contractual obligations with third parties and technology partners/suppliers, including negotiation and drafting of legal terms and conditions, ensuring compliance with internal contractual standards and review of information security and privacy issues
- Product Management - Responsible for building features and products for customers and defining the product roadmap. Actively communicating the changes to external and internal stakeholders such as customers and employees
- Sales - The sales department is composed of specialized and experienced sales personnel. It is responsible for selling and optimizing sales to Dynamic Signal's customers
- Business Development- The business development department is responsible for identifying, building and managing partnerships with third-party entities
- Marketing - The marketing department is responsible for building the company's image, generating sales opportunities, and other marketing activities

Data

Data, as defined by Dynamic Signal, constitutes of the following:

- Transaction Data
- Files
- Tables
- Data Output
- Reports (Analytics)
- System Logs

Data is stored in Production environment and is loaded into the environment and accessed remotely from customer systems via the Internet. Dynamic Signal classifies this data as Service Data.

Customer data is managed, processed, and stored in accordance with the guideline described in this document.

Dynamic Signal's platform enables customers to upload and store data such as, text, video, images, PDF, MS Office files and more. The data is stored and associated to customer's community.

Content accessibility is governed by customer configuration and classification. In some configurations, data may be publicly accessible in w/o requiring authentication (depends on the service and configurations).

Requests can originate from different client endpoints and will be handled by Dynamic Signal's Application Programming Interface (API), which governs the authentication process, content delivery and more. As the communication to the API is stateless, it is not required to retain the session information or status for the duration of multiple requests.

Dynamic Signal Stores user passwords in hashed format and encrypts using crypt or pbkdf2. All data stored is encrypted at rest, including database and backup data.

Dynamic Signal stores additional application and system logs to provide monitoring and analytic information on the systems functionality, errors and capacity. Dynamic Signal SaaS service is a multi-tenant solution, and additional measures are taking to guarantee the data security for their customers. Logical separation of tenets / communities is maintained and enforced.

Processes, Policies and Procedures

Processes include the automated and manual procedures involved in the operation of the Platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to Operations, Security, Engineering, IT, etc., as detailed later in this System Description. These procedures are drafted in alignment with the overall Information Security Policies and are updated and approved as necessary for changes in the business, but no less than annually.

Physical Security

The in-scope systems are hosted by EdgeConneX and Interxion; therefore, EdgeConneX and Interxion are responsible for physical security.

Logical Access

Dynamic Signal uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Dynamic Signal implements monitoring of one or more of the responsibilities.

Monitoring is performed by Technical Operations Team that is responsible for performing the conflicting activities or by the Dev/InfoSec team.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees personnel sign on to the Dynamic Signal network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory and when applicable, a two factor (2FA) systems is utilized. Passwords must conform to the NIST 800-63b, section 5 standards and are enforced through parameter settings in the Active Directory.

These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Dynamic Signal network are required to use a two-factor authentication system with a secure VPN connection. Employees are issued access upon employment and access is revoked during their exit interview. Vendor personnel are not permitted to access the system from outside the Dynamic Signal network.

The Dynamic Signal application is available via the public Internet. Customers are provided with a unique logon user ID and password to access the application. Communications between a browser and the Dynamic Signal's application are encrypted via transport layer security (TLS) and secure socket layer (SSL) with support for forward secrecy. Customers have the option to integrate with their own or third-party identity and access management infrastructure using security assertion markup language (SAML) or may leverage the application itself to provide direct web-based authentication. Customers may access only their own data. The data for each customer resides in a database specific to that customer.

On an annual basis, access rules for each role are reviewed by a working group composed of the security review team. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO/ CTO. As part of this process, the CISO/ CTO reviews access by privileged roles and requests modifications based on this review.

On any position or responsibility change, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review and indicate the required changes in the event management record. The record is routed back to the HR team for processing and follow up with a ticket with the Information Security team.

In order to assist in the prevention of unauthorized access to data, user accounts within the Dynamic Signal production environment and supporting tools, access is disabled promptly upon termination of employment. Terminated employees complete a termination clearance process on their last day at Dynamic Signal while the termination notification is documented and accessible within the Internal IT management ticket system. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data and equipment.

Computer Operations - Backups

Dynamic Signal Technical Operations Team is responsible for scheduling, monitoring, and resolving backup- related issues. Dynamic Signal receives daily reports from the backup system, confirming that the data was backed up successfully. Database servers are backed up by a local File Backup server with a 60-day retention and Amazon Web Services S3 cloud file storage. All databases are backed up nightly.

If an issue were identified and a backup did not run successfully, the Technical Operations Team would acknowledge the failure and take corrective action. Ongoing readability of backup and retained data is tested annually through restoration or other methods by the Dynamic Signal's technical Operations Team. Evidence of a successful restoration is retained.

Public Cloud Restoration

The public cloud service vendor will be formally activated if the Disaster Recovery Lead determines that the primary facility is no longer sufficiently functional or operational to sustain normal business operations. Once this determination is made, the Disaster Management/IT Team will be commissioned to bring the cloud platform to functional status, after which the Disaster Recover Team will meet to assess the following next steps:

1. Determination of impacted systems.
2. Critical ranking of impacted systems.
3. Recovery measures required for high critical systems.
4. Assignment of responsibilities for high critical systems.
5. Schedule for recovery of high critical systems.
6. Recovery measures required for medium critical systems.
7. Assignment of responsibilities for medium critical systems.
8. Schedule for recovery of medium critical systems.
9. Recovery measures for low critical systems.

10. Assignment of responsibilities for recovery of low critical systems.
11. Schedule for recovery of low critical systems.
12. Determination of other tasks, outstanding and required.
13. Determination of further actions to be taken.

Restoring Platform Functionality

Dynamic Signal has a detailed plan of action to restore platform functionality in the event of a disaster. Unless otherwise specified, the IT Team is responsible for restoring platform systems. The following table describes and ranks the platform systems to be recovered:

Rank	System	System Component (In Order of Importance)
1	Database	CentOs 6.x/ 7.x Postgres 9.3 (x86_64)
2	Cache	CentOs 6.x / 7.x Redis 2.6x
3	Queue	CentOs 6.x / 7.x RabbitMQ 3.3x w/Erlang R16Bxx
3	Web Servers	Windows 2016
4	Services	Windows 2016
4	Proxy	Nginx w/OpenSSL

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents.

Dynamic Signal monitors the system capacity, reliability, availability, application performance, response time, error rate, throughput, and running services of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Dynamic Signal evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

Ongoing monitoring and reporting of the technical infrastructure and service systems provides continual real-time feedback to Dynamic Signal Technical Operations Team. Using third-party and in-house monitoring tools, Dynamic Signal is able to proactively monitor and maintain the delivery infrastructure for their application service to clients. In addition, Dynamic Signal performs regular audits of their operations to obtain reasonable assurance with compliance with their operational policies.

The in-scope systems are hosted by EdgeConneX and Interxion; therefore, EdgeConneX and Interxion are responsible for environmental security.

Change Control

Dynamic Signal maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes.

Formal change-management policies and procedures outline the process for making changes to the Dynamic Signal application and databases. The Quality Assurance team initiates patches and bug fix releases via a ticket within the change management system. Requests have to be approved by the supervisor or the manager of the initiator. In certain exceptional cases, approval may be performed at the peer level.

New features are developed and then tested within the test environment. No production data is allowed in the test environment, so specifically generated dummy test data is utilized for these purposes. Test plans are utilized, where applicable, to guide testing procedures. Application regression testing validates key application inputs, processing, and output for the application during the change management process. Associated plans, scripts, and results are retained in the Dynamic Signal internal change management system. Minimum acceptance testing criteria documentation is:

- Acceptance Testing Actions Performed - describe what testing activities were executed in order to prove that new functionality performs as specified or that a change resolves identified problem
- Acceptance Testing Results - document success or failure for each testing action
- Acceptance Tester Name - Formal final approval is made for test results and migration to production prior to migration to production. Approvals may be submitted via e-mail/Slack or recorded within the change tracking system. Access to move changes into production is restricted to the Technical Operations Team. Changes with possible customer impact are performed during published maintenance windows. Implementation is performed in a manner that allows the original environment to be restored, if necessary. Major releases are preceded with a customer e-mail notification that indicates the scheduled system unavailability and provides details of the release. This notice is followed up with a release confirmation and more detailed release resources once the new version is live
- Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers

Operating System - CentOS 6.x / 7.x FreeBSD, Windows Server 2016. The Technical Operations Team is responsible for the application of patches to system software and operating systems. As additional layers of defense, Dynamic Signal employs preventative firewall security, intrusion detection/prevention and penetration testing. Dynamic Signal contracts with qualified third parties to perform Web/ Mobile penetration testing and web application testing at least once a year. Patch application follows the same procedure as application and database development and maintenance. User Acceptance Testing, for operating system changes, is performed.

Emergency Changes

Emergency changes follow the formal change management policy, except for the following:

The emergency change is to resolve an immediate system wide issue that impacts the systems availability or stability. An emergency change request will be documented in the change management system and will include an authorized appropriate approval from the CTO/ VP of Engineering or another authorized approver. The approval will take place within three business days following migration of the emergency change into production.

Quality Assurance testing of the emergency change is made within a reasonable time frame following migration of the emergency change into production. For emergency changes, the following quality Assurance acceptance test components will be retained in the internal wiki or within the change tracking system:

- Test actions indicating what activities was taken to ensure that the emergency change functioned as desired
- Results of the test action pass or fail
- Testers - name of the persons performing testing activities

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

When applicable, redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a manual penetration test, simulating all permission levels available in the system to simulate an insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes Web and Mobile application layers testing.

Vulnerability scanning is performed internally on a quarterly basis in accordance with Dynamic Signal's policy. The team uses industry standard scanning technologies and a formal methodology specified by the Information Security Team. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the production system are implemented through the Change Management process.

Network Device Implementation and Maintenance

The Technical Operations Team is responsible for network changes to network devices such as routers, switches, and firewalls including security configuration changes, and is also responsible for creating and maintaining security groups (act like a firewall). Changes performed in production are peer-reviewed by the Hosting Operations Team for correctness prior to implementation and subsequently tested upon release. Changes with possible customer impact are performed during published maintenance windows. Implementation is performed in a manner that allows the original environment to be restored, if necessary.

Boundaries of the System

The scope of this report includes the Employee Communication and Engagement Platform Services System performed in the Santa Clara, California facilities.

This report does not include the colocation and managed hosting and infrastructure as a service (IaaS) provided by EdgeConneX at the Santa Clara, California, Tempe, Arizona facilities; and the colocation and managed hosting/IaaS provided by Interxion at the Dublin, Ireland and the Amsterdam, Netherlands 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, Availability, and Confidentiality criterion were applicable to the Dynamic Signal's Employee Communication and Engagement Platform Services System.

Subservice organizations

This report does not include the colocation and managed hosting/IaaS provided by EdgeConneX at the Santa Clara, California, Tempe, Arizona facilities; and the colocation and managed hosting/IaaS provided by Interxion at the Dublin, Ireland and the Amsterdam, Netherlands facilities.

Subservice Description of Services

EdgeConneX is used to provide colocation and managed hosting/IaaS for the Dynamic Signal platform. Interxion is used to provide European colocation and managed hosting/IaaS.

Complementary Subservice organizations Controls

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

The following subservice organizations controls should be implemented by EdgeConneX to provide additional assurance that the trust services criteria described within this report are met:

Subservice organizations - EdgeConneX		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	Documented physical security policies and procedures are in place to guide personnel in physical security practices.
		A Personal Identification Number (PIN) based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.
		At EdgeConneX managed facilities, a mantrap is utilized to restrict access to the facilities and prevent tailgating.
		Contractors and other third parties are issued expiring PINs based on access request submissions.
		Visitors are required to be escorted by an employee when visiting the data center facilities.
		Visitors are required to sign a log when visiting the data center facilities.
		Surveillance cameras are installed at the data center facilities and monitored by NOC personnel.
		Video surveillance footage of the EdgeConneX managed data center facilities is stored and retained.
		User access requests are documented, tracked, and approved by a direct supervisor.

Subservice organizations - EdgeConneX		
Category	**Criteria**	**Control**
		Physical access of terminated employees is revoked as a component of the termination procedures.
		Physical access reviews are performed on a monthly basis.
		Doors that bypass mantraps can only be opened by the PINs of designated personnel.
Availability	A1.2	Environmental protections are installed at the data center facilities that include the following: • HVAC • Battery and generator backup in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Dry pipe sprinklers
		Monitoring software is used to identify and evaluate ongoing environmental protections. This software sends automated messages to the operations personnel when specific predefined thresholds are met.
		Environmental protections receive maintenance on at least an annual basis.
		Disaster recovery plans, including restoration of backups, are tested at least annually.
		EdgeConneX uses a multi-location strategy for their facilities to permit the resumption of operations in the event of a disaster at a specific data center facility.

The following subservice organizations controls should be implemented by Interxion to provide additional assurance that the trust services criteria described within this report are met:

Subservice organizations - Interxion		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.

Subservice organizations - Interxion		
Category	**Criteria**	**Control**
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Environmental protections are installed at the data center facilities that include the following: • HVAC • Battery and generator backup in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Dry pipe sprinklers
		Monitoring software is used to identify and evaluate ongoing environmental protections. This software sends automated messages to the operations personnel when specific predefined thresholds are met.
		Environmental protections receive maintenance on at least an annual basis.
		Disaster recovery plans are developed and updated annually.
		The entity uses a multi-location strategy for their facilities to permit the resumption of operations in the event of a disaster at a specific data center facility.

Dynamic Signal management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Dynamic Signal performs monitoring of the subservice organizations controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Dynamic Signal'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 Dynamic Signal's services to be solely achieved by Dynamic Signal control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Dynamic Signal'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 Dynamic Signal.
2. User entities are responsible for notifying Dynamic Signal of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Dynamic Signal 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 Dynamic Signal services.
6. User entities are responsible for providing Dynamic Signal with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Dynamic Signal of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.