Élan Cloud Solution

November 2017

Last update date: 11/11/2017

Author: Ron Motley (CIO)

Table of Contents

Summary:

This document intends to provide information to assist Media Services customers with evaluating Élan Cloud services and integrating Élan Cloud solutions into their existing IT control framework.

This document also addresses Media Services-specific information around general cloud computing compliance questions.

Élan Cloud Security:

- Encryption for External Connections

  User access to the systems is via the Internet. SSL encryption technology is utilized for all Élan Cloud Service access. SSL (TLS 1.2) connections are negotiated with at least 128 bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. SSL is implemented or configurable for all web-based SSL certified programs deployed at Media Services. It is recommended that the latest available browsers certified for Élan solutions, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs. The list of certified browsers for each version of Élan solutions can be found on the Élan Support portal (www.msgl.com). In some cases, a third party tool that the Customer wishes to integrate with Élan may not accept an encrypted connection.

- Segregation in Networks

  Media Services data centers utilize an isolated network topology which is used to deliver services to Élan Cloud customers. In each “Client SDDC”, networking technologies are deployed in a layered approach designed to protect Customer data at the physical, data link, network, transport, and software level. Access controls are multi-tiered, consisting of the network, system, database, and software layers. All access is authorized on a "deny by default" base policy.

- Network Access Control

  Élan Cloud operation teams access customer environments through a segregated network connection, which is dedicated to environment access control and isolated from Media Services internal corporate network traffic. The dedicated network functions as a secure access gateway between support systems and target application and database servers. Regional VPN gateways are designed to provide continuity of support operations in the event any one of the gateways were to fail. Authentication, authorization, and accounting are implemented through standard security mechanisms designed to ensure that only approved support representatives and engineers have access to the systems. Cryptographic controls are implemented to provide Cloud operations and support with secure, easily configured access to target programs.

- Network Bandwidth and Latency

  Media services is not responsible for Customer’s network connections or for conditions or problems arising from or related to Customer’s network connections (e.g., bandwidth issues,

excessive latency, network outages), or caused by use of the Internet. Media Services monitors its own networks and will notify customers of any internal issues that may impact availability.

- Network Routing Control
    - Routers

      Router controls implemented for the Élan Cloud solution provide the connection point between Élan Cloud Services and the Internet. Border routers are deployed in a fully redundant, fault tolerant configuration. Routers are also used to enforce traffic policies at the perimeter.
    - Firewalls

      Media Services Cloud utilizes Enterprise level firewalls to control access between the Internet and Élan Cloud Solution by allowing only authorized traffic. Firewalls are deployed in a layered approach to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address to identify authorized sources, destinations, and traffic types.
- Network Security Management
    - Network Controls

      Network controls implemented for Élan Cloud Services address the protection and control of data during its transmission from Customer's site to the Élan hosted systems. The network security infrastructure is designed to secure the servers from a network-based attack. Redundant, managed firewalls, using stateful packet inspection, provide barriers between tiers of the architecture. All traffic is filtered, and only valid connections are allowed through into the network demilitarized zone. Traffic within each tier is restricted and controlled for security purposes.
    - Network Intrusion Detection/Prevention System

      Élan Cloud Services utilize Network Intrusion Detection Systems (IDS) to protect the environment. IDS sensors are deployed in either IPS (Intrusion Prevention Mode) or IDS (Intrusion Detection Mode) on the network, to monitor and block suspicious network traffic from reaching the internal network. IDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24x7x365.
    - Network Vulnerability Assessments

      The Élan Cloud Services team (NETOPS) utilizes network vulnerability assessment tools to identify security threats and vulnerabilities. Formal procedures are in place to assess, validate, prioritize, and remediate identified issues. Media Services subscribes to vulnerability notification systems to stay apprised of security incidents, advisories, and other related information. The NETOPS team takes actions on the notification of a threat or risk once confirmation that a valid risk exists, that the recommended changes are applicable to service environments, and that the changes will not otherwise adversely affect the services.

- Anti-Virus Controls

  Media Services employs enterprise-level anti-virus software/services from Trend-Micro to scan data at rest and in motion. Viruses that are detected are removed (or quarantined) automatically, and an alert is automatically generated which initiates Media Services incident response process.
- Configuration Control/Audit

  Élan Cloud solutions utilize a centralized system (SYSOPS) for managing the access and integrity of network device configurations. Change controls are in place to ensure only approved changes are applied. Regular audits are also performed to confirm compliance with security and operational procedures.

- System Hardening

  Media Services employs standardized system hardening practices across all Élan Cloud servers. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, aggressive patch management, and appropriate logging.
- Physical Security Safeguards

  Élan utilizes secure computing facilities from CORESITE communication (http://www.coresite.com) for both primary and backup cloud infrastructure locations. Common controls employed at datacenters include:
  - Physical access requires authorization and is monitored.
  - Everyone must visibly wear official identification while onsite
  - Visitors must sign a visitor's register and be escorted and/or observed when on the premises
  - Possession of keys/access cards and the ability to access the locations is monitored. NOTE: Staff leaving Media Services employment must return keys/cards immediately.

  Additional Physical Security Safeguards are in place for Élan Cloud data centers:
  - Premises are monitored by CCTV
  - Entrances are protected by physical barriers designed to prevent vehicles from unauthorized entry
  - Facilities are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management
- System Access Control & Password Management

  Access to Élan Cloud systems is controlled by restricting access to only authorized personnel. Élan enforces strong password policies on all infrastructure components and cloud management systems used to operate the Élan Cloud services. This includes requiring a minimum password length and complexity. Strong passwords or multi-factor authentication are used throughout the infrastructure to reduce the risk of intruders gaining access through exploitation of user accounts.

System access controls include two-factor system authentication (2FA), authorization, access approval, provisioning, and revocation for employees and any other Élan-defined 'users'. Media Services does not manage Customer's desktop security. Customer may configure the Élan software (Screen/Menu/Fields/Etc.) and additional built-in application security features to meet their business or compliance needs.

- Review of Access Rights

  Network and operating system accounts for Media Services employees are proactively monitored (ManageEngine ADAUDIT), and reports are periodically reviewed to ensure appropriate employee access levels. In the event of employee terminations, Media Services takes prompt actions to terminate network, telephony, and physical access for such former employees.

- Security-Related Maintenance

  Élan Engineers perform security related change management and maintenance as defined by Élan Cloud Change Management Policy. For any security patch that Media Services makes generally available for designated Élan Programs, Engineers will apply and test the security patch bundle on a staged environment of the applicable Cloud Services. Media Services will apply the security patch bundle to the production environment after successfully completing tests on the staged environment.

- Data Management / Protection
  - Data Protection

    The Élan Cloud solution utilizes several standard encryption technologies and tools to protect data while in transit or at rest. Data at rest is stored on Self-Encrypting drives, for network transmission, Media Services employs secure protocols (such as SSL) to protect data in transit over public networks. Secure protocols available in the Élan Cloud utilize "Strong" encryption algorithms.
  - Data Disposal

    Upon termination of services or at Customer's request, Media Services will delete environments or data residing therein in a manner designed to ensure that they cannot reasonably be accessed or read (unless there is a legal obligation imposed on Media Services preventing it from deleting all or part of the environment or data).
  - Secure File Transfer

    Secure file transfer functionality is built on commonly used network access storage platforms and uses secure protocols for transfer (such as SFTP or WebDAV over SSL). The functionality can be used to upload files to secure Élan repositories dedicated to each customers use; most commonly used for data import/export on the Élan Cloud hosted services, or downloading data at service integration points.
  - Security Incident Response

    Media Services evaluates and responds to incidents that create suspicion of unauthorized access to or handling of Customer data. When Media Services Security Operations (SECOPS) is informed of such incidents, and depending on the nature of the

activity, SECOPS defines escalation paths and response teams to address those incidents. SECOPS will work with customer resources, and the appropriate technical teams, as well as law enforcement where necessary to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of the customer's environment, and to establish root causes and remediation steps.

- Data Privacy

  Media Services Data Protection Agreement for Élan Cloud Services ("Data Protection Agreement"), and the Élan Cloud Solution Privacy Policy, describes Media Services treatment of customer data that resides on Élan cloud systems. The Data Protection Agreement describes Media Services and Customer's respective roles for the processing and control of Data the Customer provides to Media Services as part of the Cloud Services implementation. These documents are supplied as part of the Contract Package upon successful execution of cloud service agreement.

- Regulatory Compliance

  The Élan Cloud services are aligned with the security framework of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), specifically ISO/IEC 27002:2013 Code of Practice for Information Security Management and standards.
  The ISO security framework includes a comprehensive set of security controls that are used as a baseline for the operational and security controls utilized to manage and secure the Élan Cloud Services.

  Élan Cloud facilities internal controls are tested regularly and audited annually for compliance. These audits are based on the Statement on Standards for Attestation Engagements (SSAE) No. 16, and reporting on Controls at Service Organization ("SSAE 16") criteria.
  Facility SSAE 16 certification of compliance is available upon request.

  Elan sites are PCI compliant and undergo quarterly scans by certified ASV providers (https://www.trustwave.com/Services/Compliance-Management) - Élan software utilizes token based credit-card processing with selected gateway processors, no credit-card information is stored within the Elan software.

  Customers remain responsible for regulatory compliance in the use of any Élan Cloud Service. Customers must make Media Services aware of any technical requirements that result from additional regulatory obligations prior to contract signing.

  Customers must not import payment card or other sensitive personal information that requires specific regulatory, legal or industry data security controls without notifying Media Services in advance.

Media Services understands that some customers may have additional regulatory audit requirements, and Media Services will participate in cooperative Audit procedures as necessary at Customers expense when applicable.

Élan Cloud Systems Resiliency:

The resiliency described in this document apply only to Élan Cloud services. Each Customer is solely responsible for developing a business continuity plan to ensure continuity of its own internal operations in the event of a disaster, and for backing up and recovering any non-Élan cloud hosted applications and data.

- Élan Cloud Services High Availability Strategy

  Media Services deploys Cloud services on resilient computing infrastructure located at CORESITE Tier 4 data facilities. CORESITE production data centers have component and power redundancy with backup generators in place to help maintain availability of data center resources in the event of crisis as described below.
- Redundant Mechanical Infrastructure

  The mechanical-electrical-plumbing infrastructure design includes redundant power feeds to the data center and redundant power distribution for the data center and to the data center racks. Data center cooling components (chillers, towers, pumps and computer room air conditioning units) include redundancy. The emergency standby power includes redundant battery backup with generator fuel stored onsite and contracts in place for refueling.
- Redundant Network Infrastructure

  Network designs include redundant circuits from different carriers, firewall pairs, switch pairs, and load balancer pairs.
- Redundant Application Servers

  Customer's application environment consists of a set of virtual servers that provide services to Customers. The overall application tier functionality is distributed across multiple virtual servers.
- Redundant Storage

  All Élan Cloud services data resides in redundant storage configurations with protection from individual disk or array failures.
- Élan Cloud Services Backup Strategy

  The Media Services Cloud solution is built in a fully redundant VMware Enterprise environment on VMware ESX platforms. This infrastructure includes redundancy at the hardware, network, and data center levels. To ensure data is always available, Media Services utilizes a multi-layered image-based and file-based backup strategy that ensures backup copies of the customer's virtual environments and configurations are replicated to secondary locations.

Élan Cloud Disaster Recovery Services:

- Scope

  This Policy applies only to Customer's production environments within Élan Cloud Services. The activities described in this Policy do not apply to Customer's own disaster recovery or backup plans or activities; each Customer is responsible for archiving and recovering any non-Élan software & data.

  Disaster Recovery services are intended to provide service restoration capability in the case of a major disaster, as declared by Media Services, that leads to loss of a data center and corresponding service unavailability.

  For the purposes of this document, a "disaster" means an unplanned event or condition that causes a complete loss of access to the primary site and/or systems used to provide the Élan Cloud Services such that the Customer production environments at the primary site are not available.
- System Resilience
  - Media Services maintains a redundant and resilient infrastructure designed to maintain high levels of availability and to recover services in the event of a significant disaster or disruption. Media Services designs its cloud services using principles of redundancy and fault-tolerance with a goal of fault-tolerance of a single node hardware failure.
  - Élan Cloud Services provide an infrastructure that incorporates a comprehensive data backup strategy based on VMWare HA and FT modules and replication services.
  - The Élan Cloud solution includes redundant capabilities such as power sources, cooling systems, telecommunications services, networking, application domains, data storage, physical and virtual servers, and databases.
- Disaster Recovery
  - Media Services provides for the recovery and reconstitution of its Cloud Services to the most recent available state following a disaster.
  - Media Services has established alternate processing sites to accommodate limited operating capabilities in the event of loss of service at a primary facility.
  - Disaster recovery operations apply to the loss of infrastructure at Élan Cloud facilities.
  - Media Services reserves the right to determine when to activate the Disaster Recovery Plan.
  - During the execution of the Disaster Recovery Plan, Media Services provides regular status updates to customers.
  - Recovery Time Objectives

        - Recovery time objective (RTO) is Media Services objective for the maximum period of time between Media Services decision to activate the recovery processes, and the point at which Customer can resume production operations in the standby environment.
            - The RTO objective is 4 hours from the declaration of a disaster.
    - Recovery Point Objective
        - Recovery point objective (RPO) is Media Services objective for the maximum period of data loss measured as the time Media Services declares the disaster to the last full data replication copy.
            - The standard RPO objective is a maximum of 24 hours from the point of service loss.
            - More aggressive RPO objectives can be negotiated as part of Client specific Service Level Agreements (SLA).
        - Note: the RTO and RPO do not apply to Customers custom modifications that depend on external components or third-party software. During an active failover event, non-critical fixes and enhancement requests are not supported. Customer is solely responsible for issues arising from third party software and external components.

- Approvals and Reviews

  This document and corresponding Disaster Recovery Plans are reviewed annually. The Plans are revised during the review process to incorporate problem resolutions and process improvements.

- Disaster Recovery Plans

  The following are the objectives of Media Services Disaster Recovery Plan for Élan Cloud Services:
    - In an emergency, Media Services top priority and objective is human health and safety.
    - Maximize the effectiveness of contingency operations through the established Disaster Recovery Plan that consists of the following phases:
        - Phase 1 - DRP Launch Authorization phase - to detect service disruption or outage, determine the extent of the damage and activate the plan.
        - Phase 2 - Recovery phase - to restore temporary Cloud operations, potentially at the secondary sites.
        - Phase 3 - Restoration phase - to restore processing capabilities and resume primary operations.
    - Identify the activities, resources, and procedures to carry out processing requirements during prolonged interruptions.
    - Assign responsibilities to designated personnel and provide guidance for recovery, during prolonged periods of interruption.
    - Ensure coordination with other personnel responsible for disaster recovery planning strategies.

- Ensure coordination with external points of contact and vendors and execution of DRP plan.

Élan Cloud Service Level Objectives:

- Service Availability Provisions
  Commencing at "Go-Live" of Customer's production environment, and provided that Customer remains in compliance with the terms of the Contract (including the service-level-agreement) and meets Media Services recommended minimum technical configuration requirements for accessing and using the services from Customer's network infrastructure and Customer's user work stations as set forth in the Cloud Services Documentation, Media services works to meet the Target Service Availability Level in accordance with the terms set forth in this document.
- Target System Availability Level of Élan Cloud Services
  Media Services works to meet a Target System Availability Level of 99.9% of the production service, for the measurement period of one calendar month, commencing at Media Services activation of the production environment.
- Definition of Availability and Unplanned Downtime
  "Availability" or "Available" means Customer is able to log in and access the Legacy (Unidata) or ElanWeb (IIS) portion of the Élan Cloud Services, subject to the following provisions. "Unplanned Downtime" means any time during which the services are not Available, but does not include any time during which the services or any services component are not Available due to:
  - A failure or degradation of performance or malfunction resulting from scripts, data, applications, equipment, infrastructure, software, penetration testing, performance testing, or monitoring agents directed or provided or performed by Customer;
  - Planned outages, scheduled or announced maintenance or maintenance windows, or outages initiated by Media Services at the request or direction of Customer for maintenance, activation of configurations, backups or other purposes that require the service to be temporarily taken offline;
  - Unavailability of management, auxiliary or administration services, including administration tools, reporting services, utilities, third party software components not within the sole control of Media Services, or other services not supporting core Elan processing;
  - Outages occurring as a result of any actions or omissions taken by Media Services at the request or direction of Customer;
  - Outages resulting from Customer equipment, third party equipment or software components not within the sole control of Media Services;
  - Events resulting from an interruption or shut down of the services due to circumstances reasonably believed by Media Services to be a significant threat to the normal operation

of the services, the operating infrastructure, the facility from which the services are provided, access to, or the integrity of Customer data (e.g., a hacker or a virus attack);
    - Outages due to system administration, commands, or file transfers performed by Customer Users or representatives;
    - Outages resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and Media Services upstream vendors), and other force majeure events;
    - Inability to access the services or outages caused by Customer's conduct, including negligence or breach of Customer material obligations under the agreement, or by other circumstances outside of Media Services control;
    - Lack of availability or untimely response time of Customer to respond to incidents that require Customer participation for source identification and/or resolution, including meeting Customer responsibilities for any services;
    - Outages caused by failure of network or telecommunications equipment or lines outside of Media Services control (e.g. Customer ISP routing issues).

- Measurement of Availability

  Following the end of each calendar month of the Services Period under a Customers contract, Media Services measures the "System Availability Level" over the immediately preceding month. Media Services measures the System Availability Level by dividing the difference between the total number of minutes in the monthly measurement period and any Unplanned Downtime by the total number of minutes in the measurement period, and multiplying the result by 100 to reach a percent figure.

  Availability Monitoring

  Upon request, Media Services can provide customers with automated service-outage notifications via the proactive Cloud monitoring tools utilized by Media Services.

- Monitoring

  Media services utilize a variety of software tools to monitor;

    - The availability and performance of Customer's production services environment.
    - The operation of infrastructure and network components.

    - **Monitored Components**

      Media Services monitors all levels of the service infrastructure, and currently generates alerts for over 200 components, including but not limited to; CPU, memory, storage, database, network components, and transactions. Media Services Cloud Operations staff attends to any automated warnings and alerts associated with deviations of the environment from defined monitoring thresholds, and follows standard operating procedures to investigate and resolve underlying issues.
    - **Customer Monitoring & Testing Tools**

Due to potential adverse impact on service performance and availability, Customers may not use their own monitoring or testing tools (including automated user interfaces and web service calls to any Élan Cloud Service) too directly or indirectly seek to measure the availability, performance, or security of any program or feature of or service component within the services or environment. Media Services reserves the right to remove or disable access to any tools that violate the foregoing restrictions without any liability to Customer.

- **Automated Workloads**
  Customers may not use nor authorize the use of data scraping tools or technologies to collect data available through the Élan Cloud Service user interfaces or via web service calls without the express written permission of Media Services.

Élan Cloud Change Management:

- Change Management and Maintenance
  - Standard Maintenance
    - Media Services Engineers perform changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, performance, and currency of the Élan Cloud solution. Media Services follows formal ITIL change management procedures to provide the necessary review, testing, and approval of changes prior to application in the Élan Cloud production environment.
    - Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and Customer specific changes where required. Change Management procedures are designed to minimize service interruption during implementation of changes.
    - Media Services reserves specific maintenance periods for changes, and may require the Cloud Services to be unavailable during these maintenance periods.
    - The current standard scheduled maintenance period is Saturday night between 23:00-01:00 LA (PST) data center local time. Actual maintenance time averages approximately 15 minutes.
    - Where possible, Media Services will work to coordinate the maintenance periods with Customers business requirements.
    - The durations of the maintenance periods for planned maintenance are not included in the calculation of Unplanned Downtime minutes in the monthly measurement period for System Availability Level.
    - Media Services uses commercially reasonable efforts to minimize the impact of these reserved maintenance periods and to minimize the duration of maintenance events that cause service interruptions.
  - Emergency Maintenance

        - Media Services may periodically be required to execute emergency maintenance in order to protect the security, performance, availability, or stability of the production environment. Emergency maintenance may include application patching and/or core system maintenance as required. Media Services works to minimize the use of emergency maintenance and will provide as much notice as reasonable under the circumstances as to any emergency maintenance requiring a service interruption.
    - Major Maintenance Changes
        - To help ensure continuous stability, availability, security and performance of the Cloud Services, Media Services reserves the right to perform major changes to its hardware infrastructure, operating software, applications software and supporting application software under its control, no more than twice per calendar year. Each such change event is considered scheduled maintenance and may cause the Cloud Services to be unavailable for up to 4 hours. Each such change event is targeted to occur at the same time as scheduled maintenance period. Media Services will work to provide up to 30 days prior notice of the anticipated unavailability.
- Software Versioning
    - Software Upgrades and Updates
        - Media Services requires all Cloud Services customers to keep the Élan software current with the versions that Media Services designates as currently available (CA).
        - For Cloud Services that support multiple versions, Media Services typically designates the current and immediate previous 2 version as CA.
        - Media Services may specify automatic update schedules for release of specific Élan Software patches. Software patches will follow the release of every CA version, and are required to maintain version currency.
        - Élan Cloud Hosting and delivery policies are dependent on Customers maintaining version currency.
        - Media Services is not responsible for performance or security issues encountered with the Cloud Solution that may result from running End-of-Life (EOL) versions.
    - End of Life

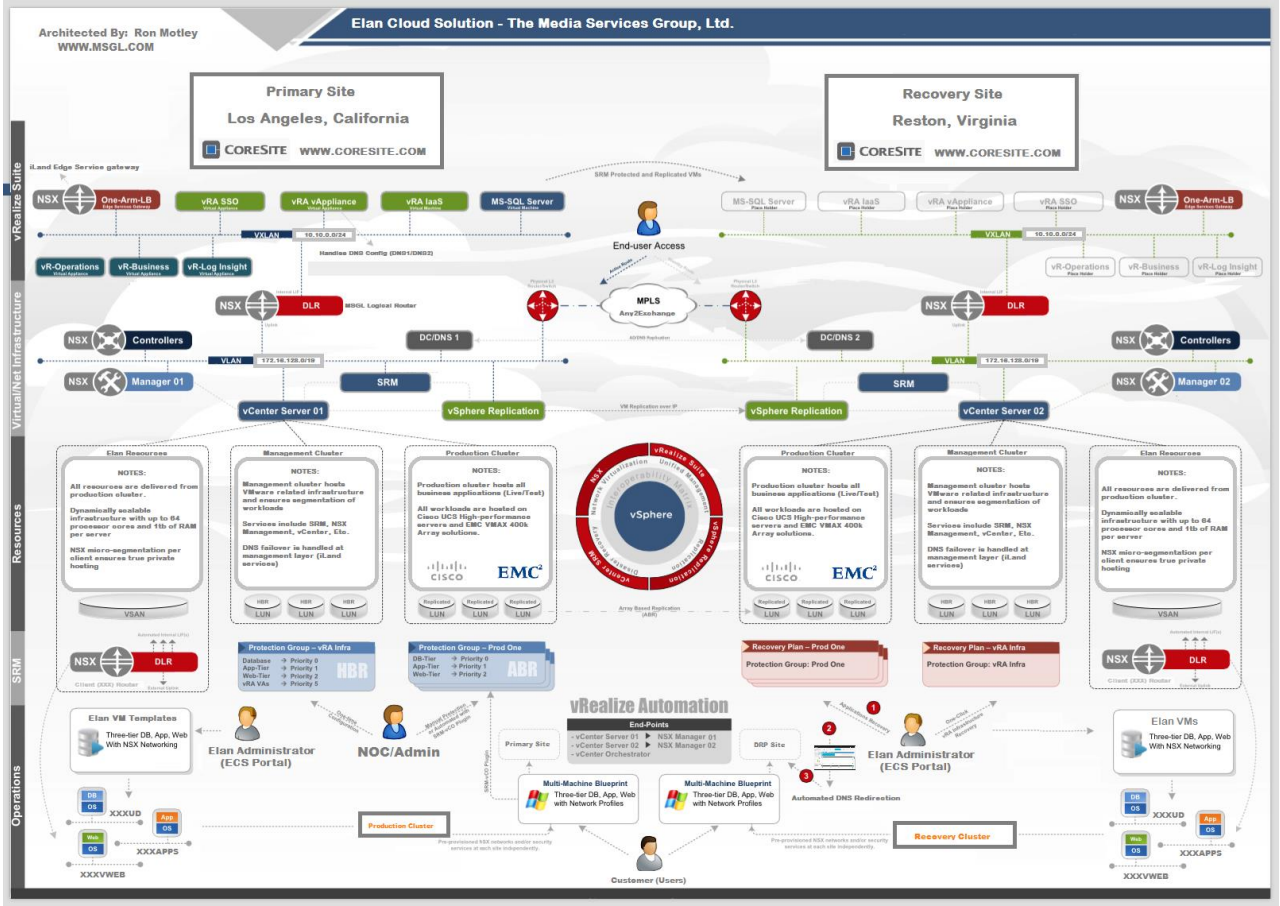
      Media Services recognizes that customers may have legitimate business reasons for not upgrading to the latest version of the software as soon as it becomes available. However, Media Services will not support older versions beyond the End of Life Policy described as follows:
        - Media Services will support only the designated CA versions of the Élan software, and 1 previous version. All other versions of the software are considered as “end of life” (EOL).

- Media Services does not provide Cloud hosting for EOL versions. Customers are required to complete the upgrade to the latest version before the EOL of a given version.
- Failure to complete the upgrade prior to the EOL of a specific version may result in an automatic upgrade.
-

Deprecated Features

A deprecated feature is a feature that appears in prior or existing versions of the Élan software and is still supported as part of the Cloud Solution, but for which Media Services has given notification that the feature will be removed from future versions. Media Services makes commercially reasonable efforts to post notices of feature deprecations 180 days in advance of their removal and reserves the right to deprecate, modify, or remove features from any new version.

Architecture Diagram



Starting from the top of the diagram, the following are the key components:

Datacenters:

This layer shows the redundant Datacenter environment currently implemented by Media Services, the primary (protected) site is in Los Angeles, and the default secondary (recovery) site is located in Reston VA.

Clients can explore site features/capabilities using the following link (http://www.coresite.com/).

VMWare vRealize Infrastructure:

This is the Coresite supplied vRealize layer that is controlled from the Management Cluster. This layer includes the various front-end appliances, ECS SSO, Coresite IaaS components, etc.

All management servers on VXLAN are accessed via secure NSX switch (Élan Edge).

Virtual Components & Network Infrastructure:

This layer of the architecture provides all management components of the infrastructure, including vCenter, SRM, NSX, etc.

All components at this layer are dedicated to each Datacenter independently – no VMWare controls are failed-over – they are pre-allocated and always available in each Datacenter.

Infrastructure Resources:

In this layer, we detail the vSphere clusters;

- Management Cluster
  The management cluster is pre-allocated and controlled by Coresite NOC and runs all VMWare related infrastructure services for Media Services.
- Production Cluster
  The production cluster is dedicated to Élan workloads and is utilized for all business applications.
  NOTE: All client specific traffic is segmented using VMWare NSX virtual routers to ensure true private hosting.

Site Recovery Manager (SRM):

Layer showing the SRM construct in terms of the key Protection Groups and Recovery plans and their association with the Élan operations layer beneath.

Élan Operations:

This layer details the various operations from resource provisioning all the way to the SRM admin recovery process.

Élan Helpdesk/Coresite NOC monitors all applications, services and servers through the vRealize operations tools.