Limelight Networks, Inc.

System and Organization Controls (SOC) 3

Report on Limelight Networks, Inc.'s Content Delivery Network System Relevant to Security and Privacy

Throughout the Period
May 1, 2021 to September 30, 2021

Limelight NETWORKS

Contents

I. Indpependent Service Auditor’s Report

Tel: 612-367-3000
Fax: 612-367-3001
www.bdo.com

800 Nicollet Mall, Suite 600
Minneapolis, MN 55402

Independent Service Auditor's Report

To the Management of
Limelight Networks, Inc.
Scottsdale, Arizona

Scope

We have examined Limelight Networks, Inc.'s (Limelight or service organization) accompanying assertion titled Assertion of Limelight Networks, Inc. Management (assertion) that the controls within Limelight's Content Delivery Network system (the system) were effective throughout the period May 1, 2021 to September 30, 2021 to provide reasonable assurance that Limelight's service commitments and system requirements were achieved based on the trust services criteria relevant to security and privacy (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).

Limelight uses subservice organizations to provide datacenter/colocation facilities. A list of these subservice organizations and the activities performed is provided in Section III. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Limelight, to achieve Limelight's service commitments and system requirements based on the applicable trust services criteria. Limelight's description of the boundaries of the system in Section III presents the types of complementary subservice organization controls assumed in the design of Limelight's controls, but does not disclose the actual controls at the subservice organization(s). Our examination did not include the services provided by the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Limelight 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 Limelight's service commitments and system requirements were achieved. Limelight has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Limelight is responsible for selecting, and identifying in its assertion, the applicable trust service criteria, and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organizations' service commitments and system requirements were achieved based on the applicable trust services criteria. 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 management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Limelight's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the operating effectiveness of controls is subject to the risks 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 Limelight's Content Delivery Network system were effective throughout the period May 1, 2021 to September 30, 2021, to provide reasonable assurance that Limelight's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted Use

This report is intended solely for the information and use of Limelight, user entities of Limelight's system during some or all of the period May 1, 2021 to September 30, 2021, business partners of Limelight subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- 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
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks

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

BDO USA, LLP

January 10, 2022

II. Assertion of Limelight Networks, Inc. Management

Assertion of Limelight Networks, Inc. Management

We are responsible for designing, implementing, operating and maintaining effective controls within Limelight Networks, Inc.'s (Limelight or the service organization) Content Delivery Network system (the system) throughout the period May 1, 2021 to September 30, 2021, to provide reasonable assurance that Limelight's service commitments and system requirements relevant to security and privacy were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

Limelight uses subservice organizations to provide datacenter/colocation facilities. A list of these subservice organizations and the activities performed is provided in Section III. The description of the boundaries of the system in Section III indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Limelight, to achieve Limelight's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Limelight's controls. The description of the boundaries of the system does not extend to the actual controls at the subservice organization.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Limelight, to achieve Limelight's service commitments and system requirements based on the applicable trust services criteria. The description the applicable trust services criteria and the complementary user entity controls assumed in the design of Limelight's controls. The description does not extend to controls of the user entities.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2021 to September 30, 2021, to provide reasonable assurance Limelight's service commitments and system requirements were achieved relevant to security and privacy (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). Limelight's objectives for the system in applying the 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 the description of the boundaries of the system in Section III.

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 were achieved.

We assert that the controls within the system were effective throughout the period May 1, 2021 to September 30, 2021, to provide reasonable assurance that Limelight's service commitments and system requirements were achieved based on the applicable trust services criteria.

Limelight Networks, Inc.

January 10, 2022

III. Limelight Networks, Inc.'s Description of the Boundaries of Its Content Delivery Network (CDN) System

Limelight Networks, Inc.'s Description of the Boundaries of Its Content Delivery Network (CDN) System

Scope and Description of the Boundaries of the System

This is a System and Organization Controls (SOC) 3 report and includes a description of the boundaries of Limelight's (Limelight, service organization, or Company) Content Delivery Network system (CDN or the system), and the controls in place to meet the criteria for security, and privacy (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), throughout the period May 1, 2021 to September 30, 2021, which may be relevant to users of the system. It does not encompass all aspects of the services provided or procedures followed for other activities performed by Limelight.

The CDN system uses the following subservice organizations to provide datacenter/colocation facilities across the globe:

- 365 Data Centers
- AMS-IX
- Bezeq
- DRT
- Equinix
- H5
- Interxion
- Irideos
- Market Halsey
- Nxtra Data
- Telehouse
- VPLS

The description of the boundaries of the system does not extend to the actual controls at the subservice organization(s).

Company Background

Limelight provides digital content delivery, online video delivery, cloud security, edge computing, and cloud storage services. Limelight's edge services platform includes a globally distributed private network, intelligent software, and support services.

Services Provided

The services provided by Limelight help customers optimize and deliver digital content to a wide variety of devices leveraging Limelight's private global network, which offers distributed computing resources and extensive connectivity to last-mile broadband network providers, making it well suited to emerging edge compute workloads where rapid response times are needed. These services provide advanced features to enable digital workflows for live and on-demand video publishing, online gaming, content distribution, and website and web application acceleration. Limelight incorporates content and application security, video transformation, and distributed storage functionality into the services, as well as the analytics and reporting associated with them.

Limelight's Global Network

Limelight's CDN platform and architecture is managed by the Company's proprietary software and automatically responds to network and data center outages and disruptions. Most delivery locations are interconnected via a global network and are connected to multiple internet backbone and broadband internet service provider (ISP) networks.

The Limelight global network has three main features:

- *Fiber Backbone* - The Limelight network includes a fiber backbone that connects delivery points of presence (PoPs) and enables content to bypass the public internet as it is distributed to the end-user. Each Limelight PoP has servers that enable cache hit efficiency and facilitate fast delivery performance.
- *Global Scalability* - Limelight's global network infrastructure includes PoPs in every region of the world to cache and deliver content from locations close to where it's being requested. Limelight's network is also interconnected with more than 1,000 major ISPs and last-mile network providers, shortening the distance and number of hops that content needs to take.
- *Intelligent Software* - Limelight has developed proprietary software that manages its global network. This software manages, among other things, the delivery of digital content, the retrieval of dynamic content, storage and retrieval of objects, activity logging, and information reporting.

Principal Service Commitments and System Requirements

Limelight designs its processes and procedures related to the CDN to meet its business objectives. Those objectives are based on the service commitments that Limelight makes to its customers, the laws and regulations that govern the provision of the CDN services, and the operational and compliance requirements that Limelight has established for the services.

Service commitments (including security and privacy commitments) to customers are documented and communicated within the Terms of Service and Privacy Policy, as well as in the description of the service offering provided on the Company's website, and in its marketing materials.

Limelight establishes operational requirements that support the achievement of security and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Limelight's system policies and procedures and in system design documentation.

Information security and privacy 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 CDN service.

Components of the System Used to Provide the Services

Infrastructure

The CDN consists of various infrastructure components such as networking equipment, servers, monitoring and analytics systems, which utilize tools to support software and configuration management and deployment, access and authentication, communication services, messaging management, database systems, and security tools. The CDN platform is located in a mixture of data centers distributed across six continents. These data centers are typically in tier 3 or tier 4 colocation facilities.

The networking equipment consists of routers, load balancers, and switches which provide secure interconnections between public and private environments. This equipment filters traffic with access control lists (ACLs) and provides protections against distributed denial-of-service (DDoS) attacks and other malicious network traffic.

The server environment consists of various virtual and physical systems that provide application, database, storage, authentication, logging, security, monitoring, and data backup. These systems are configured to be resilient and, where practical, redundant to reduce single points of failure and service outages. The security and operations functions include authentication and privileged access management systems, which restricts access to only authorized users. Logging and monitoring systems are also utilized to alert on performance, possible security issues, and malicious software.

Limelight has multiple databases designed to perform at optimal functionality depending on the services provided by the database.

Software

Limelight utilizes software and system configuration management tools to manage configurations and properties for deployable artifacts. It's centrally managed to automatically control application behavior in a given environment.

The CDN is deployed by a variety of processes to data centers in major metropolitan locations worldwide, which Limelight uses to run its proprietary CDN caching software and supporting technology.

Limelight uses industry standard code repositories as part of its system development methodology. Build, test and deploy processes are automated where possible using both commercial and open-source software and tools. A ticketing system is used to manage programs of work, monitor project progress and backlog, and combined with other tools provides an integrated view of work in progress.

Limelight uses proprietary asset lifecycle management tools for physical and virtual servers in its environment, which helps to manage physical and virtual host and internet protocol (IP) address inventory.

People

The Limelight staff are organized into the following functional areas to support the CDN services:

- *Executive Management* – Accountable for mission achievement, revenue results, and cost management to provide exceptional service to customers.
- *Product Management* – Provides leadership and management in the creation of multi-year product and business development strategies. Responsible for transforming organizational strategies into product and business planning requirements, artifacts, and initiatives used by the enterprise to execute and deliver products and services into the marketplace. Facilitates and drives strategic partnerships, opportunities and identifies creative and intentional markets and channels that further Limelight's vision and mission.
- *Architecture* – Responsible for driving technology and architecture decisions across aspects of the CDN platform, including the backend server, end-user facing Web UI and mobile clients, integration products, content production, and on-and-off-premises cloud environments.
- *Information Technology (IT)* – Responsible for providing Limelight with a reliable and scalable environment that supports 24x7 enterprise IT operations. This includes ensuring the reliability, availability, safety, security and integrity of Limelight's enterprise computing systems, data storage, virtual and physical environments, and corporate networking.
- *Customer Support* – Responsible for ensuring Limelight platforms and associated services are available to CDN customers in accordance with availability service level agreements, which generally translates to 24x7 operations. This includes ensuring the reliability, availability, safety, security and integrity of Limelight non-development computing systems, data storage and access.
- *Quality Assurance (QA)* – Ensures the overall quality (productivity, reliability, and accuracy) of the systems and data used within Limelight CDN computerized testing and reporting applications.
- *Software Engineering* – Employs and guides appropriate development practices to ensure robust commercial grade production.
- *Corporate Technology* – Responsible for the direction and management of the organization's business technology infrastructure. This function provides guidance in the design, implementation, and support of business technology goals to maintain the high-availability environment of the corporate systems.
- *Implementation Support* – Works with customers and provides support as they begin using Limelight services.
- *Information Security* – Performs regularly scheduled vulnerability scans and audits based on defined best practices and standards, provides continuous improvement feedback, and responds to security events and queries from internal and external sources.

Processes and Procedures

Formal privacy and information security policies, procedures, and guidelines describe safeguards and requirements to protect against unauthorized access to system resources. These items include identity and access management, system configurations, appropriate use of assets, third party reviews, change control, business continuity and disaster recovery, and incident management.

Employees are expected to adhere to the policies and procedures that define how services should be delivered. Organization-wide policies are located within Limelight's policy management software and detailed procedures are available on Limelight's intranet sites, accessible to Limelight team members.

Data

Maintaining the security and privacy of customer data is one of Limelight's highest responsibilities. Limelight CDN data includes log file data in W3C compliant Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) extended format, various system log files (e.g., authorization, system, access, IPv4/IPv6, Uniform Resource Identifier, etc.), aggregated usage data for billing and reporting, and raw log data for operational activities required to support the CDN services. Additionally, data is collected on network utilization, traffic management, and quality of service.

Data containing personally identifiable information (PII) is managed, processed, and stored in accordance with the relevant data protection, and other, regulations.

Complementary Subservice Organization Controls (CSOCs)

Limelight's controls related to its Content Delivery Network system cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by Limelight's controls. The CSOCs in the table below are expected to be implemented and operating effectively.

Number	CSOCs	Applicable Criteria
365 Data Centers, AMS-IX, Bezeq, DRT, Equinix, H5, Interxion, Irideos, Market Halsey, Nxtra Data, Telehouse, VPLS		
1.	Subservice organizations are responsible for having controls in place to understand and comply with their contractual obligations.	All
2.	Subservice organizations are responsible for having controls in place to limit and restrict physical access to Limelight-designated areas.	CC6.4
3.	Subservice organizations are responsible for having controls in place to notify Limelight stakeholders immediately upon the identification of an actual or suspected security incident.	CC7.4

Complementary User Entity Controls (CUECs)

Limelight's controls related to its Content Delivery Network system cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by Limelight's controls. The CUECs in the table below are expected to be implemented and operating effectively.

Number	CUECs
1.	Customers are responsible for understanding and complying with their contractual obligations.
2.	Customers are responsible for ensuring the security and privacy of their content data.
3.	Customers are responsible for reporting any actual or suspected information security or privacy issues in a timely manner.
4.	Customers are responsible for notifying Limelight of any changes to account contacts in a timely manner.
5.	Customers are responsible for maintaining user access to their CDN Control web portal.
6.	Customers are responsible for encrypting sensitive data in transit over the network.
7.	Customers are responsible for providing notice to data subjects about its privacy practices.
8.	Customers are responsible for communicating choices regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
9.	Customers are responsible for limiting the personal information collected from data subjects.
10.	Customers are responsible for obtaining explicit consent from data subjects when collecting personal information.
11.	Customers are responsible for granting data subject access to their stored personal information.
12.	Customers are responsible for correcting personal information based on information provided by data subjects.
13.	Customers are responsible for obtaining explicit consent from data subjects when disclosing personal information.
14.	Customers are responsible for disclosing data subject personal information.
15.	Customers are responsible for obtaining privacy commitments from third-parties with access to data subject personal information.

Number	CUECs
16.	Customers are responsible for notifying data subjects and regulators of breaches and incidents affecting personal information.
17.	Customers are responsible for collecting and maintaining complete and accurate data subject personal information.