Limelight NETWORKS

EXPERIENCE FIRST

limelight.com

Limelight Networks, Inc.

Information Security Processes & Protocols Overview

August 2020

Publication Note
This Overview document or any information contained herein may not be provided to parties outside of Limelight without prior approval of the Senior Director of Business Operations, who will confirm that the recipient is a party to a non-disclosure agreement with Limelight. This Overview represents the current state of Limelight's Information Security Program and service offerings as of the version date. Any responsibilities and liabilities as between Limelight and its customers are controlled by an agreement or agreements between the parties, and this Overview is not a part of any such agreement or agreements

Limelight Networks Public Information
The following material contains Limelight Networks information suitable for public distribution.

Table of Contents

Table of Figures

1. Introduction

Whether it is your website, mobile applications, videos, music, software, games, or APIs, your content needs to reach customers quickly, reliably, and securely. Limelight provides the capacity, coverage, and performance to cost-effectively deliver a better experience for you and your customers. Unlike traditional CDN vendors who rely on third-party technologies for key components of their content delivery infrastructure, Limelight's ongoing investment in the development and optimization of every component of its content delivery platform lets us deliver industry-leading delivery performance in a more secure environment.

This overview of Limelight's security processes and protocols as they pertain to Limelight's physical and logical security (Overview) is intended to provide you with a summary of how Limelight has designed and implemented a suite of business and technical controls, processes and procedures to help identify, protect, detect, and respond to security threats in order to protect customer content. Outlined here are some of Limelight's measures, policies, procedures, protocols, and guidelines to ensure security of its network and its service offerings.

This Overview, along with each of the measures, policies, procedures, protocols, and guidelines described herein, are reviewed and updated periodically.

2. Definitions

This table lists definitions of terms that may be helpful for reference while reading this overview.

Term	Definition
Access Control List (ACL)	A list of permissions attached to an object. An ACL specifies the users or system processes granted access to objects, as well as the operations allowed on given objects.
Authentication	The process of identifying an individual, usually based on a username/ password combination, to ensure that the individual is who he or she claims to be. Authentication is distinct from authorization, which manages access rights of the individual.
Bastion host	A computer that lives in the public subnet that itself is unprotected by a firewall or filtering router and is fully exposed to attack.
Business Continuity (Plan) (BCP)	Business continuity planning covers disaster recovery planning and business resumption planning. BCP is the preparation and testing of measures that protect business operations and also provide the means for the recovery of technologies in the event of any loss, damage, or failure of facilities.
Cipher	An algorithm for performing encryption or decryption; a series of well-defined steps that can be followed as a procedure.
Cloud Storage	Limelight Service that allows customers to manage, add, upload, and download millions of files in the cloud, while automatic replication ensures objects are always available.
Confidential	Classification of data or information that may only be shared with individuals who have a “need to know,” who are authorized to access such data or information, and who are bound by contractual obligations concerning treatment of confidential information.
Content Delivery Network (CDN)	A CDN is a system of distributed servers (network) that delivers web pages and other web content to a user based on the geographic location of the user, the origin of the web page, and a content-delivery server.
Credentials	Information used by a process or user to confirm users are authorized to access a particular service. Credentials include passwords, secret keys, and multi-factor tokens.
Cross-Origin Resource Sharing (CORS)	CORS is a mechanism that uses additional HTTP headers to tell browsers to give a web application running at one origin access to selected resources from a different origin. A web application executes a cross-origin HTTP request when it requests a resource that has a different origin (domain, protocol, or port) from its own.
Cryptography (Cryptographic)	The use of sophisticated mathematical algorithms and secret keys to encrypt and decrypt data. Cryptography is used to provide secrecy and integrity to data, as well as authentication and anonymity to communications.
Data handling	The process of ensuring that data is stored, archived, and disposed of in a safe and secure manner during the entire lifecycle of the data. This includes the development of policies and procedures to manage data handled digitally as well as through analog means.
Defense in Depth (DiD)	An approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack.
Disaster Recovery (DR)	The process and procedures undertaken to recover from an event deemed to have been a disaster. Usually a company-wide exercise as part of the Business Continuity Plan.
Edge caching	Distributing content (e.g., videos and other high-bandwidth data) from a local web server to caching servers that are closer to the end user (i.e., nearer the "edge").
Endpoint(s)	A URL that is the entry point for access to Limelight services. Connection to the endpoints is via HTTP and HTTPS.
Firewall (FW)	A part of a computer system or network designed to block unauthorized access while permitting outward communication.
Hash	Any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called *hash values*, *hash codes*, *digests*, or simply *hashes*.
Identity and Access Management (IAM)	A framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. Also called identity management (IDM), IAM systems fall under the IT and Information Security teams.
Information systems	The system of persons, data records, and activities that process data and information, including the organization's manual and automated processes.
Internet Protocol (IP)	A set of rules governing the format of data sent over the Internet or other network.

IP address	A unique string of numbers separated by periods or colons that identifies each computer using the internet protocol to communicate over a network.
IP spoofing	Creation of IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.
Logical security	The software protection of the entity's systems, including configurations like password parameters, as well as access controls such as access authorization and authentication.
Multi-Factor Authentication (MFA)	A method of computer-access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism.
Network ACLs	A layer of security deployed at the edge of the Limelight network that acts as a firewall for controlling traffic in and out of one or more subnets.
Non-public	Classification of data or information that has not been cleared for public distribution. The data or information could include confidential information, be intended for internal use or use by Limelight and third parties, or otherwise is not intended for public consumption.
Origin Storage	Limelight service that allows customers to manage, add, upload, and download millions of files in the cloud, while automatic replication ensures objects are always available.
Physical security	The protection of the entity's physical assets, including authorization to physically access information systems.
Port scanning	A series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, that the computer provides. This gives the assailant an idea where to probe for weaknesses.
Public	Classification of data or information that is free of confidential information that may be distributed publicly, such as publication on Limelight’s website, distribution to Limelight’s customers, third parties, or regulatory agencies.
Secure Shell (SSH)	A network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implements the protocol.
Secure Sockets Layer (SSL)	The standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remains private and integral.
Transport Layer Security (TLS)	Cryptographic protocols that provide communications security over a computer network. Web sites use TLS to secure all communications between their servers and web browsers. Successor to SSL.
Virtual Private Network (VPN)	A network that is constructed using public wires - usually the Internet - to connect to a private network, such as a company's internal network. A number of systems enables the creation of networks using the Internet as the medium for transporting data.

3. Information Security Program

Today, digital security is top of mind. From the boardroom to the breakroom, everyone is asking the same questions:

- How do we protect our digital content?
- How do we make sure no one can steal our content?
- How do we leverage the cloud/ edge and still maintain security?

Limelight understands security. We know our customers and partners place a trust in us that is only given because we do the right thing, remain vigilant, and maintain high standards in designing our systems, operating our networks, and delivering flawlessly, using the best processes and technology available.

We also understand that security is a team effort. Everyone in the digital delivery supply chain must take a share of the responsibility because no one link is responsible for all aspects. This Overview contains a general discussion of Limelight's security processes and protocols and the way we have approached the implementation of the information security program.

The details contained in this Overview speak to how Limelight secures, manages, and protects the resources and infrastructure utilized in the delivery of content over Limelight's edge cloud platform. Safeguarding digital content is not a one-size-fits-all solution; it involves multiple techniques and layers of security so as to provide defense in depth whilst planning for the worst to happen to ensure response and recovery processes are appropriately implemented and tested.

The level of security configurability and options available vary by service offering and are dependent on the intended use of the service and the data sensitivity that a customer may be uploading, storing, and delivering through the service.

Limelight uses the National Institute of Standards and Technology (NIST) Cyber Security framework to manage cybersecurity-related risk. The framework is prioritized and flexible and provides Limelight with a structured cybersecurity risk-management approach that is designed to promote the protection and resilience of infrastructure critical to Limelight and help Limelight identify, assess, and manage cyber risks generally. The framework core consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of our management of cybersecurity risk. The framework core then identifies underlying key categories and subcategories – which are discrete outcomes – for each function, and matches them with example informative references such as existing standards, guidelines, and practices for each subcategory, to which our technical and business controls are mapped.

This document references the framework core categories to assist the reader in understanding how the NIST framework is applied.

4. Identify

This section describes the steps taken and techniques used to ensure Limelight creates an approach to security that fosters and expands the organizational understanding necessary to manage the cybersecurity risk to systems, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables Limelight to focus and prioritize its efforts in a manner consistent with its risk management strategy and business needs.

4.1. Asset Management

Security starts with knowing where the assets are on the network, what those assets are, who owns the assets, and what are the purpose(s) of the assets.

4.1.1. Physical and Virtual Assets

Limelight manages all assets centrally using a custom asset-management database. All assets, and their relevant metadata, are held and maintained in this asset-management database, and permissions to view, add, delete, or edit are controlled. This allows Limelight to know which assets are on the Limelight network and where the assets are located. Each host is entered into the asset-management database, and Limelight systems take this information for monitoring and measurement functionality.

Every new Point of Presence (PoP) deployment is managed in the same way. Where the Bill of Materials (BoM) varies for scale, that is captured in the naming conventions used for the PoP, and it is all recorded in the asset-management database. Every service in the PoP relies on accurate asset records for its most basic functionality.

4.1.2. Software and Inventory Management

All code is stored in approved repositories which are hardened against relevant risks. The Limelight configuration-management platforms pull from explicitly configured repos, thus helping to ensure that only known and approved software, applications, and libraries are deployed to the environment and the risk of unknown software being present on the assets is reduced.

Limelight software inventory is populated automatically from the hosts directly. The software, packages, and libraries installed on the hosts are audited periodically. Variations in the installed software are reviewed. Alerts are triggered if a host has software that is not approved or if the version of that software is behind the latest available and supported version. The review of software installed enables Limelight to continually monitor the environment to ensure anomalies are recorded and reviewed and appropriate action is taken.

Limelight follows a standard design and implementation review process for all points of presence. This includes architectural review, operational process support review, and cybersecurity risk analysis and overall system audit. The architecture has been developed and deployed in compliance with the Limelight governance objectives, and the controls implemented are aligned with Limelight's overall regulatory, legal, risk, and operational requirements.

4.1.3. Data Privacy

Data Classification

Generally speaking, resources and information are classified as one of these types:

- Confidential
- Non-public
- Public

Every Limelight employee and contractor are bound by confidentiality covenants prohibiting that individual from disclosing confidential information to others who do not need to know such information. This includes Limelight confidential information and third-party confidential information. Limelight employees are trained to identify and properly handle confidential information, as well as identify instances when confidential information may need to be handled more securely.

Data Handling

Our practice, when possible, is to label documents containing confidential information as being confidential. Non-public information may be shared with individuals who have a need to know such information and who are bound to confidentiality. All confidential information is considered non-public. Information may become public so long as it is not (or is no longer considered) confidential information and if Limelight has permission to make public. Examples of this could include, but are not limited to, Limelight financial statements, marketing materials, investor relation presentations, and public-facing company policies, such as Limelight's Privacy Policy, Acceptable Use Policy, Terms of Service, or Code of Business Conduct and Ethics.

Limelight also utilizes certain access controls and logical and physical storage separation to limit the access of confidential information to those with a need to know, and, when possible, places limitations on the amount of confidential information to which third-party service providers have access.

4.1.4. Governance

Limelight is committed to conducting its operations in a lawful and ethical manner. To protect Limelight's reputation and to assure uniformity in standards of conduct, Limelight has adopted and manages its global compliance program. The foundation of the program is the Limelight Code of Ethics and Business Conduct (Code), which applies to all Limelight employees, directors, contractors, and agents. The Code is our statement of expectations concerning business and professional standards of conduct. The program also features specific policies and procedures, addressing risk areas including but not limited to insider trading, anti-bribery, security, anti-harassment, conflicts of interest, import/ export control, intellectual property management, and more. These policies have been adopted, and others will be adopted as needed, to address specific ethical, legal, and regulatory risks, as well as compliance with federal, state, and local laws; compliance with standards of accrediting bodies; promotion of good corporate citizenship; prevention and early detection of misconduct; and identification and education relating to areas of particular concern to Limelight and its customers. The program upholds these following objectives:

- Focus on management of Limelight's most significant risks, as periodically assessed by Limelight management
- Participation of each Limelight officer and employee, as well as certain contractors and agents, in education and training sessions concerning the compliance program

- Continued implementation of a system of monitoring, auditing, and reviewing of the compliance program and detecting and correcting instances of failures to mitigate the most significant risks
- Executing procedures for reporting suspected violations of the compliance program, investigating suspected violations, and implementing corrective action, including, when appropriate, disciplinary action to prevent recurrence of violations.

To ensure the management objectives continue to be met, Limelight continuously assesses the risk in the environment using vulnerability audits and penetration tests using both automatic and manual methods. The results of these assessments are reviewed, and appropriate treatments are proposed and implemented to reduce the risk likelihood, impact, or both.

Compliance Program
Limelight is committed to conducting its operations in a lawful and ethical manner. To protect Limelight's reputation and to assure uniformity in standards of conduct, Limelight has adopted and manages its global compliance program. The foundation of the program is the Limelight Code of Ethics and Business Conduct (Code), which applies to all Limelight employees, directors, contractors, and agents. The Code is our statement of expectations concerning business and professional standards of conduct. The program also features specific policies and procedures, touching on risk areas including but not limited to insider trading, anti -bribery, security, anti-harassment, conflicts of interest, import / export control, intellectual property management, and more. These policies have been adopted, and others may be adopted as needed, to address specific ethical, legal, and regulatory risks, as well as, compliance with federal, state, and local laws, compliance with standards of accrediting bodies, promotion of good corporate citizenship, prevention and early detection of misconduct, and identification and education relating to areas of particular concern to Limelight and its customers. The program upholds these objectives:

- Focus on management of Limelight's most significant risks, as periodically assessed by Limelight management
- Participation of each Limelight officer and employee, as well as certain contractors and agents, in education and training sessions concerning the compliance program
- Continued implementation of a system of monitoring, auditing, and reviewing of the compliance program and detecting and correcting instances of failures to mitigate the most significant risks
- Executing procedures for reporting suspected violations of the compliance program, investigating suspected violations, and implementing corrective action, including, when appropriate, disciplinary action to prevent recurrence of violations.

Executive and Board Review
Management reports on compliance program matters generally to the Board of Directors at least annually. This report may include a variety of topics, such as employee training and education, as well as Limelight policies and procedures on various topics including business conduct, crisis preparedness considerations, and changes in laws or trends. Reporting is also expected to include discussion of incident response efforts to material incidents should they exist. Management also reports to the Audit Committee on a quarterly basis regarding financial and Information Technology (IT) controls and procedures.

Communication
Information is the lifeblood of a well-managed, customer-focused organization. Effective security relies on this well managed and standardized communication process in order to mitigate any issues that occur in the shortest possible time frame with the minimum of impact. Limelight constantly reviews and updates its communication capabilities in order to deliver the quality services that its customers expect.

Limelight's global headquarters is in Arizona, USA; however, Limelight employs a globally diverse workforce, which helps mitigate risks inherent with centralized operations. Various methods of internal communication are used to help employees from different corners of the world collaborate and communicate significant events in a timely manner.

Limelight's communication efforts begin with the onboarding and new-hire orientation processes. These processes include structured new-hire training programs. Once on board, important company messages, including those concerning Information Security, are reinforced through discussions at regular management meetings for updates on business performance and other matters, through electronic means, such as video conferencing, electronic mail messages, Internet chat services, and the posting of information and policies, procedures, and guidelines on Limelight's intranet site.

Limelight also has various methods to communicate with customers. Mechanisms are in place to allow customer-support teams to be notified of operational issues that impact the customer experience. Multiple service dashboards are available and maintained by the customer-support team to alert on any issues. The 24x7x365 Network Operations Center (NOC) and customer-support team respond to phone calls and emails, send out proactive and reactive event communication, and follow up with direct communication when an event has been resolved.

Limelight's change-management process uses automatic and manual communication methods to advise customers of any standard or emergency changes with up to two-weeks' notice before scheduled activity for standard changes.

The incident-management process adheres to a highly specific communication plan as directed by the incident's severity.

Communication practices, both internal and external, ensure that issues are avoided whenever possible, processes are standardized to reduce complexity, and issues that do occur are resolved quickly.

Risk Management and Assessment
Limelight applies the NIST risk framework principles to its risk-assessment and risk-management activities. This enables Limelight to use a standardized and repeatable process for integrating security and operational risk into the system lifecycle, from software development to the running of systems in the production network.

Risk management objectives are aligned with Limelight strategy, and each objective is reviewed annually. This ensures Limelight continues to align its security and privacy objectives with its priorities and risk decisions. The risk-management process includes internal and external services and ensures considerations of risk are made for both standard and custom deployments of infrastructure and known and novel risks present in the environment.

5. Protect

Limelight has developed and implemented safeguards to ensure delivery of its critical infrastructure services is protected from cybersecurity threats. These safeguards are intended to provide Limelight with a defense in depth approach to addressing and ensuring the availability, integrity, confidentiality, and safety of its cloud computing infrastructure, wherever it is deployed across the globe.

5.1. Access, Authentication and Audit

The basis of user management is a robust implementation of user-management controls to ensure the *who*, *what*, and *where* of a user interaction is understood and monitored.

5.1.1. Identity and Access Management (IAM)

Limelight has a standardized IAM plan that covers credential management, access management, and audit. All access is provided on a least-privileged basis with mandatory approval, complexity, audit, and review activities.

5.1.2. Individual User Accounts

All users must have individual accounts. No shared accounts are permissible. The sharing of individual user accounts is an offense that can lead to discipline, up to and including termination of employment.

5.1.3. Remote access

Access to the Limelight infrastructure is managed via VPN, which supports mandatory multi-factor authentication, and all users are locked to profiles that are further restricted to only appropriate segments of the environment.

VPN session idle timeouts and active timeouts expire periodically, and all access is logged. Logs are reviewed and alerts configured for anomalies.

5.1.4. Access Controls

All logical access to Limelight's information systems, networks, and/ or resources must be approved and granted on a least-privilege basis. Access to information resources and systems must be controlled based on business requirements, as well as an individual's role and responsibility level.

All Limelight information systems, including applications, operating systems, networks, databases, and resources, must be assigned an owner. Owners are responsible for granting and approving access on a least-privilege basis.

Once proper approval has been received and documented, the Limelight IT department is responsible for granting system access.

Physical access to systems is restricted and a least-privilege method is used to ensure only the individuals who need access have the correct access. All employees wear visible badges to enable access to office spaces and data centers. Employees are required to challenge or report unknown individuals who are not displaying a badge.

5.1.5. Review of User Accounts & Audit

A process for effective and prompt removal of accounts associated with terminated users is followed to prevent unauthorized access by former employees, consultants, or third-party users who may possess inside knowledge of the operation of Limelight information systems. Upon the termination of an employee, consultant, or third-party user, the Human Resources department disseminates a notification email to system owners or Limelight management of terminations to ensure prompt removal of user accounts.

Procedures are performed to ensure that user access is removed from all network and application resources. Terminations of user accounts must be processed within five business days as do access changes (e.g., due to transfer). Following termination, a step-by-step process is initiated to ensure prompt and proper access removal.

User accounts must be reviewed and approved by Limelight data/ business owners quarterly. These reviews occur in the last month of each quarter and must be completed within two weeks of the end of the quarter for which they are reviewing. User privileges must be updated in a timely manner upon change in employment/ contract status, including promotion, departmental transfer, leaves of absence, and employment/ engagement termination. Inactive accounts that have not already been disabled or deleted are disabled or deleted as a result of this review. Disabled IDs remain in the system in an inactive state for 60 days and are not permitted log in to services. Disabled accounts due to termination are removed after 60 days unless explicit exception is requested and granted for business reasons.

5.1.6. Credentials Policy

Limelight's Information Security department has established a Credentials policy with required configurations and expiration intervals.

All passwords have complexity and expiration intervals. Passwords must be complex, and users are forced to change passwords after a set period of time. Limelight also enforces additional complexity and usage requirements.

Limelight reviews credentials periodically and revokes credentials automatically upon termination of employment/ engagement or when unauthorized use or suspicious activity is detected.

5.1.7. Awareness Training

Limelight provides its employees with a tailored awareness and compliance training program. This training is delivered on an ongoing basis and includes compliance and cybersecurity training necessary to perform duties in line with Limelight's policies and procedures and the agreements with customers and vendors.

5.2. Communication Protection

Limelight provides a number of methods for connecting to the service. HTTP and HTTPS using TLS are supported for content delivery. Limelight continuously reviews the cryptographic strength of our implementation, and new ciphers are deployed on a monthly cycle as older ciphers are deprecated.

For customers accessing the Origin Storage service, Limelight has established secure Application Program Interface (API) endpoints supporting HTTPS, which allows customers to establish secure sessions for uploading content. Limelight also supports other secure connection methods should a customer require.

5.3. Monitoring and Protection

Limelight continuously monitors the transmission of traffic across and over the network in order to limit risk and to simplify network management. Limelight deploys network devices, including firewall and other boundary devices, to monitor and control communications at the boundary of the network and at key internal boundaries within the network.

These boundary devices enforce policies, Access Control Lists (ACLs), and configurations to enforce the flow of information to specific information systems and services.

ACLs and flow policies are established on each managed interface, which manage and enforce the flow of traffic. ACLs and policies are approved by Limelight Information Security.

Corporate Segregation
Limelight logically segregates production networks from the corporate network. Limelight developers and administrators on the corporate network who need to access Limelight production components in order to maintain them must explicitly request access through Limelight ticketing systems. All requests are reviewed and approved by the applicable service owner. All access to off-net hosts/ services is managed by firewall policies, which are reviewed periodically.

To access any Limelight device on the Limelight network, approved individuals need to log on to the network from an approved IP address. Once authenticated, Limelight personnel then connect to the device through a bastion host that restricts access to network devices and other cloud components, logging all activity for security review. Access to jump hosts requires SSH public key authentication for all user accounts on the host. Approval is reviewed quarterly, and any changes are made at that time to ensure permissions are current and appropriate.

5.4. Patch Management

Limelight is responsible for ensuring the confidentiality, integrity, and availability of Limelight data and customer data stored on its systems. Limelight has an obligation to provide appropriate protection against malware threats, including viruses, trojans, ransomware, and worms, which could adversely affect the security of the system or the data on the system.

Limelight's Development and Operations teams follow an N-1 policy with regard to patches and updates as a means to meet its protection obligation. Secure, standardized packages are kept in the Limelight repository, where access is controlled and reviewed. Limelight's Development and Operations teams manage a constant reporting on patch availability and support, and a constant deployment model ensures up-to-date systems. Explicit approval is required for any variance from this policy, and controls are implemented where possible to manage the exceptions.

5.5. Change Management

Change management is the process responsible for controlling the life cycle of all changes implemented into the production environment. Operational change management creates discipline and quality control for planned changes to the production environment. Attention to change-control governance, policies, and procedures is key to ensuring service stability and availability. An effective change-management process minimizes service downtime and unexpected impact to the production environment.

Change management policies and processes apply to all Limelight internal users and any third-party consultants that Limelight may engage for assistance, each of whom operates within Limelight's production environments and internal business systems. Limelight applies a systematic approach to managing change so that changes to customer-impacting services are thoroughly reviewed, tested, approved, and well-communicated. Routine, emergency, and configuration changes to existing Limelight production infrastructure are authorized, logged, tested, approved, and documented and are audited as part of the Limelight Sarbanes-Oxley Act (SOX) IT General Controls. The Limelight change-management process is designed to avoid unintended service disruptions and to maintain the integrity of service to the customer.

Change is typically deployed into production in a phased approach starting with specifically designated sites where impact is lowest. Deployments are tested on a single system and closely monitored so impacts can be evaluated. The Operations team utilizes a number of metrics to measure the health of the service's upstream dependencies, and these metrics are closely monitored with thresholds and alarming in place.

Changes are scheduled during regular change windows. Emergency changes to production systems that require deviations from standard change-management procedures are associated with an incident and are logged and approved as appropriate.

Limelight performs periodic audits of changes to monitor quality and facilitate continuous improvement of the change-management process. Any exceptions are analyzed to determine the root cause, and appropriate actions are taken to bring the change into compliance or roll back the change if necessary. Actions are then taken to address and remediate the process or resource issue.

5.6. Storage Device Decommissioning

When storage devices are decommissioned, we select responsible recycling (R2) certified vendors to properly dispose of our e-waste. All data on any storage device is destroyed in compliance with the data sanitizing standards of all applicable state and federal laws and regulations listed here and every data storage device that passes through the processing facility receives this level of destruction.

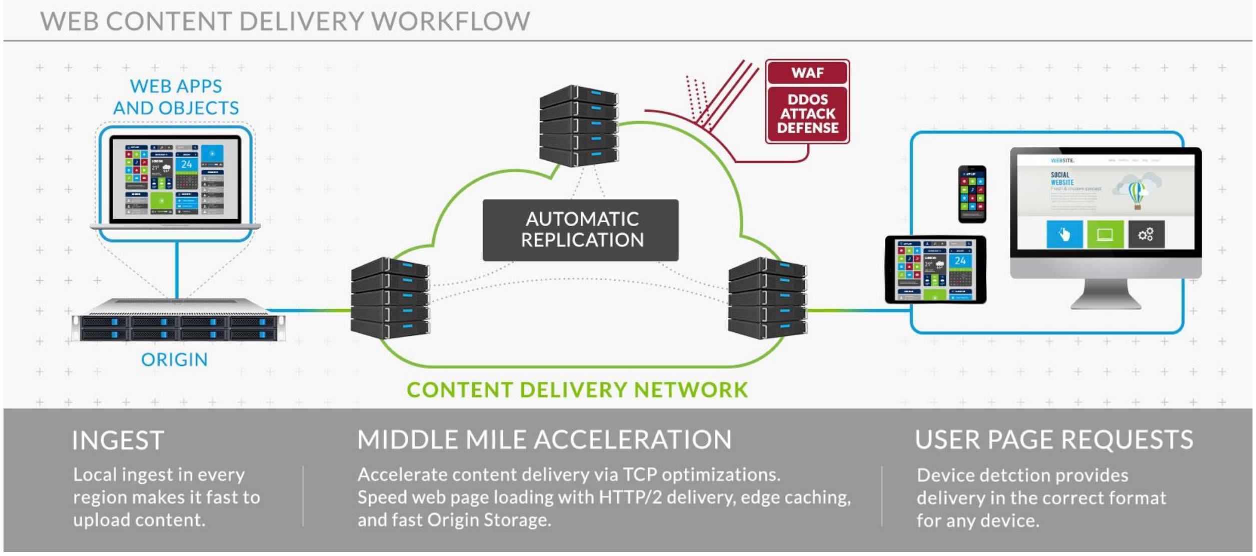
- Federal Information Security Management Act (FISMA) of 2002, Public Law 107 -347
- National Institute of Standards and Technology (NIST) Special Publication 800-88
- Department of Defense (DoD) 520.22-M
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX) Act
- Gramm-Leach-Bliley Act
- Bank Secrecy Act
- Patriot Act of 2002
- Identity Theft and Assumption Deterrence Act
- Identity Theft Penalty Enhancement Act
- United States Food and Drug Administration (FDA) Security Regulations (21 CFR Part 11)
- Statute 325E.61 Data Warehouses; Notice Required for Certain Disclosures
- Statute 325E.64 Access Devices; Breach Security Act

6. Protect: Limelight Service

This section describes security processes and protocols of the Limelight edge cloud platform.

6.1. Content Delivery & Web Acceleration

Limelight's Content Delivery and Web Acceleration services offer many features to provide security, including IP access control/ geo blocking, method access control, MediaVault, CORS, referrer blocking, and ARC Light. Additionally, these services can be combined with Limelight's Cloud Security services to ensure secure delivery of customer content.



Local ingest in every region makes it fast to upload content.

Accelerate content delivery via TCP optimizations. Speed web page loading with HTTP/2 delivery, edge caching, and fast Origin Storage.

Device detction provides delivery in the correct format for any device.

Figure 1: The Limelight solution for web content delivery accelerates both dynamic and static content using the Limelight CDN, which includes globally distributed Origin Storage services, middle-mile acceleration, and edge caching.

6.1.1. IP Access Control/ Geo blocking

The IP Access Control service offers the ability to allow/ deny access to an IP address, IP ranges, anonymizers, and geographical locations. Customer-specific groupings of IP ranges can be allowed or denied access, regardless of an IP address' geolocation. Customer-specific groupings, anonymizer status, and geo blocking can be used in concert on a customer rewrite.

6.1.2. Method Access Control

GET, POST, HEAD, and OPTIONS can be allowed or denied based using Method Access Control.

6.1.3. MediaVault

MediaVault is a high-performance, server-side authentication service used to assist customers in securing content from unauthorized views. The system uses cryptographic hashing based on the MD5 algorithm. This algorithm is designed so that any changed byte of the hash propagates new changes throughout the remainder of the calculation, resulting in a completely unique hash.

6.1.4. CORS Management

Customers can Add, Set, and override CORS directives on a per-request basis, allowing multiple content origins, while restricting resource sharing to designated origins. In this way a customer has a fine-grained control over how to control resource access.

6.1.5. Referrer Access Control

This service enables the ability to allow or deny referrer URLs. Only requests that have a referrer header matching a domain in the list will be allowed or denied.

6.1.6. ARC Light

ARC Light brings compute to the edge. User request and origin responses contain ARC Light-actionable data, including: IP address, URL, query strings, header, and cookies. ARC Light can execute complex security logic in real-time at the edge using these data sources.

6.2. Origin Storage

Limelight Origin Storage is a high-performance, secure cloud solution that enables customers to replicate, move, and securely store data in the locations that provide optimal content delivery performance using Limelight's high-speed global network and regional ingest locations. Origin Storage supports industry-standard file-transfer protocols and simple web services to globally store and deliver data 24x7.

6.2.1. Accounts

Within the Origin Storage platform, all aspects of customer accounts (e.g. billing, reporting, and directory configuration) are delineated by account *shortnames*. Many customer organizations choose to use multiple, different shortnames/ accounts to separate data storage, configuration, reporting, and billing.

6.2.2. Users

Within a shortname/ account, customers have the ability to create multiple users. Each user can be either granted access to the account primary/ root directory or restricted access to any subdirectory or subdirectories within the root directory. Users then have the ability to add as needed sub-directories that will inherit the permissions of the parent directory.

6.2.3. Account Management

When users and/ or applications no longer require access to the Origin Storage account, Limelight advises customers to revoke access for the individual users/ applications.

6.2.4. User Credential Security

Limelight supports the use of secure protocols (e.g., HTTPS, SSL, SSH, etc.) when accessing the Origin Storage platform and anywhere credentials are required to ensure the integrity of the user.

6.2.5. API Token Management

Critical to the security of the Origin Storage API is the API token and the account credentials. Tokens are created when users call the API login function (or the account/ login endpoint in HTTP), which generates an alphanumeric token string that must be used with all subsequent API calls to authenticate the application with the system and permit the requested transaction. The Origin Storage API relies on the presence and validity of these tokens when verifying the authenticity of transaction requests.

By default, tokens are automatically removed after a predetermined amount of time, usually an hour. When engaging in a single transaction or group of transactions, customers can add protection against token reuse by unauthorized parties by calling the API logout function. On logout, the token is no longer valid on subsequent transaction attempts.

Unencrypted web protocols, such as HTTP, are vulnerable to eavesdropping. To keep tokens invisible to would-be malicious actors, customers are advised to make API requests via HTTPS rather than HTTP.

6.2.6. Data Upload

Origin Storage supports these secure upload methods:

- Origin Storage customer portal (https://control.llnw.com/)
- FTP-SSL (File Transfer Protocol over Secure Socket Layer)
- SFTP (Secure Shell File Transfer Protocol)
- SCP over SSH (Secure Copy Protocol over Secure Shell)
- Rsync over SSH (Remote Sync over Secure Shell)
- API (HTTPS) (Application Interface over HyperText Transfer Protocol Secure)
- Aspera FASP (Fast Adaptive and Secure Protocol)

Origin Storage also supports FTP and API (HTTP), insecure upload methods, and Limelight advises customers to use these at their own risk.

As an additional security mechanism, all upload methods except the Customer Portal and API require customer IPs to be *allowed* in order to connect to an upload server.

6.2.7. Data Transfer

For maximum security during upload and management, customers can securely connect to Origin Storage using any of the secure upload methods identified in the Data Upload section.

For maximum security on download, refer to MediaVault section of Content Delivery & Web Acceleration.

6.2.8. Data Durability & Reliability

Origin Storage is designed to provide 100% durability and 100% availability of objects over a given year. Objects are replicated on multiple hosts across multiple facilities when using a standard Origin Storage policy. For some lower-tier services, Origin Storage may store objects on multiple devices in the same facility. Once stored, Origin Storage maintains the durability of objects by quickly detecting and repairing lost redundancy. On upload, objects are catalogued using a SHA-256-bit hash function to meet the criteria defined by policy (geo-location, number of copies, and so on), using the NIST Federal Information Processing Standard. Origin Storage verifies the integrity of data stored using the checksums during the process of replicating objects from the point of upload to the long-term storage devices. If corruption is detected, the object is discarded, and a new replica is created using a known good object.

6.2.9. Storage Device Decommissioning

When a storage device has reached the end of its useful life, Limelight Origin Storage procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Limelight Origin Storage uses the techniques detailed in the National Industrial Security Program Operating Manual DoD 5220.22-M or in NIST 800-88 (the Guidelines for Media Sanitization) to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

6.3. Video Delivery

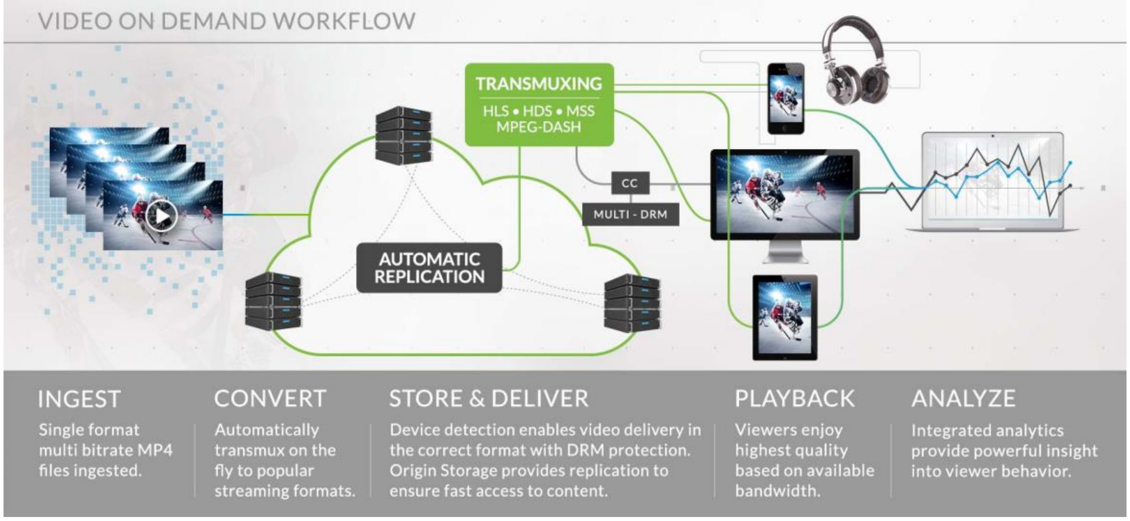
6.3.1. Limelight Video Platform

Limelight Video Platform (LVP) provides customers with a comprehensive set of cloud-based tools to manage and distribute their video library. A login allows customers to access the Media Library interface, where videos can be uploaded, tagged, placed into playlists, and more. Logins must meet minimum format standards, and temporary passwords are automatically generated for new accounts and sent only to the email address used to log in. Customers may create sub-accounts that have restricted access to some of the Media Library functions. An email address may be used to log in to only one account, and a forgotten-password email can be restricted to be sent only if a secret question is answered. The Media Library interface is provided over HTTPS.

LVP also provides a robust set of APIs customers can use programmatically to perform the same functions that can be accomplished manually in the Media Library interface. All API calls must be authenticated using a signature. A signature is generated by doing a SHA-256 hash on the request URL and its parameters to generate a keyed-hash message authentication code (HMAC).

Video on Demand
The Video on Demand (VoD) streaming service is designed to distribute video files to any device, anywhere in the world. Customers provide Limelight with the origin source of their video files, and the service converts them on demand into multiple video formats, delivering them through the Limelight CDN. The origin source may be the customer's origin or Limelight's Origin Storage.

Delivery of on-demand streams is through the Limelight CDN edge servers. Customers can configure their delivery to use HTTPS, tokenization via the Limelight MediaVault service and with Digital Rights Management (DRM). Widevine, FairPlay, and PlayReady DRM can be used to encrypt HLS and DASH content segments. Customers can modify their player to request a license and decryption key to play back DRM content. In addition, customers can take advantage of Limelight's DDoS Attack Interceptor and Web Application Firewall (WAF) attack detection and mitigation services to further secure and enable their delivery needs.



INGEST: Single format multi bitrate MP4 files ingested.

CONVERT: Automatically transmux on the fly to popular streaming formats.

STORE & DELIVER: Device detection enables video delivery in the correct format with DRM protection. Origin Storage provides replication to ensure fast access to content.

PLAYBACK: Viewers enjoy highest quality based on available bandwidth.

ANALYZE: Integrated analytics provide powerful insight into viewer behavior.

Figure 2: Limelight's VOD solution architecture

Video Live
Video Live is a live streaming service used to distribute live streams to any device, anywhere in the world. Customers send an RTMP stream to the Limelight Networks ingest servers, and the service delivers that live stream in multiple video formats through the Limelight CDN. Customers are able to configure their live streaming service through the Limelight Control interface, which requires two-factor authentication to access for added confidence in its security.

Ingest servers are published to by customers' encoders. The encoders must support the Limelight authentication protocol, which involves a handshake between the encoder and the ingest server using the proper authentication credentials. The ingest servers are restricted to accept connections from outside the Limelight network on only specific ports.

Delivery of live streams is through the Limelight CDN edge servers. Customers can configure their delivery to use HTTPS, tokenization via the Limelight MediaVault service with DRM. In addition, Video Live customers can take advantage of Limelight's DDoS Attack Interceptor and WAF attack detection and mitigation services.

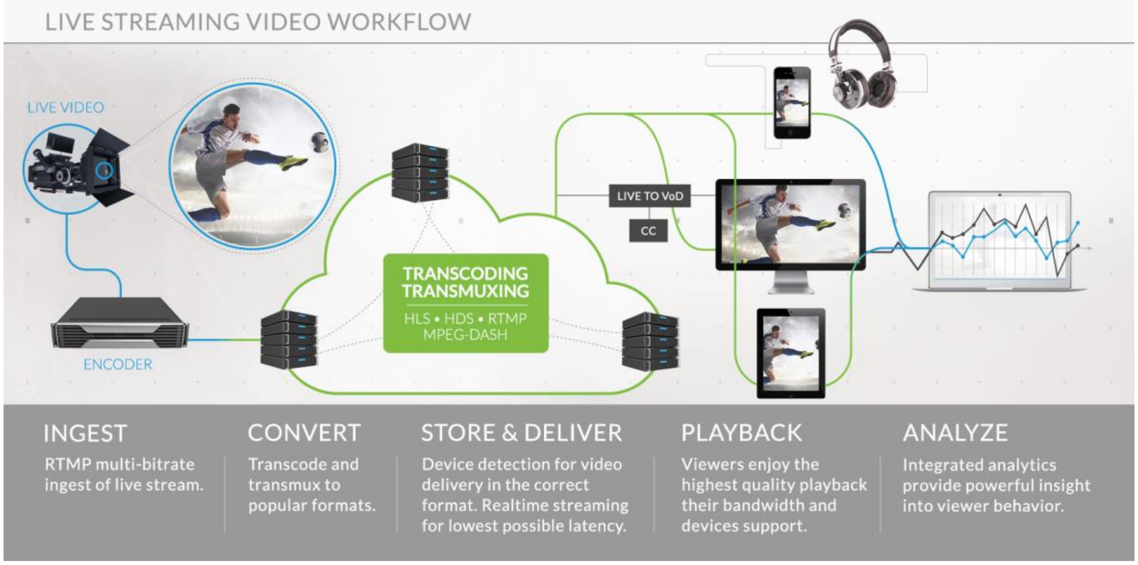

LIVE STREAMING VIDEO WORKFLOW
LIVE VIDEO
ENCODER
TRANSCODING TRANSMUXING
HLS • HDS • RTMP MPEG-DASH
LIVE TO VoD
CC
INGEST
RTMP multi-bitrate ingest of live stream.
CONVERT
Transcode and transmux to popular formats.
STORE & DELIVER
Device detection for video delivery in the correct format. Realtime streaming for lowest possible latency.
PLAYBACK
Viewers enjoy the highest quality playback their bandwidth and devices support.
ANALYZE
Integrated analytics provide powerful insight into viewer behavior.

Figure 3: Limelight's Video Live solution architecture

6.3.2. Cloud Security

Limelight’s Security Alert and WAF services offer customers many security protections. Customer origins have passive protection from request flooding by virtue of the CDN's caching behavior, when configured appropriately. When used in conjunction with Limelight's WAF offering, requests to origin can pass through an additional layer of protection, including mitigations for many of the OWASP top 10 web application security risks.

Globally Distributed Anycast Addresses
Large attacks are distributed to multiple Limelight PoP locations rather than a single PoP for improved mitigation. In this way, extremely large attacks are effortlessly absorbed with minimal impact to customers’ service delivery or performance.

DDoS Attack Notification and Alerts
Attacks are detected and communicated through an email-alert, so customers are aware and can take appropriate measures to defend valuable assets.

Rate Limiting
Customers control the maximum number of requests per second from a single IP address.

CAPTCHA support
Customer can protect web sites against bots and scripts by requiring human logic.

Bad Bot Detection and Mitigation
Incoming requests for content are challenged and fingerprinted to determine if the request was generated by a bot/ scriptor human user.

Active Mitigation of Layer 7 DDoS Attacks
Multiple defenses can be deployed by customers to protect web applications, including good-bot/bad-bot detection, IP rate limiting, IP access control, and CAPTCHA challenges.

24/7 Security Operations Center Monitoring
Limelight provides customers with the ability to receive daily threat intelligence monitoring, vulnerability and threat analysis, full-threat simulation, and regression testing.

6.3.3. Limelight Edge Cloud Compute Services

Limelight’s edge cloud eliminates the cost, complexity, and latency of utilizing traditional cloud-computing environments to enhance streaming video and content-delivery services, deploy global applications, create digital content, and perform real-time data processing. Unlike traditional cloud service providers who only offer compute in a limited number of centralized regions, Limelight edge computing instances are embedded in PoPs around the world. Compute infrastructure is integrated with Limelight’s secure global network, which provides direct peering with more than 1,000 ISPs and cloud service providers to deliver the fastest performance. Limelight's flexible edge compute options include serverless, virtual machine and bare-metal solutions. Limelight offers edge compute capabilities, how and where you need them.

Serverless Compute at the Edge
Limelight EdgeFunctions is a serverless compute platform that automatically makes your code available to many edge locations around the world, executes at the network edge close to the user to ensure the lowest latency, and scales to meet demand. EdgeFunctions is ideal for customers needing to implement streaming video and content-delivery use cases, such as personalized streaming, access control, dynamic ad insertion, A/B testing, image manipulation, and more. It is tightly integrated with one of the world's highest-performing video and CDN. EdgeFunctions gives developers tools to boost performance, customize workflows, and scale rapidly while only paying for resources used.

Virtual Machine Compute Services
Limelight offers global virtualized compute capacity that makes it easy to scale and grow as needs change. Intel processors and SSD storage deliver high performance for any compute task. Multiple virtual Linux server distributions are available with varying levels of CPU, RAM, storage, and network bandwidth to meet specific requirements. An easy-to-use control panel lets customers manage and monitor deployments as well as load-balance or back up configuration. APIs and a command-line interface are also available.

Bare Metal Compute Services
Dedicated bare-metal servers are available to give compute power where needed without having to share resources or deal with hypervisors. Limelight offers an array of hardware configurations featuring Intel and AMD processors with multiple levels of physical cores, RAM, storage, and network bandwidth. Dedicated servers can be deployed across Limelight's global network to support workloads in any region or location. Customers can choose a Limelight-provided operating system or load their own remotely. Customers have remote management capability via an intuitive portal or RESTFUL APIs and a secure IPMI lights-out management capability.

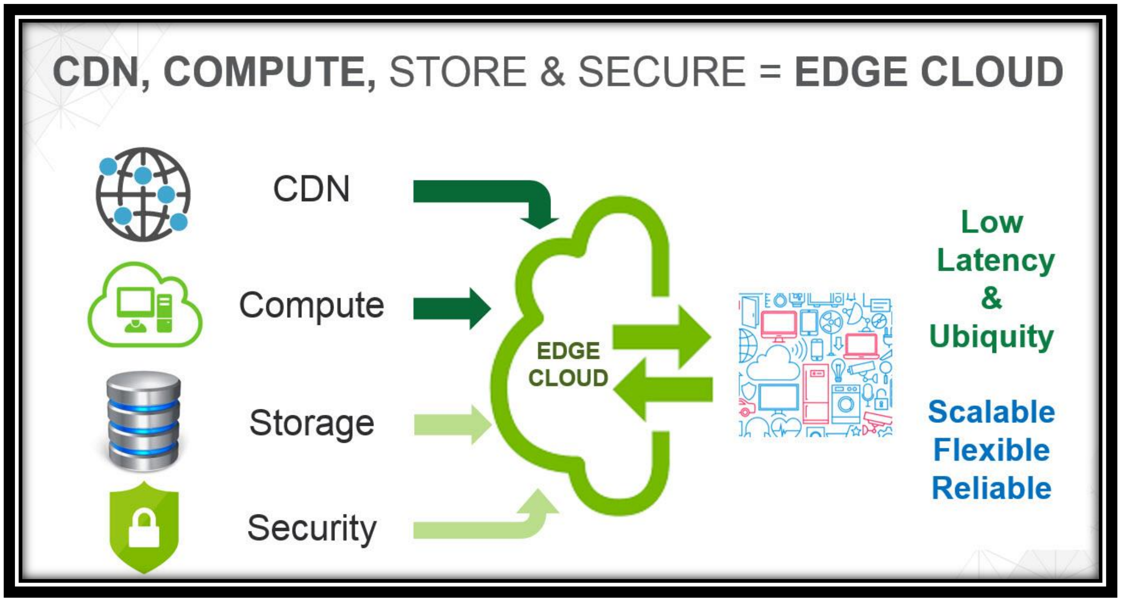

CDN, COMPUTE, STORE & SECURE = EDGE CLOUD
CDN
Compute
Storage
Security
EDGE CLOUD
Low Latency & Ubiquity
Scalable Flexible Reliable

Figure 4: The Limelight edge cloud platform

7. Detect

Limelight Networks has developed and implemented an array of technologies, processes, and procedures to support the activities intended to identify and respond to the occurrence of a security event on the cloud infrastructure.

7.1. Security Operations

Limelight Operations uses industry-standard tools and technologies to collect, monitor, and measure events and anomalies in the network. Limelight's NOC is staffed 24x7x365 to respond to alarms and alerts in real time, and to take prompt and decisive action when necessary to ensure that the event triggering the alert or alarm is understood, and when necessary, mitigated, thereby blunting the potential impact to Limelight network, services, and business generally. Limelight continuously monitors the transmission of traffic across the network to limit risk and to simplify network management. Limelight deploys network devices, including firewall and other boundary devices, to monitor and control communications at the edge of the network and at key internal boundaries within the network. These boundary devices enforce policies, ACLs, and configurations to govern the flow of information to specific information systems and services. Each managed interface has its own ACLs and flow policies, which manage and enforce the flow of traffic. Limelight's Information Security team approves each ACL and policy. Limelight continuously monitors hosts deployed into the service provider network using manual and automatic tools from commercial and homegrown technologies, and Limelight reviews events to ensure the effectiveness of the measures taken to protect the availability and integrity of the systems.

7.1.1. Network Management

Limelight utilizes a broad range of tools, devices, metrics, and analysis for network management and to form a multi-layer defense and response capability.

Network ACLs are implemented on all network ingress points in the Limelight network. Limelight deploys these network ACLs to protect the network and minimize the risk and impact of accidental or malicious infrastructure attack. This works because using network network ACLs enables Limelight to explicitly permit only authorized traffic to the infrastructure equipment. while denying unauthorized traffic access to the infrastructure.

In addition, Limelight deploys bastion hosts to manage and secure access from non-Limelight hosts and off-net locations. The access-control methodology implemented at the bastion hosts is distinct from other applications of access control to increase the level of security of network access.

Access to all Limelight information systems requires authentication of the identity of the individual requesting access. All systems require sufficient authentication (e.g., password, token, public key, certificate, etc.) based on each system's individual risk profile.

Limelight deploys and utilizes a number of commercial and customized monitoring and management tools to ensure a high degree of performance and availability. Management and monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor, among other things, server and network usage, port-scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to alert and automatically respond when measurement thresholds are breached. Policy-based responses ensure identification and prevention occur at machine speed rather than human speed.

Limelight's systems are extensively instrumented to monitor key operational metrics. Limelight configures alarms to automatically notify Operations personnel and management when early-warning thresholds are crossed on key operational metrics. Limelight's NOC is staffed 24x7x365, and on-call resources are deployed at all times so that personnel are always available to respond to emergency operational issues.

7.1.2. Vulnerability Management

Limelight utilizes automated and manual intrusion detection and prevention tools and actively monitors and responds to threats. These tools provide multiple functions, including file-integrity checking and log file monitoring/ analysis, as well as rootkit detection, port monitoring, and detection of rogue executables and hidden processes. Limelight utilizes automatic and manual tools that are policy-driven in their response to detected events. System owners set these policies, which the Limelight Information Security team periodically audits for effectiveness. The tools used generate logs and metrics, which are ingested into a SIEM for analysis and alerting in the event that issues or anomalies are detected. Limelight monitors the logs and metrics generated by its global infrastructure so that any potentially disruptive threats are immediately identified and corrected.

7.1.3. Intrusion Detection / Prevention

Limelight deploys and utilizes various tools and techniques to detect and prevent intrusion into the network and hosts. Limelight leverages firewalls, ACLs, and HIDS and NIDS tools. Limelight also uses automatic policy- and event-based responses to defend the environment and protect the hosts.

8. Respond & Recover

Limelight has developed and implemented the appropriate activities to face a detected security event, as well as the appropriate activities for resilience and restoration of any capabilities or services that were impaired due to a security event.

8.1. Incident Management

The Limelight Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Limelight provides 24x7x365 coverage to detect and respond to incidents and to manage the impact and ultimately resolve the incident as efficiently as possible.

The primary objectives of the Incident Management process is to restore normal service operation as quickly as possible following an incident and minimize the adverse impact on customer and business operations. These principles are used to guide the actions of Limelight incident-response actions and drive improvement:

- Incidents are properly logged.
- Incidents are properly routed.
- Incident status is accurately reported.
- Queue of unresolved incidents is visible and reported.
- Incidents are properly prioritized and handled in the appropriate sequence.
- Resolution provided meets the requirements of Service-Level Agreements with customers.

Incident Management includes any event that disrupts, or that could disrupt, a service. This includes events that are communicated directly by customers or Limelight staff through the NOC or through an interface from Event Management to Incident Management tools.

8.2. Crisis Preparedness

Crises cannot be predicted. They are, by their very nature, unexpected events. While nobody can predict what crisis will come, how it will come, or when it will hit, Limelight takes measures to prepare for real-time response when a particular crisis occurs. Limelight maintains a Business Continuity Plan that serves as a blueprint for its response to crises that impact the continuity of services. Limelight also works with building management at its global headquarters and other offices to provide staff advice on how to address crises that could impact individuals at these locations, such as reacting to fire, poison, or active-shooter situation. Limelight maintains copies of building management-generated crisis preparedness policies and procedures on an internal Intranet page, and Limelight periodically sends links of these policies and procedures to staff.

8.3. Business Continuity

Business-continuity planning at Limelight includes a Pandemic Response Policy (PRP) and a Disaster Recovery Policy (DRP) at its core. These documents form the baseline guidelines for scenario- and system-specific plans as appropriate. Once either of these policies is activated, senior leaders from multiple functions are brought together to execute the policy. This approach is appropriate to the scale and complexity of Limelight business and ensures the continuity of critical business processes and functions, mitigates risk, safeguards provision of services, and sustains Limelight’s financial stability and customer confidence.

The policies outline core procedures for the relocation or the recovery of operations in response to varying levels of disruption. Factors considered include pandemic response, staff unavailability, loss of a single production site, loss of vendor services, and loss of application software. These plans provide information for responsible personnel to evaluate the business disruption and initiate appropriate action, which may include safeguarding employees and property, fostering effective communication between Limelight and Limelight employees, regulators, customers, and business-critical partners, protecting critical records, and recovering/ resuming normal operations.

8.3.1. Roles & Responsibilities

Policies define roles and responsibilities, which are documented in Limelight’s corporate plans. This fosters a constant and effective approach to the provision of resiliency throughout Limelight and results in an efficient fit-for-purpose business-continuity capability.

8.3.2. Crisis Management & Implementation

Limelight has a Business Continuity Plan that covers critical systems to ensure a clearly defined, documented, and tested process for assuring, escalating, and managing disruption that may affect the ability to continue business operations. This includes contact and escalation processes. In addition, these processes are designed to be implemented in response to varying levels of business disruptions. The nature of the business disruption affects whether all or only parts of plans are executed.

8.3.3. Business Continuity Solutions

Limelight has a broad policy in place to deal with the impact of an incident or crisis. We have a number of solutions designed to facilitate the quickest possible resumption of work for the critical businesses and support functions.

Alternate Sites
Limelight has self-managed, dedicated standby facilities for critical support services. The alternative sites provide dedicated seats and infrastructure to provide for the needs of the business. All sites are physically separated from normal business locations to prevent both sites being affected by the same incident.

Reciprocal Agreements
Limelight's office locations have the capacity to allocate a number of seats and workstations. This provides the necessary infrastructure, hardware facilities, and space for staff to continue the activities of Limelight should one office location be inaccessible for long periods of time. Normal business locations are geographically separated from each other to prevent both sites being affected by the same incident.

Remote Access
All staff can work remotely in the event of a disruption, accessing Limelight systems via VPN. All critical staff are provided with the means to work anywhere for extended periods of time if necessary.

Pandemic Planning
Limelight maintains a risk-based approach to epidemic planning, using public federal and local health agency information as a guide.

9. Additional Security Processes & Protocols

Limelight continuously implements, reviews, and updates its policies, procedures, and protocols as the needs of the business adapt and evolve. The previous sections provide a more general discussion of Limelight's Information Security Program, as well as security features in Limelight's suite of services in the edge cloud platform. This section, on the other hand, addresses specific processes and protocols related to Information Security.

9.1. Physical Security

Limelight operates a globally distributed, high-performance private network over which Limelight provides a multitude of services. Physical security refers to all activities, processes, and protocols concerned with the protection of Limelight operations and the prevention of harmful actions, internal or external in origin, from impacting the service.

9.1.1. Offices

We have offices in nine countries globally to support a distributed workforce. No single location is critical to the functioning of the service or for the running of the Enterprise. Each location has redundant power and network connectivity sources, physical security, and access control.

9.1.2. Building & Environmental Security

Limelight's global headquarters is located within a Class A, professionally managed building with 24x7x365 professional security. Access is badge-restricted with access controlled at all doors into the main floors. Access is further limited by function and role within the floors, and overall access is restricted. The building manager for Limelight's global headquarters maintains strict fire-evacuation procedures.

9.1.3. Fire Prevention & Power Continuity

All office locations are managed offices that comply with relevant local laws pertaining to fire suppression and evacuation. Fire regulations are adhered to, and local authority certifications are displayed in each location.

Limelight's global headquarters in Arizona, USA, employs an uninterruptible power supply (UPS) with extra battery cabinets to allow for a seamless transition to a secondary NOC in the event of a power failure at the global headquarters building. A secondary NOC is maintained as a *warm standby* in a location accessible from the global headquarters building but distant enough to be locally isolated from any incident that could impact access or functionality of the headquarters building.

9.1.4. Business Continuity

All office locations are independent of one another, and none are critical to the functioning of the business or the service customers use. In the event that an office location (or locations) does not function properly, employees are enabled to connect and work remotely. This process is periodically tested. Business services continuity is ensured by resiliency and redundancy factored into the network and supplied business systems.

9.2. Data Centers

9.2.1. Locations

Limelight leverages a globally distributed network of colocation facilities at Tier 3/4 carrier-neutral data centers in order to deliver the edge cloud platform. These colocation facilities are necessary for the operation of Limelight's global network and are generally operated by large enterprise service providers with years of industry-standard operating experience.

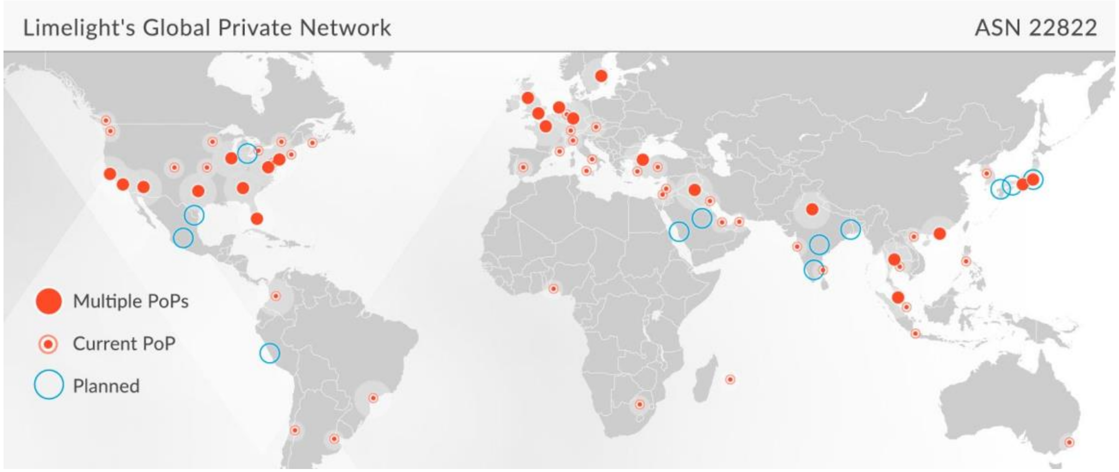


Figure 5: Limelight's globally distributed network

9.2.2. Building & Environmental Security

Physical security at colocation facility data-center locations is a multi-tiered approach that typically includes:

- At least a 22-foot high wall that surrounds the perimeter of the property providing a physical barrier to unauthorized access
- Multiple Closed-Circuit Television (CCTV) cameras that record 24x7x365 with real-time observation, with every entry portal having a dedicated camera
- A mantrap entry point at the security bunker with anti-tailgating technology to control access
- A multi-tiered biometric access system
- All doors are alarmed and cannot be propped open beyond a predetermined interval
- All data-center tenant rooms are individually locked and have the same multi-tiered biometric access controls at every doorway.

9.2.3. Fire Prevention, Power Continuity, & Climate Control

Colocation facilities that house Limelight equipment contain fire- and smoke-detection and suppression systems. Each facility also typically contains:

- Industry-standard dry pipe pre-action sprinkler system
- A gaseous fire-suppression system
- Redundancy that allows for maintenance and unexpected outages to the Computer Room Air Conditioning (CRAC) units that condition the environment. At a minimum, N+1 redundancy is maintained, and in many cases that number is exceeded
- Very Early Smoke Detection Alarm (VESDA) systems
- Power that always consists of three elements to ensure uptime:
    - Utility power in some locations is redundant and delivered from a separate grid
    - Generator power in most locations is provisioned at N+1 redundancy or greater
    - Uninterruptible Power Supply (UPS) power is at a minimum provisioned at N+1 redundancy to bridge the transition from utility power to generator power in the event of a utility failure.

9.3. Email Security

Limelight information systems use commercial email software services, which provide a suite of security features to protect against viruses, malicious scripts, corrupt files, phishing scams, and spam. All employees must use Limelight-provided email services to maintain the required level of protection against such attacks.

9.4. Virus Protection

Limelight's approach to virus protection and mitigation depends on the systems and processes that a host supports. Limelight has anti-virus application software installed for instant virus protection. Anti-virus software is loaded on Limelight computers and configured to scan for viruses on all data and software before being downloaded to any system. Limelight regularly monitors, updates, and reviews anti-virus software to address any events that may occur and to ensure up-to-date protection.

Access to all corporate resources are restricted by controls that block any access to a device that either does not have the approved anti-virus agent installed and running or if the agent is out of date.

Limelight deploys multiple anti-virus controls where anti-virus software cannot be implemented due to lack of commercial availability. These controls include highly abstracted operating system (OS) implementations using a highly customized, proprietary OS with no user interface, advanced configuration management, and active intrusion detection and prevention technologies that detect and quarantine any file or traffic profile changes. Limelight minimizes the risk of a material virus impact through the combination of anti-virus controls and the deployed highly abstracted OS.

Appendix: Document Version History

Version	Effective Dates
2.0	August 2020 - present
1.0	June 2017 – July 2020