Gateway Security

The MultiSight Gateway is an appliance running an embedded Linux® operating system. The system does not support direct end-user access or OS level interaction thus minimizing security vulnerabilities. Unnecessary services and ports are turned off under normal operation to minimize security vulnerabilities.

Software updates and security patches are applied to the MultiSight Gateway via instructions from the MultiSight Cloud. The gateway queries the MultiSight Cloud database for a software version number and when updated applies a software update downloaded from a trusted location. MultiSight Camera updates are applied in a similar fashion, with the gateway acting as a proxy for the camera software update.

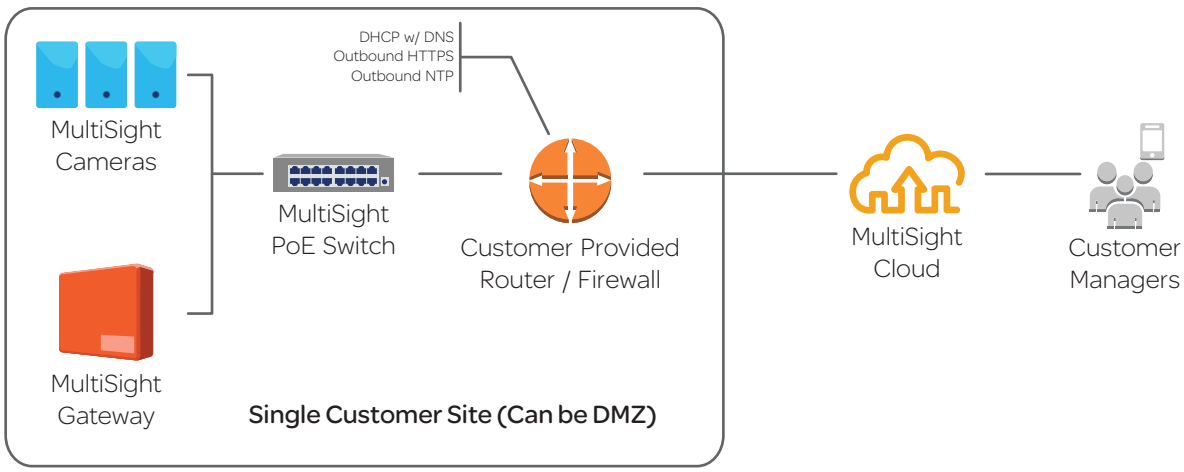

Figure 1: MultiSight On-Site Architecture

The MultiSight Gateway does not accept inbound network connections from the public Internet. Only two communication paths are necessary between the MultiSight Gateway and any outside devices:

1. Communication to the MultiSight Cloud are initiated via outbound HTTPS connections from the MultiSight Gateway to the MultiSight Cloud.
2. Communication between the MultiSight Gateway and the MultiSight Cameras on the LAN are via discovery of the camera's SSDP advertisements, followed by an RTSP connection initiated by the gateway to the camera.

The MultiSight Cameras never communicate outside the LAN to the internet.

With the exception of communication between the MultiSight Gateway and MultiSight Cameras, MultiSight requires no network communication on-site. Thus customers may chose to provision a DMZ explicitly for MultiSight's LAN operations which isolates any potential security threat presented by MultiSight devices from their local networks. If necessary, network traffic can be limited to outbound HTTPS and NTP to *.multisight.com.

The on-site LAN network services required by MultiSight are:

- IP and DHCP service from the LAN network router
- HTTPS to *.multisight.com
- NTP to *.multisight.com
- DNS as specified by the LAN network router

Communications Security

All communication from the MultiSight Gateway to the MultiSight Cloud is encrypted.

No ports need be opened inbound to a site to facilitate operation of MultiSight.

All communication with the MultiSight Cloud API requires authentication credentials and is session based, or in the case of a MultiSight Gateway, requires the installation of a per-gateway security token that is installed on the gateway upon installation.

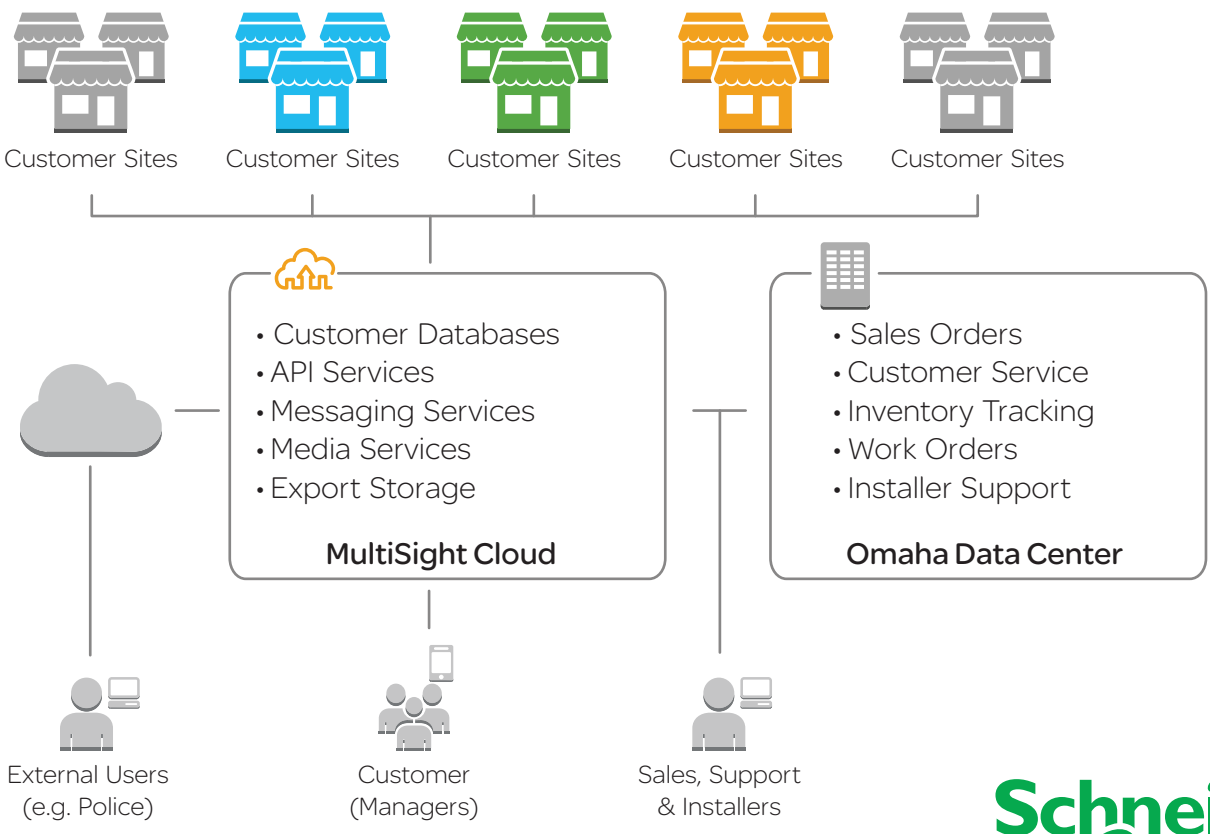

Figure 2: MultiSight Communications Overview

Communication between a MultiSight Gateway and MultiSight Client is via the MultiSight Cloud API, and not direct. The MultiSight Cloud API is a proprietary and unpublished protocol only available via NDA.

Note: there does exist an optional "local mode" to facilitate direct communication between a client and gateway when they coexist on the same network in order to avoid traversing the internet during high bit-rate streaming. This local mode can be disabled. In "local mode" the MultiSight Client and Gateway must still connect to and authenticate against the MultiSight Cloud and use the API for communication--only streaming is local.

MultiSight Cloud Security

MultiSight Cloud is operated on Amazon Web Services, and enjoys many of the security benefits built into the AWS infrastructure. Amazon's security features are documented in the following whitepaper:
http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

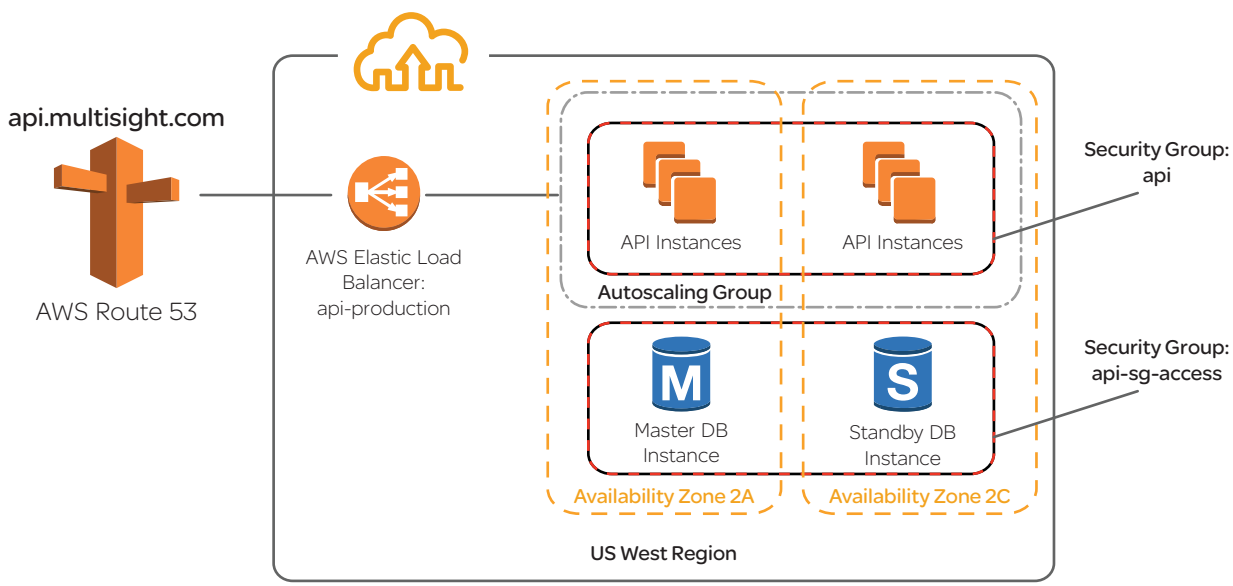

Figure 3: Example API Service using Security Groups

MultiSight Cloud EC2 instances and services make use of AWS security groups to only permit communication between internal services that are necessary for application operation.

A limited number of MultiSight development and operations staff can access MultiSight's Cloud infrastructure via certificate based authentication.

MultiSight software updates and artifacts are distributed via AWS CloudFront and are explicitly limited to access from only those countries in which MultiSight is sold and operated. Countries with known hacking activity such as Russia, North Korea, China, etc., are blacklisted.

MultiSight customer client logins are assigned to organizations and partitioned via entitlements within the MultiSight database. Customers within different organizations cannot access each others data.

Public internet facing MultiSight Cloud services follow OWASP guidelines.