Refraction Point Inc.
340 S Lemon Ave #5258
Walnut, CA 91789
United States

# Core Concepts

limacharlie.io

This document outlines core concepts for those getting started with LimaCharlie's endpoint detection and response platform.

Any questions related to this document, or the LimaCharlie platform in general, can be directed to: answers@limacharlie.io

# Endpoint Detection & Response (EDR)

LimaCharlie is a cross-platform endpoint detection and response solution delivered as a serverless utility. It provides a real-time connection to endpoints where activities are monitored against a set of rules to determine if an automated action or an investigation is warranted.

A software sensor - or agent - installed on the endpoint maintains a persistent TLS connection to the cloud where events are monitored and evaluated. Round-trip times for a detection and response to take place are generally under 100ms.

The total footprint of the agent on disk combined with what is in memory is approximately 2MB. The agent typically runs under 1% CPU with small spikes around certain events and usually uses less than 50MB of RAM.

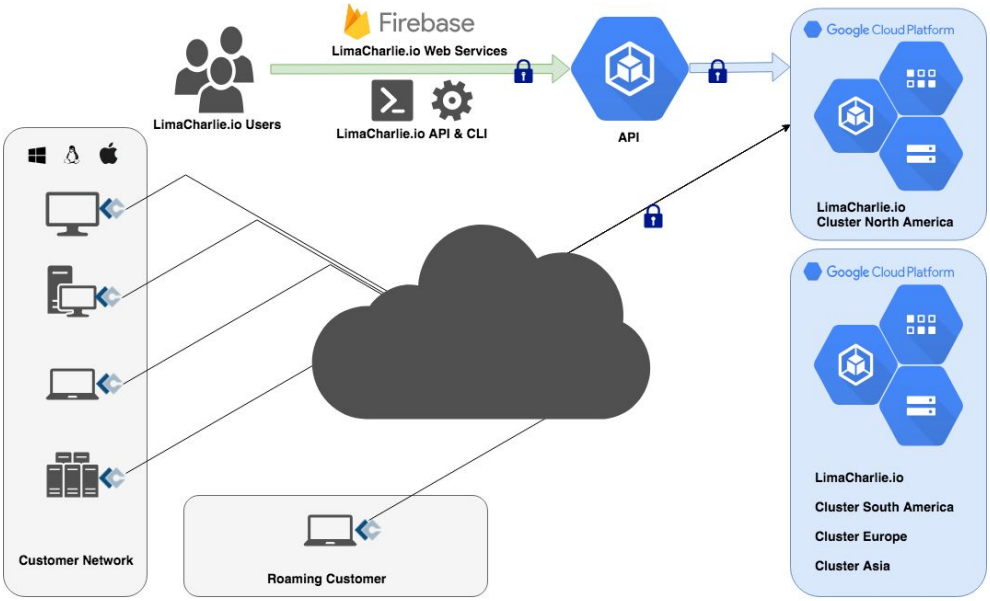
The amount of data that is produced by the agent is dependent on how much, and what kind of activity is taking place on the endpoint. That being said, the average data produced per endpoint across thousands of deployments is approximately 1MB per day.

The LimaCharlie agent has zero impact on endpoint performance, even when analyzing, searching and investigating incidents. The agent deploys in seconds with no reboot required and will not be picked up by antivirus software (it does not hook into the kernel and abides by all APIs).

Agents support Windows XP and up, MacOS and Linux distributions across x86, ARM and MIPS architectures (32 & 64 bit). Custom builds of the agent for OpenBSD and Solaris can be made upon request.

# Architecture

LimaCharlie employs a multi-tenant architecture built on top of Google Cloud Platform.




Security is of the utmost importance, which translates into multiple levels of security.

Every cluster is built across multiple availability zones to maintain high-availability. Clusters are available in multiple regions to deal with any legal requirements and all access to these clusters is transparent, allowing MSSPs to provision new customers wherever they see fit.

Connectivity between agents and the clusters is done point-to-point and is secured using pinned SSL certificates.

This enables extremely easy deployments and seamless transition of assets between offices and networks.

Each cluster has its own transport keys and each organization has its own command keys. All keys are encrypted in storage and runtime access to the envelope keys is limited to server containers. All sensitive output configurations are encrypted per organization.

# High-level Concepts

The first concept to understand is the concept of an Organization. Each of the following types of objects are managed per-organization:

- **Agents** belong to a specific organization.
- **Installation Keys** are keys used to enroll an agent within the organization.
- **Outputs** are forwarding rules for parts of the data generated by an organization's agents.
- **D&R rules** are automation rules used both to manage agents as well as to perform automated Detection & Response and are managed by organization.
- **API Keys** are secret keys you use to interact with our API and are limited to the scope of an organization.
- **Quotas** are simply the maximum number of agents that may be online at one time for an organization. There is no minimum and it can be adjusted at any time.

Billing / quota is also managed at the organization level. This means that in most cases, you will want to use one organization for one customer. This makes billing, onboarding, management and termination much easier.

Users are simply accounts on LimaCharlie and are identified using an email address. A user can be granted access to multiple organizations and an organization can have multiple users associated with it. Users having access to an organization are also able to transitively grant access to other users. Obviously everything is logged, auditable and the logs can be transmitted to an archival facility in order to be tamper-proof.

Advanced role based access control is available to help manage the various types of users under an MSSP's control.

Organizations can be created at will and always include a free tier (2 sensors). This makes it easy to streamline a small proof-of-concept with a new customer and simply grow it as needed when they begin wider rollouts.

All accounts have an initial limit on the number of organizations they may create. If you need more simply get in touch with us and we will increase your limit.

# Onboarding Checklist

This checklist is meant as a discussion on topics that are relevant prior to onboarding a new customer.

### Organization

Adding new organizations is simple. Organizations are free and begin with a two agent free tier. If you hit the maximum number of organizations just get in touch with us and we'll increase your limit.

Scaling up and down as well as granting access to an organization is easy. This means the first step to onboarding a new customer, even if only for a trial, should be to create an organization.

### Users

LimaCharlie supports role-based access control (RBAC) for user accounts. Through the web interface you can create additional users while controlling what it is they are able to see and do. Use pre-built access control templates designed for account owners, administrators, operators, view-only or create your own.

### Installation Keys

The Installation Keys (IK) are used to enroll new agents. One IK can be reused as many times as you want and it remains valid until it is deleted. Agents that are already enrolled will keep their access but new agents will not be able to enroll with the deleted key. This model makes it easy to revoke keys and maintain tight control over installer agents.

The main reason to have multiple IKs is to associate tags with agents. Each IK has a list of tags that are attached to agents enrolled using it. For an MSSP this provides an easy first pass at categorizing agents.

For example, you may create an IK with tag “server”, and another with “desktop”. Then it is just a matter of asking your customer to use the relevant IK for the various assets.

Tags can also be added/removed either programmatically or interactively after enrollment.

### Outputs

The Outputs is the component forwarding the data to your infrastructure. The data is composed of three main streams.

1. Event
2. Detect
3. Audit

The audit stream allows you to choose where you want to store a copy of the audit messages. It is not technically required but we recommend sending it to a write-only location like an AWS S3 bucket.

Next is the detection stream. This is high priority data and you will want it to go to a live system rather than an archiving one. It is common to send it to the SIEM or a product like Splunk.

If you find some of the detections to be overly verbose you can also customize the outputs so that only certain detection types go to a cold storage and others to a live system.

Finally, the event stream is by far the most verbose. It contains the raw events coming from the agents. Most cost-conscious MSSPs will, as a general rule, send all the events to cold storage. A popular method is to use an AWS S3 bucket with a retention period set (like 3 months), and to upload data to it with compression enabled.

The event data is very verbose so that it can be easily used operationally, but it also compresses extremely well (~90%). So for cold storage, enabling compression is a good idea.

Another common setup is to tag sensitive agents as “vip” and configure an Output to send the event stream from these agents to a live system like Splunk so that it is always readily available.

### Insight [telemetry storage]

Long-term telemetry storage with search capability is available as an optional add-on. LimaCharlie still operates as middleware but with this feature enabled we offer one year of storage and search capability for a small additional cost. This move allows MSSPs and SOCs who do not already have their own EDR infrastructure to gain a completely functional information security centre upon signing up.

Once enabled, LimaCharlie Insight will automatically send all telemetry data to secure storage on the Google Cloud Platform. The Insight user interface allows you to select a date and time from which to start and then perform complex investigations.

### Automation

The first few organizations you onboard will likely be done manually. But you will quickly want to clone your configuration and store it for use setting up future organizations. LimaCharlie provides tools to export your configuration and store your “infrastructure as code”.

Using the sync tool part of the Python API, you can backup an organization’s configuration as YAML files and organize them so that you re-use base configurations across all your customers.

The tool will allow you to export to YAML and apply the YAML back up to the cloud. This results in a more efficient onboarding process and a better repeatable process.

For a more complete discussion, see the related blog post: Infrastructure as Code

## Additional Resources

Full documentation can be found here: doc.limacharlie.io

REST API documentation via Swagger here: Swagger Doc

Free online course here: edu.limacharlie.io