

iDefense

Verisign iDefense is a closed-source threat intelligence feed available to all Lumeta customers. This feed correlates iDefense IPs against your network's IPs to produce actionable lists of zombie devices and threat flows in your network.

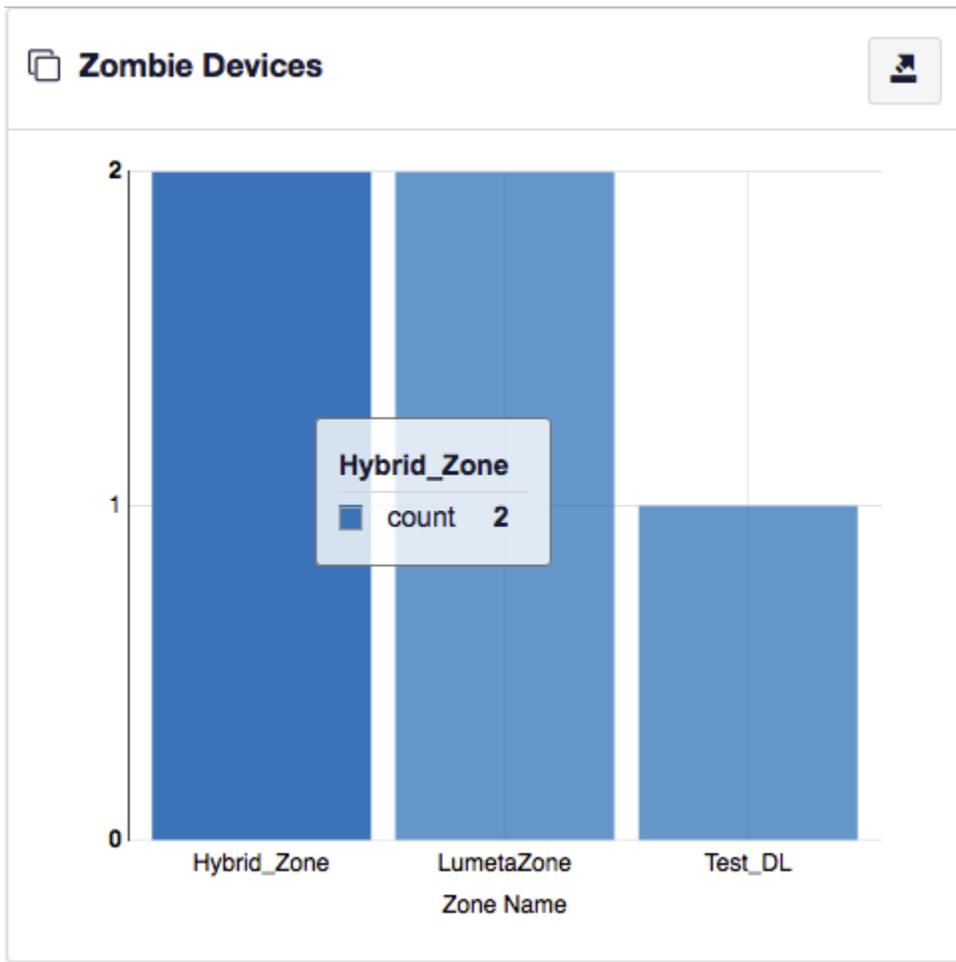
To use iDefense, you'll need the iDefense license key provided by Lumeta. Look for this key in the original welcome email message you received from Lumeta Support. If you can't find your iDefense key, please [contact us](#).

To produce threat flow results, you'll need a single source of NetFlow data such as Gigamon NetFlow. Lumeta can receive NetFlow from a single source. If you have multiples, consider using a NetFlow aggregator. You will also need to direct the NetFlow results to your Lumeta Command Center. These topics are out-of-scope for Lumeta documentation, but your [Solutions Architect and Support](#) can nevertheless help with implementation.

Threat Flows							
Destination IP	Source IP	IP in threat	Threat Attribute	Source Port	Destination Port	Protocol	zonename
65.246.245.11	93.174.93.181	93.174.93.181		50783	22	TCP	Hybrid_Zone
65.246.244.14	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.246.100	93.174.93.181	93.174.93.181		50783	22	TCP	Hybrid_Zone
65.246.242.134	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.241.135	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.244.4	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.246.128	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.244.87	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone

Records 1 — 20 of 380 Page 1

To show the zombie devices in your network, you do not need NetFlow data. This dashboard is generated using native Lumeta-indexed data.



The iDefense feed is correlated against NetFlow data. The intersection of the two populates the threat_feed_ip table. Browse to **Settings > Tables > threat_feed_ip > View** to open the table.

To configure the feed . . .

1. [Enable the capture of NetFlow data.](#)
2. [Configure and enable iDefense in Lumeta.](#)

Enable NetFlow

The NetFlow-capture service enables your Lumeta Command Center to ingest NetFlow data.

To enable NetFlow capture from the Lumeta GUI:

1. On the Lumeta main menu, browse to **Settings > Support Tools > Status of Lumeta Components.**

