

# DataDefender

## Reliable Transport of Critical Data

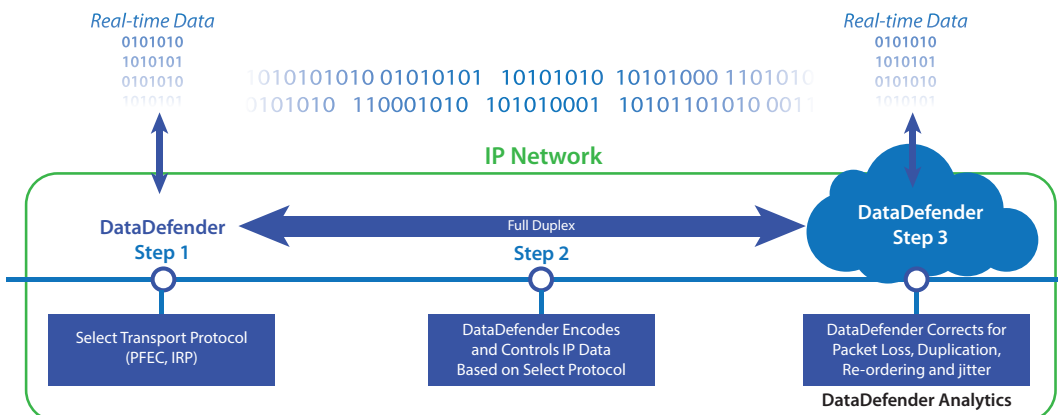


One of a network administrator's biggest challenge is to ensure the delivery of mission critical data to its destination reliably and with complete integrity. Whether it is data going to a soldier in the field, earth observation imagery downloaded to the cloud or shipment data going to a supply chain--latency, jitter and packet loss aren't an option. Anything other than 24/7 reliable data transmissions can be extremely costly. But how can a network administrator successfully transport mission critical data over impaired network links?

DataDefender is an easy to implement network protocol utility that delivers the quality transfers needed for critical applications. These crucial operations include anything from online banking systems to GPS systems used in remote military operations.

### Assured Traffic Delivery

With DataDefender, administrators are assured lossless network performance. DataDefender allows the administrator to select the transport protocol protection that best fits the application. Based on the chosen protection protocol, DataDefender encodes and controls the IP data, then corrects for packet loss, duplication, re-ordering and jitter to deliver the critical data.



### Flexibility to Configure Your Network For Secure Transport

**Packet Forward Error Correction (PFEC)** corrects lost packet errors on one way transmissions while maximizing bandwidth and keeping latency low. This results in an optimized, reliable data stream.

**Intelligent Retransmission Protocol (IRP)** is for bidirectional data transfers. It prevents loss of data while reducing overhead caused by retransmissions. This guarantees data delivery when latency is not a concern.

**Application Specific Streams** are created to support data transfers for specific applications, managing bandwidth, latency and packet errors only during an actual transfer. This results in precision support that can be applied to mission critical data without creating reserved bandwidth that cannot be used by other traffic/applications.

DataDefender streams support specific application data transfers, assisting critical network needs at the precise time they are required. This allows other traffic and applications full use of the circuit when no stream is operating.

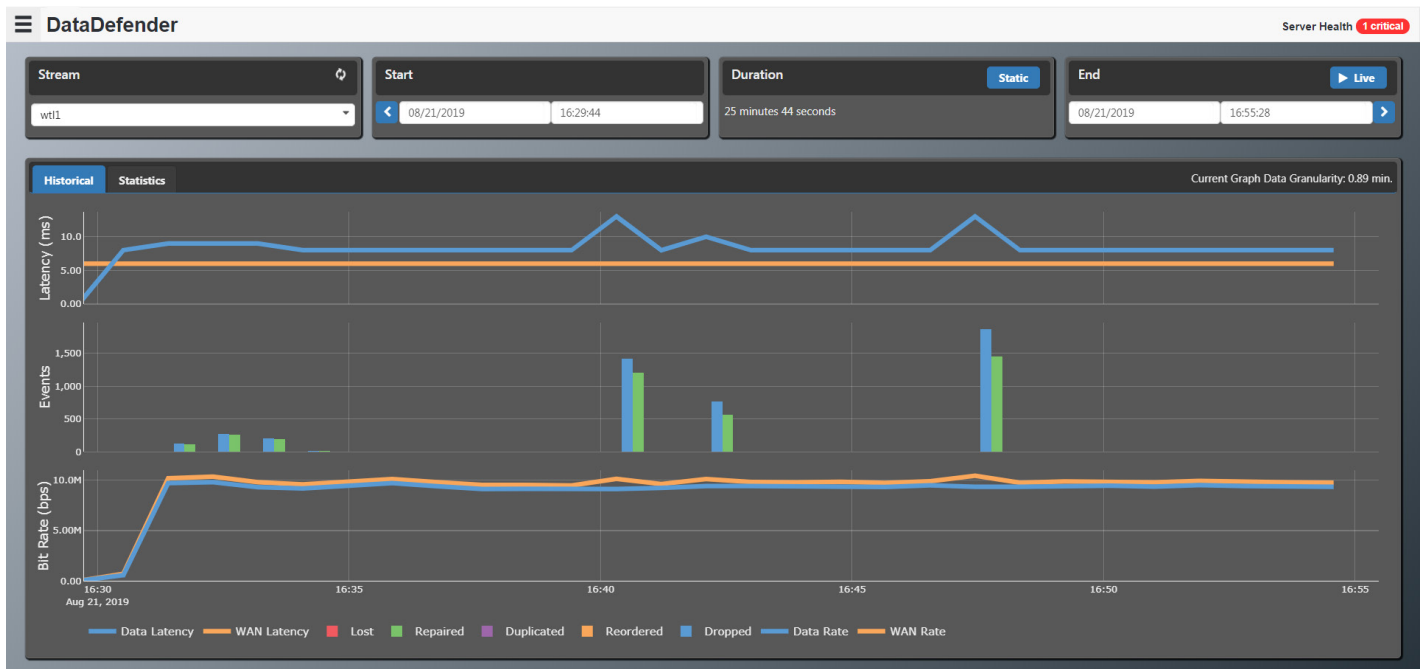
### Lower Overhead Costs

DataDefender can be deployed on your existing architecture—eliminating the need for new infrastructure and potential non-recurring engineering (NRE) charges. This ensures that all mission critical application data, including the ones that exist on legacy systems, will be reliably transported.

The product is available as a virtualized cloud solution that can be deployed rapidly and reliably. Additionally, it can support the latest security, encryption and WAN protocols. Because DataDefender can be deployed as a virtualized solution, network administrators can cut down on support and overhead costs.

### Increased Visibility into Your Network

DataDefender also provides visibility into data transport and performance by displaying errors and corrections at a sub-second measurement. This increases a network administrator’s ability to identify and isolate network problems.



*Sub-second display of packets dropped/repaired and WAN throughput*

### DataDefender Virtual Appliance

When hosting DataDefender on premise or in the cloud, these are the recommended server requirements that will support the number of protected streams as identified in the stream count.

Minimum Suggested System Requirements						
VNF	Stream Count	LAN Interface	WAN Interface	CPU	RAM	Storage
100 Mbps	10	1 Gbps	1 Gbps	1 x 2 GHz	8 GB	1 TB
1 Gbps	50	1 Gbps	1 Gbps	1 x 3.6 GHz	24 GB	1 TB
10 Gbps	100	10 Gbps	10 Gbps	4 x 3.1 GHz	192 GB	1 TB