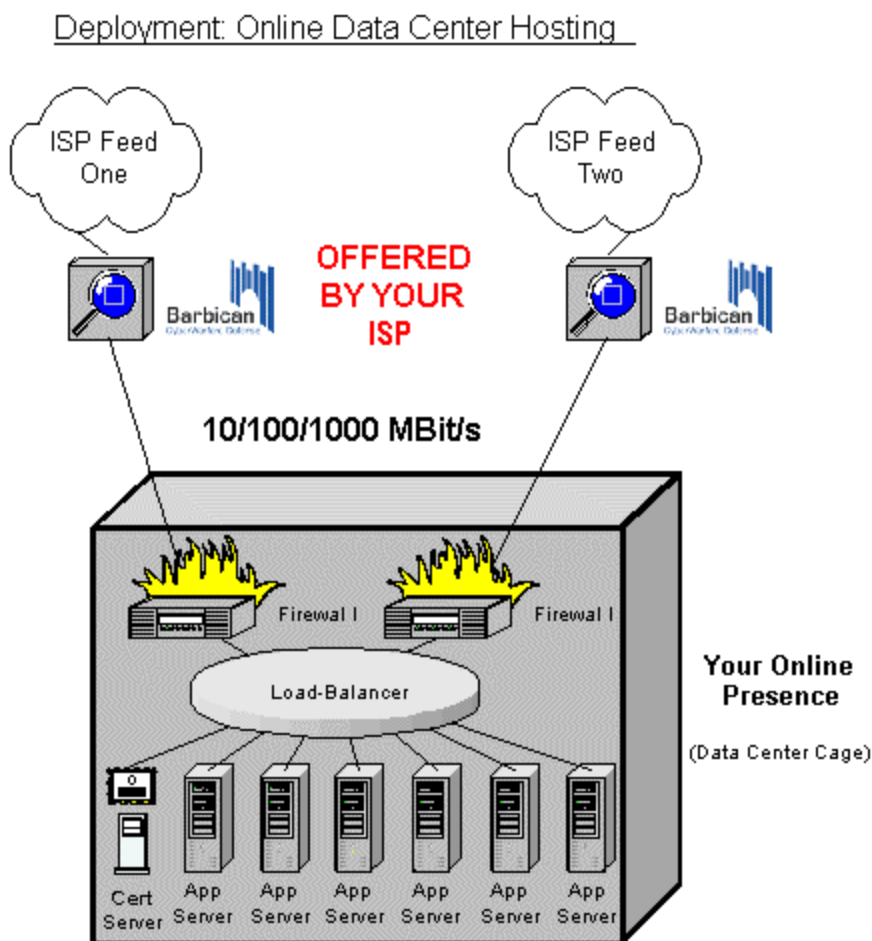


## Example 1: Barbican RNP Deployment defending Online Hosting

This document discusses the setup of Melior's Barbican RNP CyberWarfare Defense product to defend your online presence in a data center setup.



Most online presences for content web sites and e-commerce applications are hosted in data centers, in which the customer rents space in cabinets or cages for their own equipment, and ISPs provide Internet connectivity typically by way of 100 Mbit/s or faster Ethernet connections on copper or fiber wiring.

The customer's infrastructure setup is usually fairly similar: firewalls protect against basic attacks and limit the number of TCP, UDP, and ICMP ports, on which the outside world can communicate with the systems deployed in the customers' space, and a variety of network- and load balancers, as well as a number of application servers.

Location of any online presence is usually chosen for environmental redundancies, as well as for availability of a multitude of Internet feeds.

[www.dDoS.com](http://www.dDoS.com)

The customer pays for the space used within the data center (fixed cost), as well as for the amount of traffic delivered to and from the infrastructure by the ISP (dynamic cost). Usually the dynamic bandwidth cost has a fixed minimum price (subscription rate), with the capability to „burst“ from the minimum rate to the full capacity of the medium (the „pipe“).

If the customer comes under „bandwidth flooding“ dDoS attack, the amount of traffic delivered to the pipe typically goes to the maximum, resulting in saturation of the pipe by invalid traffic, thus overwhelming the transport capabilities through the pipe, and resulting in maximum revenue for the ISP. For the revenue aspect, no ISP has a business interest to defend the customer against such Denial-of-Service attacks (and Service Level Agreements –SLAs- typically exclude dDoS attacks), nor does the customer usually have other leverage to request action to be taken by the ISP without compensation.

In order for **Barbican RNP** to defend against all attacks (see brochure on „Attack Protection“), including the costly flooding of the bandwidth pipe, it must be installed „upstream“, i.e. on the ISP end of the traffic delivery medium, prior to the point of measurements for bandwidth cost.

To provide the ISP with a business incentive, ISPs typically prefer to purchase **Barbican RNP** units, and offer their deployment and usage as a premium service to the customer, to offset the lost revenue for the additional dDoS, PenTest, and junk traffic.

As a customer, you would want to choose your co-location provider from a list of ISPs, who deploy and offer **Barbican RNP CyberWarfare Defense Solutions** as an add-on service. If you already have an online presence in a co-location facility, and your ISP is not on the list of Melior resellers or premium providers (see our web site), you may want to work with your ISP to consider offering this defense as a premium service.

The cost benefit is obvious: compare the rates of ongoing bandwidth cost exceeding your monthly subscription rate, and the cost of damages, outages, and vulnerability exploitation (PenTest - against which your current security measures do not defend) against the cost of **Barbican RNP** units (or their premium service cost by the ISP).

You will find **Barbican RNP** amortizes very quickly.

For additional cost / benefit data, please contact your local reseller or Melior, Inc.'s sales department.