

## White Paper:

# Securing the Cloud, A Perspective

Andrew MacKay, Chief Technology Officer, Superna  
Michael Arno, President and CEO, Superna  
Ottawa, Canada - [www.superna.net](http://www.superna.net)  
June 2011

### Abstract

*As the options expand to the Enterprise for hosting and cloud services, there is increasingly a need to better secure the wide area network. This paper looks at the state of WAN based encryption and discusses solutions to secure the on ramp for hosted services.*



### A Period of Change and Innovation

#### *Rapid changes in the telecom market*

There has been significant change in the communications industry over the last fifteen years. The explosion of the Internet fueled the Dotcom and Telecom bubbles of the 1990's. During this time, massive investment in internet infrastructure occurred.

By the end of the 1990s, many service providers found themselves with new modern networks, but little understanding of how to actually extract value from revenue generating services. Then, by the millennium, the Dotcom economy collapsed. The Service Provider space was in disarray. As quickly as they appeared, many service providers disappeared. By 2005, many service providers retreated and a period of industry consolidation occurred.

*Securing the Cloud*

During this period of perpetual change, the Internet economy continued to evolve at dizzying rates. Fueled by government incentives and market demands, broadband access became ubiquitous. High speed connectivity is now available to everyone. Wireless connectivity options are becoming pervasive, enabling users to connect to each other from anywhere, at anytime. With easy and affordable access to high speed networks, the era of Web2.0 was born.

New applications emerge virtually overnight running “in the cloud” but without any thought about security. Quietly, the bandwidth glut which was created during the Dot-com bubble disappeared. Networks were now at capacity and new network investments are occurring.

*Security creates challenges for all businesses*

This competition also means that small and medium businesses face the same challenges as larger competitors but without the IT budget or skills to properly implement security solutions. At the same time, bigger enterprise corporations strive to reduce their IT budgets. This usually means reduction and consolidation of network infrastructure, centralizing applications and data to locations where IT expertise is located, and reducing the number of unique instances (and costs) of software applications. All of these dynamics have created new opportunities for Service Providers looking to evolve beyond low margin network plumbing providers.

**The Emergence of a New Breed of Service Provider***Hosted MSP's*

The last few years have seen the emergence of a new breed of service provider. Hosted Managed Service Providers (MSPs) provide value added solutions to enterprise and business customers of all sizes. As enterprises shift more and more responsibilities to service providers IDC predicts that the global hosting market will be a \$16 Billion dollar industry by 2011. Fueled by increasing enterprise adoption of outsourced IT, Hosted MSPs will offer services such as application hosting, online business enablement, IT consolidation, and Software-as-a-Service (SaaS).

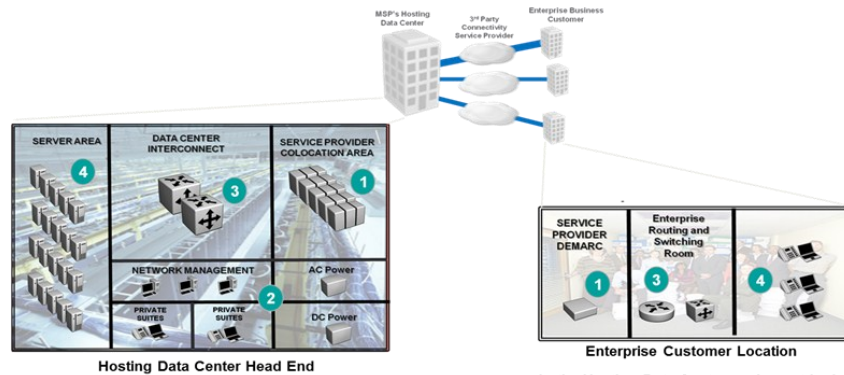
Hosted MSPs own and operate data centers and offer advanced outsourced IT services. Their data centers house servers and storage devices which remotely run applications from many enterprise customers. While some Hosted MSPs also own some network infrastructure (dark fiber network assets), the majority do not.

*Software as a Service*

In order to connect remote enterprise customers to their applications and data, Hosted MSPs must lease bandwidth from 3<sup>rd</sup> party connectivity service providers. The Hosted MSP data center will also include secure co-location areas where multiple service providers will deploy their equipment which is used to backhaul traffic from enterprise customer locations.

The key elements of a Hosted MSP network are outlined below.

*Service offerings from hosted service providers*



- 1 Service providers deploy their service termination equipment at either end of the link between the hosted data center and the enterprise customers. In the data center, many service providers may be present each having a secure co-location area. The enterprise may have a secure area or Telco room. The MSP is responsible for negotiating connectivity with each 3<sup>rd</sup> party service provider.
- 2 The Hosting MSP provides a reliable environment including redundant power, heating/cooling, network management, and secure work spaces.

- 3 In the Hosting Data Center equipment is deployed to provide interconnection between the service provider termination equipment to the servers and storage areas. At the enterprise location, the enterprise manages their own switches and routers to connect manage and connect users to the Wide Area Network.
- 4 In the Hosting Data Center, the MSP deploys server clusters and storage arrays to host applications and data from many different enterprise customers. At the enterprise location, users in their LAN environment access data and applications hosted remotely by the MSP.

*Carrier Ethernet Services*

**The Evolution of Bandwidth and Security Services**

As hosted applications require high bandwidth and high availability, they also require higher levels of security. This requirement can add significant recurring bandwidth lease costs and new investments to secure connections to MSP data centers.

Many of the MSP's enterprise customers purchase all available service, while some purchase only specific services based on their individual needs. The real-time Storage backup is the most popular service, and the most bandwidth intensive. With the current enterprise market trend to adopt more managed services a reality, the MSP expects the growth rate for their services to continue to increase by 84% over the next five years. The MSP's that ensure end to end security of their offering will take larger market share of Enterprise customers looking to outsource applications. Offering an encrypted on ramp to hosted services will differentiate the service in the market.

With the emergence of Carrier Ethernet technology, most 3<sup>rd</sup> party Service Providers offer some level of Ethernet based networking solutions. Ethernet Private Lines are most commonly leased services at this time by the MSP. Furthermore, Ethernet Private Lines are the most technically attractive options given the high bandwidth and service level guarantees they afford. The MSP leases combinations of 100M and 1000M private line services depending on the needs of any given enterprise location.

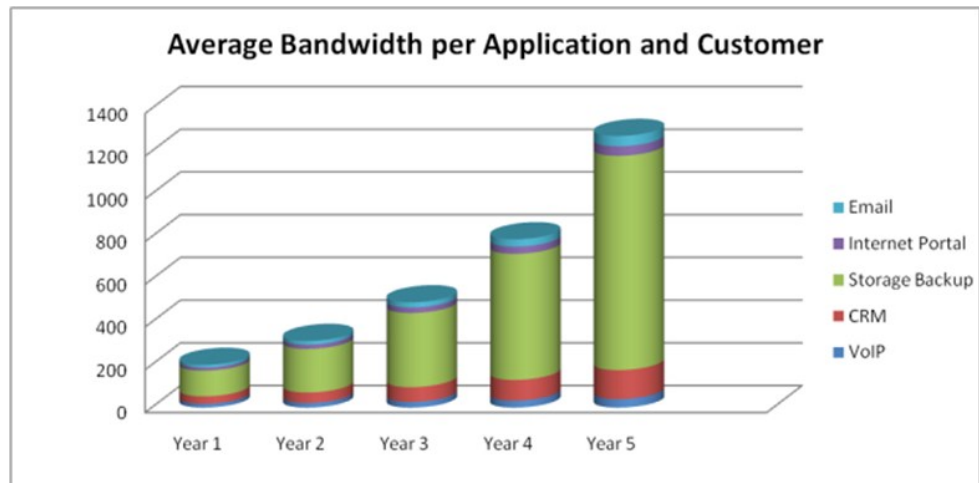
*Wire Rate Encryption Services*

Offering secure solutions is the key objective for all Hosted MSPs. The challenge is often how to do this within the framework of the current service delivery model for the MSP. The other critical challenge for the telecom provider is the time required to move to new service can become an inhibitor to the enterprise adoption. For security services, we have also seen an evolution from IPsec and SSL on a routed network to the availability today of optical security services from several service providers. We are now seeing wire speed encryption available in the market at 1 and 10 Gigabit Per Second speeds.

*Sourcing Encryption service from the Service Provider*

The number one application is storage replication traffic which has a high bandwidth and security requirement. Customers replicate business critical information which is also highly confidential data. Enterprises need to encrypt data transmitted over links to their own data centers and MSP's data centers due to regulations and concerns over data leaks. In order to take advantage of MSP and Cloud offers, Enterprises need encrypted solutions from service providers.

This introduces a challenge when encryption key management ownership dictates that the Enterprise remains in control of the security of their data.



*Encryption as a Service - New Services from the Telecom Provider*

**Case Study – Hosting and Cloud Computing need Encryption**

A large financial institution in Europe had migrated to a centralized Data center model with remote locations connected over Ethernet Private Line from a service provider. The trend to centralize or outsource (Cloud computing) applications separates users from business critical applications over unsecured network links. The customer felt encryption solution was required to secure the links between sites but they need to have control and visibility to the security of the network device encrypted data.



**Network Security Portal, Encryption device with an Ethernet Private Line Service (EPL)**

*Security management and control*

Eventually, this end user worked with the telecom provider to source an **Encryption Service** where the telecom provider provisions and administers the network device, but passes full control of the security event to the end user. The telecom provider still administers the device but enables a separate control plane for the security events and conditions.

The end user's security requirements:

- ◆ Separate device monitoring and management from security management.
- ◆ Separate GUI for managing security for the Security organization.
- ◆ Separate user login for security management with role based access.
- ◆ Encrypted connection to network elements.
- ◆ Scheduled key rotation based on corporate standards.
- ◆ Network wide view of all devices performing encryption.
- ◆ Ability to integrate with 3<sup>rd</sup> party key management platforms.

*Network Security Portal for Advanced Key Management*

The customer deployed the Superna Network Security Portal (NSP) to meet all the requirements above. As the customer planned key management solution for data at rest, they were interested in integrating network key management with a broader enterprise solution, which NSP solves with future KMIP northbound support.

NSP reduces the barriers to outsourcing expensive encryption devices for service providers. The NSP allows the Service Providers to acquire encryption as an Operational Expense versus Capital Expenditure, while retaining control of information security. NSP can rapidly integrate support for any encryption device with off board key activation interface.

NSP has been deployed in military, financial, government and business consulting market segments and has been integrated by several equipment makers in the Enterprise and Optical market segments into their encryption market offerings.

*About Superna***About Superna**

Superna is a network security solution provider with expertise in optical and storage area networks. The Superna **Network Security Portal** is used by service providers to offer Encryption as a Service to enterprises and provide a dashboard for security events. The Storage Area Network Qualification service helps network equipment manufacturers to qualify the interoperability of their WAN network solutions to meet EMC and Brocade standards and requirements.

For further information , please visit [www.superna.net](http://www.superna.net). You can follow Superna on:



Superna **Blog**: [feed://supernanet.wordpress.com/feed/](http://supernanet.wordpress.com/feed/)

**Twitter** at <http://twitter.com/SupernaNet>;

Superna on **Facebook** <http://www.facebook.com/pages/Superna/216795221678598?sk=wall>

Superna **YouTube** Channel <http://www.youtube.com/user/superna100>

**LinkedIn** <http://www.linkedin.com/company/856558>