

# Managed Web Security Services Overview



2/8/2008

V1.0

Suite 238, 3553 31st Street N.W.  
Calgary, Alberta T2L 2K7, Canada  
Tel. +1.403.276.5356. Fax. +1.403.276.5568

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

---

## Table of Content

<b>Market Overview .....</b>	<b>3</b>
<b>Features of a Web Security Solutions .....</b>	<b>3</b>
<b>Key Product Requirement - Performance.....</b>	<b>4</b>
<b>Services Overview.....</b>	<b>4</b>
<b>Web Security Financial Model .....</b>	<b>5</b>
<b>Conclusion .....</b>	<b>6</b>

## Market Overview

Today the Web is an essential resource for many businesses. Enterprises of every size rely on the Web for communication, research, marketing and everyday operations. By enabling productivity-enhancing tools and advanced business applications, the Web has fast become one of the quickest and most economically viable ways for organizations to grow and compete on a grand scale. With the adoption of the web, the threats associated with web applications continue to grow, targeting end-point devices, users, web applications, with the motive consistently being data theft and financial gain. Security technology budget decisions are based on the solutions ability to protect these web applications and its users. The driver for adoption is based on Legal/regulatory requirements like Sarbanes Oxley, GLBA, HIPAA, PCI and many other regulations. As these compliance programs become increasingly complex it creates opportunities for new technologies like the [BeSecure Web Gateway](#) to provide a new breed of solutions to Detect, Block and Defend against web threats.

## Features of Web Security Solutions

The optimal Web security solution delivers a comprehensive and customizable suite of protection services including Web virus scanning, Content Control, Web filtering and the ability to extend security policies that include Detecting, Blocking and Defending.

### *Web Virus Scanning*

To successfully defend against increasingly sophisticated and complex Web threats, an enterprise should proactively protect its network. An effective Web Virus Screener should be up-to-date, offer multiple layers of scanning, deliver real-time protection against browser vulnerabilities, and provide comprehensive statistical analysis and reporting.

### *Content Filtering*

Content Filtering is a set of individual processes that allow you to gain access and control over the way your resources are used. This is achieved by employing a variety of filters, each serving a specific purpose. These filters analyze the content, in real-time and then take appropriate action. Content filtering rules are based on the structure of the data and the importance of the data (Example: social security numbers, credit card numbers, bank accounts etc).

### *URL Filtering*

Customized Web Filtering puts the enterprise in control of how employees use the Internet. Easy-to-use tools enable employers to create, enforce and monitor a clear and comprehensive Web usage policy. Web Filtering can preemptively categorize Internet search results and block specific file types in accordance with the usage policy.

The [BeSecure Web Gateway](#) provides customer with the ability to apply the required policies to its Web Filtering, Content Filtering and URL Filtering.

*Detecting:* Consists of policies that detect conditions or violations in security policies that could lead to security breaches. The detection is logged and reported to the network administrator to allow interpolation of the data.

*Blocking:* Services that block ingress/egress attempts at data leakage, based on the policies defined in the content filter. Blocking technology can disallow traffic based on URL, file size, compliance requirements and time of day for both inbound and outbound traffic.

*Defending:* Comprised of products or services that defend against Malware and other virulent code that could cause havoc to end-point devices, users, or web applications. The common denominator for these products is their multi-purpose approach to threats by detecting and eliminating malicious code upon detection.

## Key Product Requirement - Performance

One problem of past methods of Web Security is the reduced network performance as a result of the time required for content reconstruction, inspection, and manipulation. Generally, network performance can become severely compromised when there are many users accessing large volumes of compressed content. As the exchange of large archived content is common practice over today's data networks, the inspection of such content can be highly inefficient at times. For example, when there is a new release of popular software, digital images, videos, ring-tones, and other compressed content that is being accessed by a large number of users within a relatively short time period on a network.

[Wedge Networks' Network Data Processor \(NDP\)](#) platform is the architecture for building high performance, robust, and future proofing [Web Security systems](#).

There [NDP](#) architecture consists of 3 primary layers:

- *Services Layer*– Content security inspection algorithms are implemented at the service layer by using the [best of breed partners'](#) proven solutions. The integration of partners at the service layer ensures the most accurate content inspection in the industry, and effectively addresses the “Emerging Threat Issue”.
- *Data Layer* – Supports multiple application protocols, such as HTTP, SMTP, POP3, IMAP and FTP, while managing multiple data sessions to ensure that all data is routed to the service layer to be scanned prior to the release. The data layer incorporates some proprietary techniques, such as
  - [Subsonic technology](#) (PCT/CA2007/000020, USPTO 11/620,556): which addresses the performance and stability issues of developing NBCI systems for today's data networks
  - [Green Stream technology](#): which addresses the stability issues caused by the network characteristics within a hydrogenous system
  - Protocol Factory technology: which addresses the “Emerging Protocol Issue”
- *Control Layer* – manages the content inspection policies. The content inspection results are reported to the control layer to allow for reporting. The administrator can use CLI, Web Interface, XML over HTTP, SNMP, and syslog interface to manage the operations of the [NDP](#) devices. In addition, the control layer supports the ease of deployment in different network setups with high availability requirements.

## Services Overview

[Wedge Networks BeSecure Web Gateway](#) offers several options for hosting companies to position Web Security as a solution for its customers and a revenue generation tool. Two options that are used for messaging solutions are “Hosted Security Service Provider” and “Managed Security Provider”. In both cases, the performance offered by the [BeSecure Web Gateway](#) meets customer requirements and drives the margin required by the hosting company.

*Hosted Security Service Provider (HSSP)* - Managed hosting of security services is a variation of infrastructure outsourcing, where clients outsource the management of what we call the security technology stack to a managed hosting provider. This model is based on a per user charge per year.

*Managed Security Services Provider (MSSP)* – This involves the resale of the BeSecure appliance to the customer and charge for the management at the hosting center. Enabling the host to offer CPE-based, ITC and hosted security service offerings. Hosting companies have an opportunity to drive more flexible pricing options into the MSSP market or to consider MSSP services to augment any hosting or network services already being procured.

## Web Security Financial Model

The [BeSecure Web Gateway](#) financial model works for companies who want to offer Web Security as a hosted or managed solution based on the BeSecure performance translating into a cost per transaction that is the best in the industry. Listed below are two examples of how the performance of BeSecure translates into a profitable service.

### *Hosted Security Service Provider (HSSP)*

- [BeSecure 2040](#) Proven Performance - A population of 168,000 clients and 600 servers are used to test the maximum throughput of clients retrieving 1MByte HTTP documents. A throughput of 113,229,778 Bytes/sec = 906 Mb/sec is achieved on a Gigabit network when the number of concurrent clients reaches 1,280. The test objective is to validate whether the BeSecure can deliver wire speed HTTP scan performance.
- Hosted Security Services retail of \$24 per user per year.

#### *Revenue*

Performance	Users	Revenue Per User	Revenue per Year
1Giga-bit	168,000	\$24	\$4,000,000

#### *Cost & Profit*

Capital Cost	Yearly AV Costs	Profit	Margin
\$60,000	\$300,000	\$3,700,000	90%

### *Managed Security Services Provider (MSSP)*

- [BeSecure 2040](#) Proven Performance - A population of 168,000 clients and 600 servers are used to test the maximum throughput of 10,000 concurrent (C10K) clients retrieving 32KByte HTTP documents. The test objective is to validate system performance and robustness for very large, eCommerce service providers and enterprises with typical HTTP communication overhead (32KB payload has more handshakes than 1MB payload).

#### *Revenue*

Performance	Users	Total # Clients	Revenue Per Client	Revenue per Year
1Giga-bit	168,000	170	\$60,000	\$10,320,000

#### *Cost & Profit*

Capital Cost	Yearly AV Costs	Profit	Margin
\$30,000	\$2500	\$5,000,000	60%

## Conclusion

The growth of web applications has created a new type of security threat that is designed to take advantage of web application, user and end points for the purpose of data theft. As a result of the increased threats, organizations are mandated to comply to strict security regulations or be found liable for their non-compliance. This has created an opportunity for companies that host these web applications to build a new suite of managed [web security services](#). These services can be very profitable for service providers if the products and services meet the requirements of the customer and the cost per transaction is low.

Wedge Networks [BeSecure Web Gateway](#) offers hosting companies the ability to provide Web AV Filtering, Content Filtering and URL services that will Detect, Block and Defend against known threats and data leakage. The combination of performance, accuracy, [best of breed partners](#) and ease of integration, provides hosting companies with a solution that will meet customer security requirements and drive new revenue.