FROST & SULLIVAN

REDUCING TCO IN ENTERPRISE IT SECURITY

www.frost.com

"We Accelerate Growth"

Contents

The Rise of Integrated Security Management in Enterprise Networks

After many years of having different security solutions embedded in the network, organizations are now beginning to view security as an issue that ideally needs to be integrated and managed by one main security platform. This trend has sparked Security Vendors to supply products that integrate different sub-solutions under the names of Unified Threat Management (UTM), Next Generation Firewall, Application Firewall, IDS/IPS, etc.

These solutions were initially offered as integrated, easy-to-manage security solutions to Small and Medium Businesses (SMBs) that had a need for security measures but could not afford the best of breed solutions in the market. After successfully selling to SMBs, these vendors are positioning their integrated solutions to Enterprises under the premise that an integrated solution can be more cost effective in handling the different security threats facing today's enterprises.

While this statement might be true, there are several challenges that make Enterprise-size organizations a hard sale for these solutions.

What is a UTM and is This Solution Worth the Cost?

The most representative solution in this trend of Integrated Security Management is the Unified Threat Management (UTM). UTM is a class of products which combine Firewall, VPN, Intrusion Prevention, Antivirus, URL Filtering and Anti-spam into a single network appliance, and provides all these functions at a much lower cost than if these components were purchased separately. Similar approaches are also used by Next Generation Firewall, and IDS/IPS devices.

So, do UTM appliances costing less than $1000 per office measure up in terms of security to the best of breed security products deployed at the primary corporate Internet gateway? The short answer is, some do and some do not.

High Detection Rate is a Must for Large Organizations

One of the primary issues that UTM solution providers have with Enterprise-size implementations is the relatively low detection rate. Most UTM solutions have an average detection rate of 83%. While this detection rate might be acceptable for the SMB market, Enterprise-size organizations cannot afford such a low

detection rate for several reasons. The main reason is the different regulations and standards that enterprises must comply with. Another fundamental reason is the cost of dealing with the remaining 17% in terms of additional security measures that the enterprise must implement to provide for complete security coverage.

The reason behind the relatively low detection accuracy of existing UTM solutions lays in the growth in application malware and the detection technology that most UTM solutions use. The basic technology relies on the ability to detect malware at the network layer by scanning and examining packets of information. The low detection rate comes from the fact that there is a growing trend towards using the application layer as a tunnel to transfer the malware. UTMs that attempt to address this trend are forced to use bolt-on modules to inspect content borne malware. However, due to the large and rapidly growing network throughput requirements, these bolt-on modules can only provide very limited inspection ability with simple pattern matching against a very small signature database. As a result of this trend of malware-transmission-over-applicationlayer, UTMs do not provide a complete solution for enterprise malware protection.

This mismatch between the technology and the current malware trends forces UTM customers to add more security measures in order to secure their network for compliance to mandatory regulations and standards. This, of course, creates additional spending that might not be necessary.

The Cost Reduction Angle

As cost reduction remains a strong target for CIOs and CISOs, Security vendors are working on solutions that will not only outperform the competition's but that will also show a quick Return On Investment (ROI) and a low Total Cost of Ownership (TCO). In the case of malware detection, the cost is typically a multiple of the number of computing devices that need to be constantly managed. Accurate elimination of malware on the network transport layer enables the organization to reduce the cost of managing the security of each computing devices and the number of devices that have to be aggressively managed, hence reducing the overall security spending and maintenance. Having security solutions with minimal impact on the network reduces both IT costs and the risk of business disablement.

BeSecure – The Much-Needed Touch for Enterprise Size Security

The need for a solution that is both able to process large amounts of data-in-motion with minimal impact on the network's throughput and that still has a high detection rate was the impetus that lead the Canadian company Wedge Networks to design and develop its flagship product - the Wedge BeSecure Network Security Appliance.

Wedge Networks recognized that the technology required to fulfill the two main identified needs above could only be based on Deep Content Inspection at the application layer.

The minds behind the BeSecure product developed and patented the "SubSonic" Engine. The SubSonic Engine is in charge of scanning and detecting malware at the application layer. The uniqueness of the SubSonic Engine is that it works the same way a transparent proxy would, with the ability to process large amounts of data for many concurrent user sessions without "missing" malware, and with a minimal impact on network throughput.

In recent tests carried out by the Tolly group, the BeSecure product, using the SubSonic Engine, has reached a 100% detection rate on the latest malware from Wildlist and 98% on all the malware in the past as accumulated, while a market leading UTM solution achieved 86% detection rate on Wildlist and 23% on all the malware in the past.

Wedge's BeSecure is a product that better positions UTM solutions to be a fit for Enterprise-size organizations. Adding the BeSecure solution in tandem with the capabilities of the main UTM and application firewall solutions enables these solutions to play a relevant role in large size implementations, not only due to its processing abilities, but also due to cost reduction, compliance and detection rate abilities that raise the security bar higher for the UTM and application firewall market.

ROI Case Study: Application Layer Deep Content Inspection Solution

Operation and Management

In these harsh economic times, organizations are looking to implement solutions that not only give them the security and compliance they need but also show a rapid return on investment (ROI). Organizations currently spend a great deal of time on Security patching and process management. These man hours translate into large sums of money for medium to large organizations. Wedge Networks' solution reduces IT staff costs by minimizing the need for patching, consequently enabling the management of Security patching, licensing and other UTM aspects to be an efficient, simple and time saving experience.

ROI Example

Profile of an **actual organization** using BeSecure (Base assumptions about this organization will be used in all ROI calculations below):

Organization type:	IT Software and Services
Number of employees:	17,000
Number of IT personnel:	30
Number of Servers:	2,000

Typical high costs of AV are due to the several person-hours that are required for installing and managing patches that address recent vulnerabilities in Host machines. When this requirement is removed, AV costs are reduced substantially.

The following compelling ROI example derives from the BeSecure's overall reduction of security costs. This calculation will show that compared with existing traditional UTM and Application firewall solution costs alone, the BeSecure delivers a positive and swift ROI.

To ensure that the organization is secure from malware, the security department needs to patch all servers and endpoints with up-to-date security patches. The average number of security personnel (in the above organizational profile) required to implement and maintain all anti-malware solutions is 2, and it will take them an average of 15 hours a week to manage this operation on all company servers. The average global cost of IT personnel is $75 an hour.

The calculations overleaf divide organizations with similar profiles as the above into three different anti-malware approaches as a means of cost comparison.

Approach A: having a standard UTM solution installed in the organization with no central patch or license management system.

Anti-malware patching: The calculation for a UTM solution that has no central management system would be:

(2 no. of patches per year * 1000 servers * $271 patch per server) +
(2 no. of patches per year * 1000 servers * $10 monitoring per server) =
$562,000 /year

Anti-malware licensing: The calculation for a UTM solution that requires a license per server would be:

(1 no. of license renewals per year * 1000 servers * $35 license per server) =
$35,000 /year

- This calculation excludes the one-time, first-year cost of purchasing and integrating the UTM solution for the described organization - estimated at $50,000.
- This calculation excludes an annual UTM service fee - estimated at $20,000 /year.
- All calculations are based on the above profiled organization.
- This calculation takes into consideration that organizations will implement two major patches per year.
- This calculation has taken the low end average of patch costs per server per year.
- This calculation has taken the low end average of monitoring costs per server per year.
- This calculation is excluding network performance issues. It is estimated that anti-malware software clients can consume up to 20% of the server's CPU in a given time. This fact may severely impact the network's overall performance as there needs to be an anti-malware client on each server, meaning a potential of dedicating up to 20% of the networks' CPU to anti-malware software.
- This calculation has taken the low end average cost of an annual license per server.

Approach B: having a standard UTM solution installed in the organization with a central patch and license management system:

Anti-malware patching: The calculation for a UTM solution that has a central management system would be:

(2 no. of patches per year * 1000 servers * $115 patch per server) +
(2 no. of patches per year * 1000 servers * $10 monitoring per server) =
$250,000 /year

Anti-malware licensing: The server cost calculation for a UTM solution that requires an organizational license would be:

(1 no. of license renewals per year * 1000 servers * $35 license per server) =
$35,000 /year

- This calculation excludes the one-time, first-year cost of purchasing and integrating the UTM solution for the described organization - estimated at $50,000.
- This calculation excludes an annual UTM service fee - estimated at $20,000 /year.
- All calculations are based on the above profiled organization.
- This calculation takes into consideration that organizations will implement two major patches per year.
- This calculation has taken the low end average of patch costs per server per year. The calculation takes into consideration that due to the management systems in place the overall cost per server is reduced.
- This calculation has taken the low end average of monitoring costs per server per year.
- This calculation is excluding network performance issues. It is estimated that anti-malware software clients can consume up to 20% of the servers CPU in a given time. This fact may severely impact the network overall performance as there needs to be an anti-malware client on each server, meaning a potential of dedicating up to 20% of the networks' CPU to anti malware software.
- This calculation has taken the low end average cost of an annual license per server taking into consideration the average license bundle cost for an organization with the mentioned profile.

Approach C: having a standard UTM solution installed in combination with the BeSecure product.

Anti malware patching: The calculation for a UTM solution that includes a BeSecure product would be:

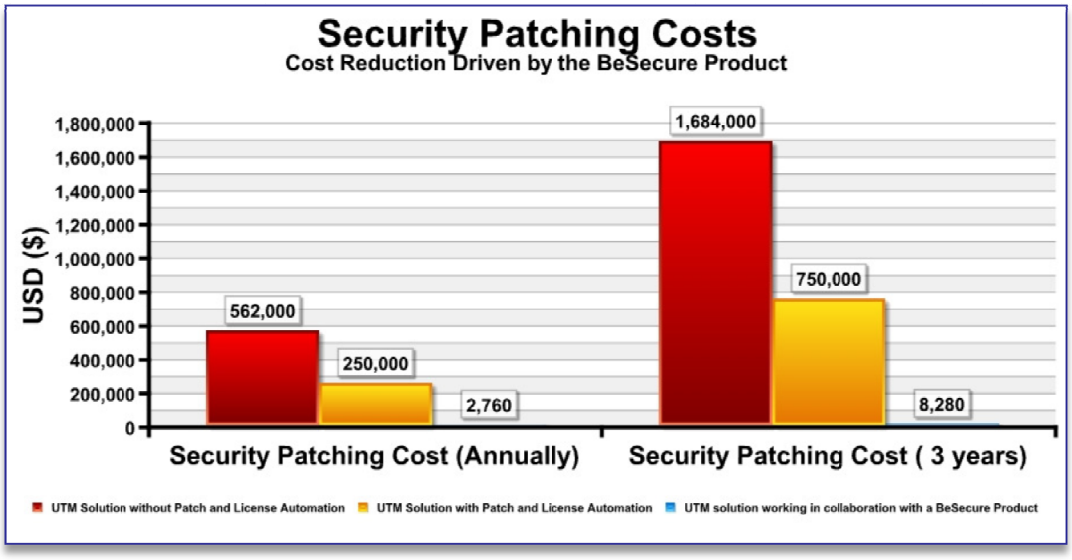
(2 no. of patches per year * 2 BeSecure products * $542 patch per BeSecure product) + (2 no. of patches per year * 2 BeSecure products * $150 monitoring cost per BeSecure product) = **$2,760 /year**

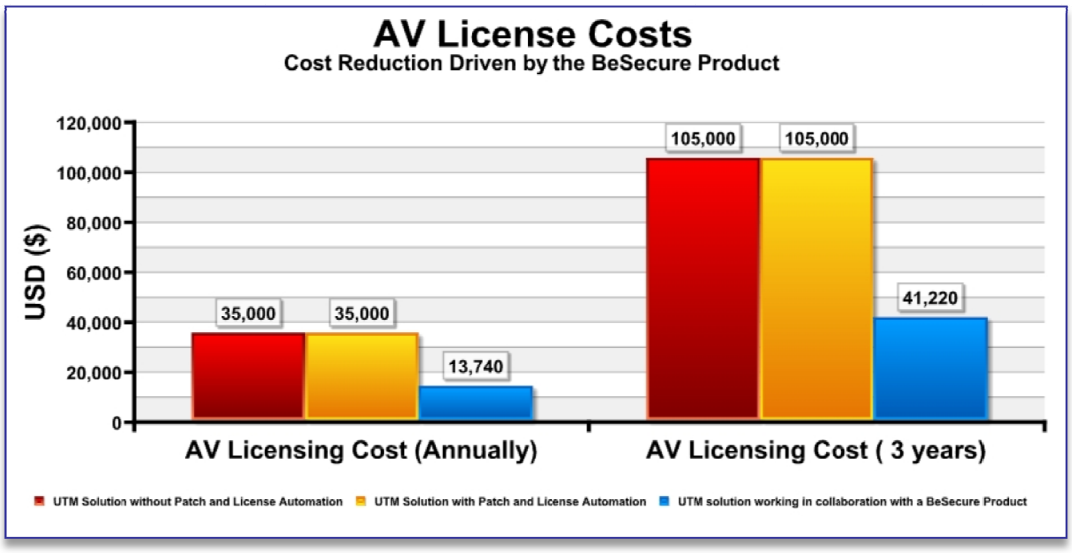
Anti-malware licensing: The server cost calculation for a UTM solution that includes a BeSecure product would be:

(1 no. of license renewals per year * 2 BeSecure products * $6,870 license per server) = **$13,740 /year**

- This calculation excludes the one-time, first-year cost of purchasing and integrating the BeSecure solution for the described organization - estimated at $25,000.
- This calculation excludes an annual BeSecure service fee - estimated at $6,000 /year.
- All calculations are based on the above profiled organization.
- This calculation includes 1 BeSecure product for production usage and another BeSecure product for backup purposes.
- This calculation takes into consideration that organizations will implement two major patches per year.
- This calculation has taken the low end average of patch costs per server per year. This calculation has taken the low end average of monitoring costs per server per year.
- This calculation is excluding network performance issues. The BeSecure product has a unique Deep Content Inspection engine that enables the product to scan a large amount of data for many concurrent user sessions with no real impact on the network. By having one device dedicated to anti-malware detection and prevention, all other servers do not need to run any anti-malware software, thus making their resources available for the different business applications in the organization.
- This calculation has taken the low end average cost of an annual license per year.

Cost of Security Patching: By implementing the BeSecure product, all servers are working under a BeSecure product and are therefore protected as long as the BeSecure product is patched on a regular basis with the most up-to-date anti-malware releases. As shown, the cost of protecting the organizations' servers is dramatically reduced. The calculation includes the number of patches per year, the number of active BeSecure products, the cost of patching each BeSecure product and the cost of monitoring each BeSecure product to ensure that the patch process was successful.





Wedge Networks – An Innovative Solution for Deep Content Inspection

Wedge Networks was founded in late 2002 and is a privately held company with headquarters in Canada and offices in the USA and the APAC region. Wedge Networks provides high performance network based web security solutions to enterprises and service providers worldwide. Wedge's technology leadership in Deep Content Inspection allows organizations to protect against new and emerging web based threats that traditional scanning methods have difficulty intercepting and controlling. Specialized in malicious-code detection and filtering at the application layer, Wedge's solutions touch millions of users and provide protection for utilities, service providers, health care, oil and gas, government, web sites, and many other enterprise customers.

Wedge Networks' customers include Fortune 500 companies and other organizations in main industry verticals. Wedge Networks is working on a global outreach program with a channel based distribution mechanism.

Conclusion

Frost & Sullivan believes that Wedge Networks has a leading Deep Content Solution that is able to ease the pain of large size enterprises. The BeSecure product and its SubSonic Engine enable large enterprises to have the security of a high detection rate Anti-Malware solution while enjoying the fact that this solution has almost no impact of the enterprise's network performance. This combination is a truly innovative and positive milestone in enterprise security. Wedge Networks' unique approach to Deep Content Inspection resulted in the development of a solution that provides enterprises a powerful tool to fend off current and future threats. The unique technology implemented in the BeSecure product will enable Wedge Networks to grow its market share rapidly.

Frost & Sullivan believes that Wedge Networks is positioned to lead the Deep Content Inspection market to the next level of detection and performance and that the company is poised to become a strong player due to its ability to deliver an effective solution with a significantly lower TCO to enterprises worldwide.

CONTACT US

London
4 Grosvenor Gardens
London SW1W 0DH
Tel. +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

Oxford
Oxford Business Park South
Oxford OX4 2GX
Tel. +44 (0)1865 39 8600
Fax +44 (0)1865 39 8601

Frankfurt
Clemensstraße 9
60487 Frankfurt a.M.
Tel. +49 (0)69 7 70 33-0
Fax +49 (0)69 23 45 66

Paris
24, rue de Londres
75009 Paris
Tel. +33 (0)1 42 81 54 50
Fax +33 (0)1 42 81 54 52

Milan
Via Mario Pagano, 38
20145 Milano
Tel. +39 02 4651 4819
Fax +39 02 4802 7054

Warsaw
ul. Domaniewska 41A
02-672 Warszawa
Tel. +48 (0)22 390 4135
Fax +48 (0)22 390 4160

Silicon Valley
331 East Evelyn Avenue, Suite 100
Mountain View, California 94041-1538
Tel. +1 650 475 4500
Fax +1 650 475 1570

San Antonio
7550 IH 10 West, Suite 400
San Antonio, Texas 78229-5616
Tel. +1 210 348 1000
Fax +1 210 348 1003

Toronto
2001 Sheppard Avenue East, Suite 504
Toronto, Ontario M2J 4Z8
Tel. +1 416 490 1511
Fax +1 416 490 1533

Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Delhi
Dubai
Frankfurt
Kolkata
Kuala Lumpur
London
Melbourne
Mexico City
Milan
Mumbai
New York
Oxford
Paris
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Tel Aviv
Tokyo
Toronto
Warsaw

About Wedge Networks Inc.

Wedge Networks is an innovator providing remediation-based Deep Content Inspection for high-performance, network-based Web security. It provides a scalable, real-time solution that understands the intent of Data-in-Motion, enabling the detection and remediation of both known and novel threats without impacting network performance. Its BeSecure appliances are easily integrated into existing environments. With its patented WedgeOS, Wedge Networks provides its global customers, partners and distributors a dramatically safer and innovative way to do business. For more information, visit www.wedgenetworks.com.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages fifty years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 40 offices on six continents. To join our Growth Partnership, please visit www.frost.com.