Meeting the Organizational Security Needs of Tomorrow

A Frost & Sullivan White Paper

Prepared by Ariel Avitan
Industry Analyst

Table of Contents:

Enterprise Evolution and Its Impact on IT

In the past several years, the work processes and dynamics in most enterprises have changed dramatically. The new age of social media and network communication software has added an additional working tool that is increasingly being adopted by enterprise employees. Software and web solutions, like Instant Messaging, LinkedIn, FaceBook and others, have the potential to help employees better connect with co-workers, partners and clients. As well, these tools enable a faster and more focused work process for some roles within the organization. This change in the enterprise environment is now referred to as Enterprise 2.0. However, do these solutions have a negative effect on the enterprise in addition to time consumption? And, if so, are the negative effects manageable or is there a need for limiting the use of such solutions?

In this white paper we will address the need for software solutions that monitor software and web solutions the context of threats that can utilize these solutions as a way to infiltrate the enterprise.

The Security Concerns Following the Change in Enterprise IT

While there is no doubt that many of the communication and social software solutions made the enterprise working environment much more interactive and efficient, there are some negative effects to the use of these solutions, most of which have nothing to do with the user and everything to do with next generation malware attacks.

Malware is programmed by hackers who are always looking for ways to infiltrate different networks. Their main goals are to either disable or cripple the infected network, or steal digital information that can be used for financial gain.

In the early network days, most of the malware were aimed at the lower level network protocols as that is where they were the most vulnerable and the most easy to exploit. Security vendors started offering solutions that would know how to look at data packets going in and out of the organizational network, making sure that no malware was penetrating the network. In recent years, hackers followed the trend of web based applications used by employees and started to create malware that hide in the applications and are therefore not detected by regular layer 2-4 malware detectors. When security vendors noticed the new hacker trend they tried to apply their solution to the application layer, only to find that in order to inspect the application layer in a cost effective manner there needed to be a new approach to this issue.

Today, the current solutions in the market do not meet the detection and efficiency demands of medium to large size enterprise. This current stage calls for a new approach to application based threats.

The Right Approach to Application Based Threats

As mentioned, the enterprise work environment is becoming heavily affected by web based applications that improve work efficiency but that also serve as platforms for potential malware threats based on web applications.

The common approach to this threat was to add a content inspection solution to the existing anti malware solutions that already exist in the market. This approach would have worked if the application layer had the same properties as the lower network layers; however the differences between the layers are quite significant. While most of the malware is detected by packet inspection on lower network layers, the same method of detection is not effective in the application layer. The application layer transmits content that might be hiding malware and therefore packet inspection, a method that does not focus on the content, cannot help in detecting the malware in most cases.

A more efficient approach to application based threats is Deep Content Inspection. These solutions inspect the content that is transferred from the web to the network and detect any suspicious malware hidden within the application. This approach has the ability to detect the malware but suffers a main challenge performance wise. Deep Content Inspection solutions have to view large amounts of information, detect and contain malware threats. These actions take a lot of bandwidth from the network, slowing down the critical web-network bottleneck within the organization.

Having a solution that prevents application layer malware from entering the organization at the cost of network performance is not a solution that most enterprises will accept. Is there a way to prevent application based malware without affecting the organizational network performance? The answer is yes.

SubSonic Engine - Enabling Business in an Agile IT Environment

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 is still capable of achieving 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 requirements, needed to be able to perform Deep Content Inspection at the application layer while meeting the high bandwidth and performance requirements.

The minds behind the BeSecure product developed and patented the “SubSonic” Engine. The SubSonic Engine controls the scanning and detecting of 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, while having 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 to 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.

Case Study - Higher Security Standards With Low Impact on IT Performance

The Case study below is based on interviews with a current client of Wedge Networks.

Companies’ Activity: A leading Semiconductor company
Company Size (employees): about 7,000 globally
AV Status: AV solutions on both endpoints and core devices.

The Need:

The organization in question has come to the conclusion that it has a malware issue even after having installed state of the art web filtering solutions and regular Anti-malware solutions.
The organization used an Anti Virus solution and extended it to the organizational endpoints to increase the detection rate. However, they still had cases of network infections that cost them time and revenues.
The organization took the security measures a step further, adding more capabilities to the Anti Malware solutions already installed in their

organization, but this effort ended with only a small insignificant increase in the detection rate.

When coming to assess new approaches to the malware issue that the organization was facing, the IT managers responsible for implementing the security efforts researched the cause of these malware infections and came to the conclusion that they needed a gateway protection solution that would detect the malware without introducing a large adverse impact on the organizational network performance.

Examining the Solutions Available:

The organization researched the security market, resulting in a final Proof of Concept stage for a web protection solution that the current Anti-Virus vendor offered along with a Wedge Networks BeSecure.

In the Proof of concept period the organization agreed on a number of criteria that would be examined in both solutions to determine which one would be the favored solution.

The first criterion was based on the detection rate. The organization set a goal of lowering the malware infection rate to a minimum, making this criterion a top priority.

The second criterion was based on performance. The IT department understood that an efficient solution would be able to stop the malware with minimal impact on the network. As this organization relies heavily on their network accessibility and high throughput performance, this criterion was also of a high priority.

The third criterion was based on an inline mode option. This option was the preferred option for the organization as it best fit the organizational network architecture.

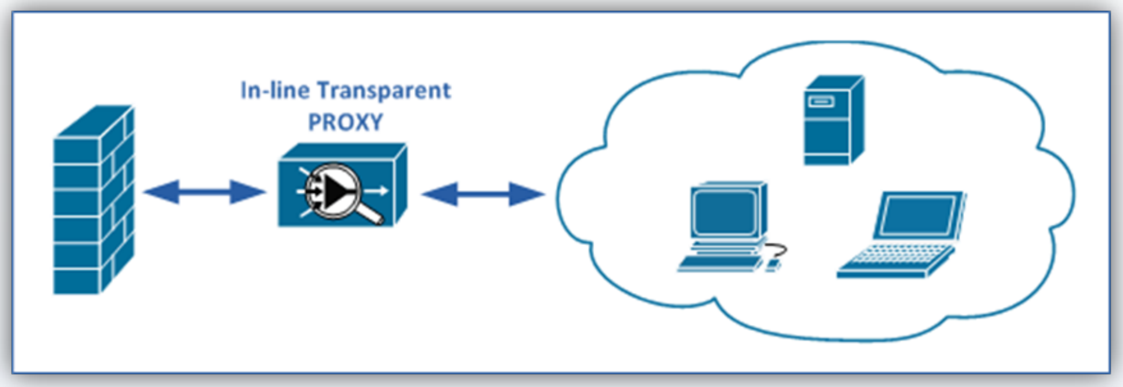
The fourth criterion boiled down to simplicity of the implementation. The IT division within the organization wanted a solution that would be as close to the “plug and play” scheme as possible.

Proof Of Concepts Results:

Detection – Both solutions had a high rate of detection on regular malware. However, when examining the detection rate for web application based malware, the Wedge BeSecure had a clear dominance over the competitor in detecting and marking malware.

Performance– In the performance criterion the BeSecure showed exceptional results in comparison to the competitor. The comparison results show that BeSecure was 3 to 5 times faster than the competitor in general Deep Content Inspection and more than 5 times faster in examining large files only.

Inline Mode – In the examination of both solutions, the competitors' solution failed to show a working L2 transparent inline mode option. As well, the proxy mode that was offered by the competitor did not achieve the required results. Wedge`s BeSecure, on the other hand, showed the ability to work inline and, as a result of their transparent proxy mode, their connection methods to the network passed the requirements needed.



Simplicity – Again, when coming to examine both solutions, the BeSecure has proven that a "plug and play" implementation, for a complex Deep Content Inspection solution, is an option.

In comparison to the competing solution, the BeSecure was, simple, easy to maintain, and easy to manage

Decision:

The organization performed the pilot with both solutions and, after three months, reached the conclusion that the BeSecure, Wedge Networks' Flagship product, was definitely the solution of choice for their Deep Content Inspection needs. Since the time that the company made the decision to choose the BeSecure, the organization has renewed the service and is in the process of ordering additional BeSecure hardware and licenses to increase security in their global offices.

Conclusion

The growing threat of malware is taking a sophisticated turn to applications; using the vulnerabilities of these applications and their demand within the enterprise working environment. Enterprise IT and security departments have tried to fight this threat with existing malware solutions and have found that while most of the solutions do not meet the needed detection rates, the ones that do meet these rates tend to have performance issues that prevent them from being the ideal solution for an enterprise size network.

The BeSecure, Wedge Networks’ flagship product, is able to meet the enterprise demand for high levels of detection with minimal impact on network performance. The Wedge BeSecure uses its unique transparent proxy solution to perform Deep Content Inspection on incoming traffic with minimal effect on the network performance and throughput. Additionally, the simplicity of the BeSecure`s user interface and management, makes it easy to deal with application-based malware and reduces management and maintenance costs substantially.

Frost & Sullivan believes that the Wedge Networks BeSecure product line redefines what fighting malware is all about. Security vendors will now need to meet a higher bar in both levels of detection and performance impact in order to compete in tomorrow’s malware battlefield.