{jcomments on}

Small and mid sized businesses in India are increasingly becoming aware of the importance of IT security. With increasing complex threats on data security, the need to protect core information and data assets is a major concern. Citing this industry segment as a big chunk of focus, Tushar Sighat, VP- Operations, Cyberoam (India), unleashes his views and perspectives towards SMBs of the country.

What are the security trends, you foresee from the small and mid sized businesses of India?

Increasing Security Awareness: Small and midsized businesses have emerged as the biggest growth drivers of IT security, particularly the UTM(Unified Threat Management) market. This potential market is huge because it has low penetration rate for IT security. Even the vendors who focused primarly on large enterprises, are now developing products exclusively for the small to medium-sized enterprises, and find it a major success too.

Technology enhancement against threats in evolving IT environment: Considering the budgetary constraints of SMBs, UTM appliance vendors continue to improve the technology to address growing threats in new and emerging environments consisting of applications like VoIP, XML, application protection, and storage. This capability is needed as these popular infrastructure components become targets of attacks.

What are the major threats to the SMB segment?

The threats to the SMBs are same as for any other enterprises/businesses and are ever on the rise with the widespread adoption and dependence on internet connectivity. Ever increasing

internet usage and the growing sophistication of Web 2.0 has opened opportunities for cyber criminals to increase their malicious activities and harm networks by compromising the confidentiality, integrity, or availability of network data or systems.

The latest cyber threat landscape is defined by three factors. The first, is the emergence of the user as the weakest link in the security chain with attacks becoming more targeted through the extensive use of social engineering techniques based on user information and vulnerabilities.

The second, is the internal threats which are high in frequency and potential and estimated at over 55% of the total threats. While the first two aspects define the route of attacks, the third important aspect pertains to the methodology and techniques of attack which spreads rapidly, causes widespread damage and are popularly known as Blended threats. Blended threats combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread attacks.

The third is insider threats. It is common to industry knowledge that insider threats comprise more that 55% of total internet threats. These threats include significant and confidential data loss by employees due to ignorance or malicious intent.

In view of the above threat landscape, Cyberoam identity-based security has emerged as a popular choice for both enterprises and SMBs as it provides a transparent shield to the network by pinpointing the actual user behind any network activity and thus, giving complete knowledge on ‘who is doing what’ in the network. This unique feature enables Cyberoam to proactively address insider threats using a combination of incident prevention, detection and response. Since, the user is the weakest link in the security chain today, linking user identity to security is the only way to fight against insider threats.

In what all ways UTM could be a choice of SMB?

Today’s SMBs are largely looking at Unified Threat Management solutions that integrate a range of security features like Fire wall, Virtual Private Network, Anti-virus, Anti-spam, Intrusion Detection and Prevention, and Content Filtering - in addition to enhanced productivity through Bandwidth Management and Multiple Link Management over a single platform. The UTMs can ward off both internal (purported to account for more than 50% of the total threats according to

Industry Sources) and external threats. Largely due to an increase in blended threats and the advent of 'zero-day' attacks, there is a greater need for layered security solutions that would proactively control these threats.

Budget constrains are a major concern for every Small sized or mid sized company. What effect does this factor have on the security landscape?

The emergence of Unified Threat Management Solution is largely attributed to the need of fighting multiple entry points of complex blended threats that demand integrated solutions with interoperable security features like Firewall, AS, AV, Content filtering, IDS etc. - all on a single platform. However, while it effectively fought off the blended threats, it also lowered the operational and capital costs while doing away with the need to deploy and manage multiple units of point solutions.

Therefore, with respect to costs, UTMs are the preferred choice for SMEs because of their cost efficiency and are also driving the UTM growth. Even in face of economic slowdown, the UTM market remained buoyant and the IT spending among SMBs for IT security continued to rise slowly but steadily.

UTMs and DLP solutions become popular among the large organisations, how do you see these technologies penetrating the small sized business segment?

UTMs are already penetrating the small and medium sized businesses because a single UTM appliance makes it easy to manage the security strategy of organisations, with just one device to worry about, one source of support and a single way to set up and maintain every aspect of security. Characteristics such as single point of contact, 24 x 7 vendor support, reduced technical training requirements and zero-hour protection enable full protection against network threats, while at the same time causing no degradation in performance. So, not only the UTM turns out to be a cost-effective purchase, but it also lowers the operational expense significantly.

What is the level of awareness about cutting edge security technologies among the SMB segment?

Awarenesss in cutting edge security technologies is rising as businesses; both SMBs and enterprises are increasingly becoming aware of threats and the need to secure their data and other information assets from the breaches. In fact, companies are beginning to correlate business decisions to things that actually happen on the network by applying business policies to internet access management and security. The constant news publicity of data thefts, viruses and online scams is also driving home the point that if trouble hits, it will be serious. Thus SMEs look for deploying security solutions in terms of lowered capital and operating costs, integrated multiple security features and ability to counter the rising insider threat.

What is Cyberoam's strategy for SMB segment?

By investing in the development of powerful, integrated solutions, Cyberoam strives to create value-added products that deliver more security advantage than comparably priced competing products so that customers from the outset, find themselves equipped with a superior product that is a step ahead in fighting Network Threats. Small and medium enterprises are as much at risk as large enterprises from targeted attacks. They need to protect their networks effectively from external and internal threats without a large security budget.

Cyberoam CR50i, CR50ia, CR100i, CR100ia, CR200i, CR250i and CR300i are powerful identity-based unified threat management appliances, delivering comprehensive protection to small and medium enterprises (SMEs) with limited investment in financial and technical resources. Cyberoam gateway security appliance offers protection from blended threats that include virus, spam, malware, phishing, pharming. Its unique identity-based security based on Layer 8 technology protects enterprises from internal threats that lead to data theft.

What potential does SMBs carry for Cyberoam?

The potential is very high. SMB is a large and fast growing market segment and the security industry is booming as businesses deal with a wide variety of security concerns ranging from identity theft, loss of confidential user data, loss of productivity, bandwidth abuse, mail flooding, etc.

How does existing infrastructure optimisation effect the SMB security market?

Deployment of UTM solution is about optimising infrastructure. Being Single security solution as against the installation of multiple point solution deployment, plug and play architecture and Web-based GUI for easy management translates into highly optimised infrastructure.

What challenges do the SMBs face in adopting cutting edge security tools?

The challenge is that while the right security solution to meet the organisation's needs is critical, lack of clarity on what one is trying to automate or protect, ensures that even the best vendor's solution comes up short. Security is no longer about keeping out viruses, worms and other threats. It encompasses enterprise business requirements as well as user behaviour. Therefore the challenge lies in risk assessment as well as aligning it with the organisational and compliance requirements and standards. A simple, easy to manage and granular solution that can monitor, control and secure the individual user activity offers flexibility in business needs while delivering comprehensive security.

This means there is a need for a layered security solution that could proactively control the thrat entry and where the various security functionalities are interoperable.

Third generation UTMs like Cyberoam find popularity among SMB sector as they provide comprehensive internet security by integrating a range of security features like Firewall, Virtual Private Network, Anti-virus, Anti-spam, Intrusion Detection and Prevention, and Content Filtering - in addition to enhanced productivity through Bandwidth Management and Multiple Link Management over a single platform. Moreover Cyberoam UTM tackles insider threats by integrating identity controls and thus can identify the exact user and not just the IP address of the Machine. Cyberoam UTM is a one-of-its-kind solution with granular controls that pinpoint the actual user, rather than merely identify him/her by the IP address of the machine, therefore giving complete visibility into the network. This not only helps in applying granular policies but helps control users and thus tackle internal and all user based threats.

What future do you foresee in this area?

SMBs are a booming market and UTMs are the most preferred security choice that leads the

pack in IT security segment. With the advent of present generation of high performing UTMs not only SMBs, but even the enterprises have emerged as bright spot in the UTM market.