

Considering next generation Security Infrastructure Platform.

Telecom Security Overview

Today's, and even more tomorrow's, telecommunication networks are universal platforms for large number of diverse services. To increase market share, Telecom Operators are constantly in hunt of innovative service offerings for their customers. The dynamic market for telecommunication services requires extremely high flexibility and very short time-to-market in order to be first to address new customer groups with new offerings. One such service offering which is rising exponentially is Managed Security Services, in addition to the vast range of security solutions now being offered by the service providers. Companies large and small now recognize how important security can be to their businesses and hence are spending increasingly more on IT and network security each year. Security for Telecom Operators is not only "one other" revenue generating stream, but it is inherently necessary as the operators themselves also need to safeguard their own networks. On the other hand rising regulatory pressures are also creating demand for full-proof protection for services offered to the mass market such as email, data and internet services. This is especially true around Parental control and content filtering. Therefore, if something is a necessity as well as a medium to get new business and eventually more revenue, it has to be taken seriously.

The telecom industry has entered a phase of revolutionary change as Internet technologies are enabling a new era of services that are dramatically changing business models. These are exciting opportunities yet they also present daunting challenges for telecom carriers. Time-to-market, competitive differentiation (not only from the traditional rivals but also from newly emerged internet vendors), customer satisfaction and cost control become increasingly critical to subscriber retention. Telecom security, either directly or indirectly, is related to all these parameters and so is the underlying infrastructure. However until recently, neither security nor infrastructure were given top priority and were always treated as an afterthought; resulting in a hodge-podge approach. We at TekPlus strongly believe that Service Providers need to shed away this approach and start evaluating security as well as infrastructure as core and address them way up in their decision cycles considering longer term benefits rather than immediate short term needs.

What Service Providers require

Telecom networks today are grasped with numerous known/unknown and constantly emerging threats. As networks are becoming more and more intelligent, hackers and intruders are also becoming smarter and finding out new ways to intrude the networks. Additionally new technologies such as IP convergence, triple/quad play, web services, Unified Communications etc. are opening new doors for attacks. On

the other hand, enterprise customers choked up by regulatory compliance and information protection worries are demanding for full-proof protection. In such a scenario what operators need are comprehensive security solutions based on advanced platforms. They need a solution which can empower them to quickly launch new security services, scale them up as per demand and maintain high QoS.

The current Telecom environment, due to its size and nature, requires a platform which is ruggedized and highly available. A ruggedized, highly-available platform will typically include redundant power supplies, redundant control modules, redundant processors, redundant network interfaces, and even redundant fans and backplanes to avoid single point of failure i.e. achieve 5 nines availability that carriers strive for. This is especially true when considering security platforms. The performance of security platforms is certainly paramount to successful deployments. Ideally carriers would want these platforms to run security application at or near wire-speed with a negligible introduction of latency. Another requirement for a telecom platform is the ability and ease to provide centralized management and policy control.

Historically, software-based security applications resulted in performance degradation which is one of the primary reasons that purpose-built security appliances came to market. Today, because of the intensified demand, carriers require a platform which has advanced high speed processors for deep packet processing. In the current environment network speed is not evolving as fast as Moore's law and this means there is more processing power available to evaluate the same amount of traffic for deep packet inspection, etc. What is even more beneficial is that this functionality is now available at decent prices via a commercial-off-the-shelf approach.

In addition to all these requirements, carriers also need to think of significant cost savings and ultimately huge ROI from these infrastructure platforms. In short, carriers require their infrastructure to be cost-effective, highly available, flexible, scalable on demand, easily manageable and providing optimum performance. In other words, best of all, a perfect blend of strengths provided by software, hardware and services. Tough ask but definitely not an impossible one, so let's evaluate what options they have and which ones can better serve their purpose.

Telecom Security Options

Traditionally operators use to buy stand-alone dedicated appliances as and when the need arose. Combating any particular threat which was of "high alert" at that point in time was the most critical deciding factor for the hardware infrastructure purchase. Soon the demand for another threat protection would raise its ugly head forcing providers to provision another box and then another. This was a never ending process unless and until the operators decided to replace these boxes or provision more floor space and resources (power and/or management). None of these options were pleasurable for service providers as the costs avalanched.

Hence TekPlus believes this approach was and is still not at all sustainable especially in the current ever changing landscape.

A better option is to go for consolidated hardware on platforms. Consolidated hardware empowers the service providers with high scalability. Using a chassis the service providers could mix and match security blades as per their needs. Consolidated hardware eats up less floor space, less power and cooling mechanism, less management issues and eventually reduced TCO. The only concern with consolidated hardware on platforms is it brings in vendor lock-in. Operators then have to rely heavily on the hardware provider to provide those upgrades/ new security blades. Another issue is the proprietary nature of such solution which hampers carrier's flexibility. Using such platforms puts restriction on reuse of the chassis for different purposes. Also carriers cannot enjoy full flexibility and control to mix and match different types of security if the vendor fails to offer a complete portfolio of blades. Simply put forward these proprietary platforms are just a fraction ahead of the above mentioned dumb boxes if the vendor and its eco-partners don't have the capability to maintain pace with the technological advancements. Again not so pleasing for service providers!

Given the above scenario many of these security platform vendors are talking about moving towards a standardized platform wherein insertion of security blades from different vendors (best-of-breed) might be readily available. TekPlus believes this will take some time to hit the marketplace and operators need to evaluate the availability timeframe vs. the opportunity/ demand generated by their customers since by the time operators deploy these platforms and develop new services the market might have shifted somewhere else.

Realizing this and given the fact that most operators are gradually migrating to new NGN infrastructure has brought demands from the service providers for the need to handle security infrastructure solutions in more profound ways which can benefit both them and the services they offer to their clients for a number of years. This means taking a more holistic view of the NGN infrastructure and how best to leverage it.

The third, and by far the best option operators have is to go for software running on COTS (commercial off-the-shelf) hardware infrastructure. This option empowers service providers to mix and match security deployment as per their needs. The COTS approach avoids vendor lock-in and also reduces dependency on vendors for technology upgrades. The key benefit of this option is the software infrastructure runs on modular hardware components. The modular approach offers economy of scale in the form of re-using different hardware and software modules in multiple products. There is a significant inherent OPEX saving as a result of module reuse. With more and more technologies such as virtualization, SOA, reuse of middleware services etc. being deployed, software is really becoming the key ingredient. The software environment can extract the capabilities of the underlying hardware to the fullest extent i.e. maximizes the utilization. Hence service providers can achieve much more output with less investment, which means huge ROI.

Considering Service Provider's security requirements and available options TekPlus, in the succeeding paragraphs, has

articulated the key ingredients of an ideal telecom security platform.

Ideal Telecom Security Platform

An Ideal Security Platform should consolidate security functions using a blade and chassis infrastructure with a corresponding software infrastructure, which is based on open standards, virtualization and standardized interfaces. The backplane of such a platform should be based around 10Gbit Ethernet network technologies and should have an integrated high-speed switching infrastructure to make it capable of supporting multiple 10 Gbit networks, which means better performance and reliability. Some of the blades that can be plugged in to this backplane should have ample ability to provide deep packet processing at high-speed to carry out intensive security functions. For this purpose the blades that slot into the standardized chassis must be running on enhanced processors. Other blades should act as general purpose server blades to provide different functionalities. This approach provides deployment flexibility to service providers who can have a different mix depending on the functionality required.

On top of the hardware there must be a virtualization environment which abstracts the applications from the underlying hardware and allows the hardware to run multiple applications simultaneously permitting scaling both up and down as workloads demand; result – great performance which is highly scalable. One other important functionality that an ideal platform should have is a common system-wide management for both internal control as well as off-platform interfacing to external OSS systems. Nevertheless the platform should be NEBS-3, ETSI and other telecom regulatory compliant. All these features are basic ingredients for a resilient, highly scalable, flexible and highly available carrier-grade solutions.

The key to success of such a platform largely depends on vendor's and/or its ecosystem partner's capabilities to create security and packet processing applications that can scale to carrier levels and run securely and cooperatively to deliver new services and/or cost reductions for a carrier's network.

TekPlus believes currently only a few vendors such as IBM have the capability to espouse such a platform or to provide the building blocks for such a platform given the requirements for high availability, scalability and stability required from such platforms. Additionally only vendors of that size are in a position to leverage a large range of ecosystem partners providing different functionalities to the hardware Platform.

In the case of IBM, some of the security ISVs in the ecosystem are CheckPoint, Symantec, McAfee, Aladdin, Finjan etc. In addition to this list, IBM has now acquired Internet Security System (ISS) which brings with it in-house security expertise. The engagements with global NEPs also help IBM to address operator's pain-points. By leveraging the strength of ecosystem partners, IBM can reduce the technology upgrade cycles. Service Providers should therefore be demanding an integrated, pre-tested and validated platform from these leading vendors to achieve reduced time-to-market.

Conclusion

TekPlus believes that Service Providers should consider the ideal telecom security platform option for their security needs while they are still in the process of developing their next generation architecture. This means taking a more holistic view of the advantages that can be obtained from modular infrastructure whilst deploying SDP and IMS on carrier grade infrastructure. This leveraging of the same infrastructure will have direct bearings on OPEX and CAPEX. Deploying security solutions on a standardized platform having modular architecture provides the option of scalability and high availability. In addition to that, the ability to easily deploy future processor technology for more intense packet processing will put service providers in a position to offer a stack of security services in conjunction with the different advanced services and thus be in a position to target a number of customer sub-segments.

Every care is taken to ensure that all contents of this Positioning Paper are accurate and opinions stated are based on information and sources we believe are reliable, but are not guaranteed. No liability can be accepted by TekPlus Limited, its directors, employees, or authors for any loss incurred as a result of using or failing to use anything contained in the report, conclusions stated or inferred.

TekPlus Limited
12th Floor York House
Empire Way, Wembley
Middlesex, HA9 0PA
United Kingdom

Tel: (44) 208 795 4500
Fax: (44) 208 795 5800
www.tekplus.com
info@tekplus.com