

<you say>

Unifying your threat management practice

By **BENJAMIN TEH**

PROTECTING sensitive corporate data and enterprise network security is imperative to a company's survival as such data can be described as the business' life blood. Thus, it is crucial for companies to ensure that confidential information is tightly guarded and made inaccessible to malicious hackers attempting to use it for monetary gains. To prevent the risk of such problems, most companies install a myriad of security solutions.

IT managers are, however, finding it tough trying to constantly identify and integrate customised security solutions that deliver the latest remedial technologies to curb potential attacks and yet ensure uninterrupted network traffic after integration. As more security applications are added to solve new threats, administration invariably becomes complicated as it involves an entire bandwagon of applications, both new and old.

Security cannot be viewed as an end in itself. It is more usefully seen as a critical part of network and application availability – of enabling users to get their jobs done. In this regard, the choice of which security technologies and products will be determined by how, in practice, they serve this goal. Thus, security decisions should be mapped against one's overall IT goals, and ultimately to the bottom line of the business they serve.

Multi-threat management

Organisations today require a multi-threat management solution that provides comprehensive functional coverage which blends a wide range of countermeasures, including ones that are preventive in nature (eg firewall) to complement those that are primarily reactive (eg anti-virus), comprehensive logical coverage which provides protection for threats against all elements of the computing infrastructure (eg networks, systems, services, applications, and data), as well as comprehensive physical coverage which is applicable

not just at Internet boundaries but at locations throughout an organisation's computing environment (eg the data centre, in remote offices, and at choke points on internal networks).

Yet, addressing the above requirements by continuously implementing additional point products to fill in the associated gaps in the defences is not a sustainable strategy. It invariably results in high capital costs, runaway operating expenses, and, despite the best efforts, is still not very effective due to the holes that inevitably appear at the seams of this type of patchwork solution.

Restoring balance

Given this situation, it is not surprising that many organisations have selectively implemented and continue to consider integrated security devices as a means to restore balance to their overall security solution. This approach, which can be described as Unified Threat Management (UTM) – has evolved into a pragmatic choice for IT managers.

Integration of multiple security functions into a single device reduces the complexity and cost of implementing and managing a network security infrastructure. Unified security solutions offer companies a better way of integrating multiple new security technologies in their network infrastructure without multiplying management touch points.

These solutions not only include security-focused network appliances, but in some cases, dedicated e-mail security appliances and end-point protection, along with timely and cutting-edge global threat research to keep the protection updated 24x7. To achieve a seamless and efficient solution, IT managers must also look for unified management and reporting consoles that reduce IT operating expenses.

According to market researcher IDC, the UTM market in the Asia-Pacific will expand by a compound annual growth rate (CAGR) of more than 26 per cent between 2007 and 2011, making it one of the fastest-growing

segments of computer security. But we can and should go further. To ensure organisations can optimally address the prevailing security challenges, one should start to look beyond conventional UTM products and seek solutions that qualify as true, purpose-built network security platforms.

A purpose-built network security platform is effectively an advanced UTM solution – one that employs an optimised design to ensure that organisations can maximise the associated gains.

To optimise security, performance, flexibility, and cost effectiveness, a purpose-built network security platform must be a turn-key system. For starters, this entails having a pre-packaged device that combines hardware, a network security operating system, and all requisite security software. It also must include research-fuelled, security subscription services, in addition to conventional maintenance and technical support services.

The next requirement that defines a purpose-built network security platform is that it must exhibit significant degrees of integration, yet still be modular in nature.

Pragmatic solution

Finally, a purpose-built network security platform must be based on engineered hardware. What this means is having hardware that guarantees sufficiently high performance based on it being "matched" to the specific security software, networking services, and implementation scenarios that it is intended to support.

The net result is an exceedingly pragmatic network security solution – one that thoroughly and uniformly addresses the functional, logical, and physical security requirements of today's organisations; achieves the highest levels of security effectiveness and operational efficiency; and, is not disruptive to business critical communications and application transactions.

The writer is sales director of South Asia, Fortinet Inc