Most organisations' security infrastructures are complex – and destined to stay that way.

Secure by design?

IT IS A TANTALISING DREAM: AN INTEGRATED security suite that manages the whole security infrastructure, with co-dependencies prioritised and event data automatically analysed for signs of dangerous trends. In this utopian future, the security suite will scan systems and applications for vulnerabilities, monitor the firewall and traffic on networks for intruders, scan files for viruses, monitor mail and web access for inappropriate content, notify when key system files have been modified, and allow organisations to manage the security configuration of their servers and network appliances from a single console.

For the moment, it remains a dream – and may remain so forever – but some parts of it are within the reach of most organisations, through the use of security event management (SEM) technologies from companies such as Computer Associates, GuardedNet, IBM Tivoli and Symantec.

"Many standalone security products have simply ended up as 'shelfware'."

As organisations have protected themselves with firewalls and installed host- and network-based intrusion detection systems and other defences, managing these has become correspondingly more difficult. Administrators are frequently flooded with too much event data to sift through – and forced to confront too many 'false positives'.

Shelfware

Many standalone security products, particularly intrusion detection systems, have simply ended up as 'shelfware' due to the high number of alerts that are generated, with many IT departments either ignoring their output or turning them off. SEM helps companies to weed out the unimportant alerts and to consolidate the data from all these disparate systems, enabling administrators to focus on the genuinely urgent events.

The real power of SEM becomes evident when these systems can understand the complex relationships between different security devices on the network, allowing organisations to uncover anomalies and trends and understand the impact of these events. Companies can have staff spend far less time monitoring individual products and their associated logs, reducing the chance of a manual error in what is often a time consuming and laborious task. IT staff can also react far more quickly when something serious happens and take corrective action before major damage occurs.

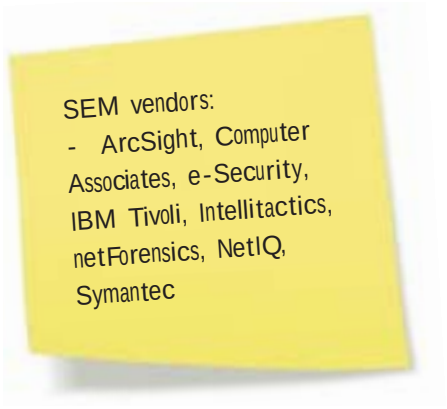
Unfortunately, there are limits to the capabilities of SEMs that may never be overcome for technical, business or industry reasons.

For example, the ability to monitor and control heterogeneous devices is limited by the vendors who own the intellectual property of different security and network devices.

Limited integration

This has resulted in only limited integration in some cases or no integration at all in others. The introduction of some standards (such as Check Point's OPSEC) will allow for closer integration of different products in the future, but most of these proto-standards are focused on the corporate perimeter and not the core of the network. Whether this changes will be determined not by anything that happens in the security industry but by issues elsewhere.

There is also some way to go with many products before SEMs have the necessary 'intelligence' to match the skills of a good security expert in analysing data and taking necessary actions. Most systems, for instance, concentrate on integrated monitoring, but lack the ability to manage the security configuration, therefore relying on operators to reset policies appropriately.



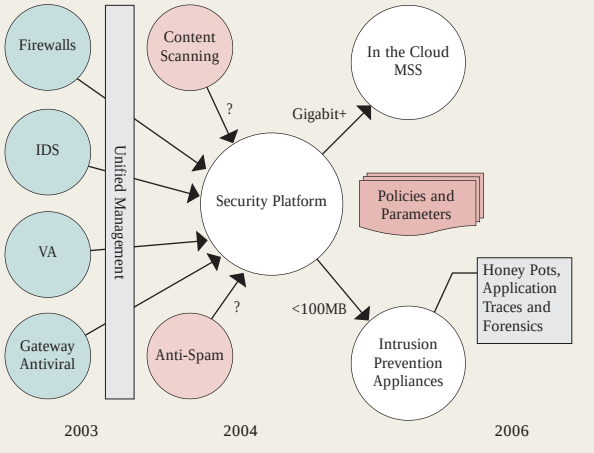
Automated analysis of logs from disparate systems to correlate possible breaches does not prevent the problems occurring in the first place; at best, it only ensures they do not happen again. The monitoring activity of these tools is also aimed at technical attacks on networks and systems, more than on the misuse of IT resources by authorised users. At the moment, this latter problem still lacks a viable packaged solution.

An alternative to SEMs are consolidated devices that can perform several security functions. These are growing in popularity. While they can reduce the administrative burden on staff, organisations need to be sure that the devices are actually up to the job, technically: they can become single points of failure, introduce latency, fail to reduce management costs, not offer sufficient granularity in terms of access privileges, and not scale without requiring additional devices from the same vendor. The best options are devices that specialise in particular aspects of security, such as email or intrusion prevention, rather than ones that try to do substantially different tasks. The right device can reduce management costs and improve security significantly.

But putting too much trust in a single, unified suite is often a mistake. Information security is an immense area and includes much more than just the firewalls and antivirus software of traditional security. Today, it covers many other elements including those related to IP telephony, biometric authentication, distributed denial of service mitigation and so on.

While some vendors claim to be able to offer up to 90% of the expertise needed to provide a secure set-up, they will never be able to provide total coverage. Security companies that have tried to become one-stop security shops in the past, most notably Network Associates, often failed to fully integrate even their own products, let alone competitors' offerings, and suffered as a result.

BEST OF BREED COMES TOGETHER ON SECURITY PLATFORMS



Source: Gartner

And technology is not the answer to all security issues, even when dealing with technological threats. While an integrated security suite may be able to monitor and control the security of systems, it will never be able to assess business needs and formulate an appropriate response. Indeed, it is in terms of management that many organisations fall down and which most need to address first before writing out any more cheques. ■

> "There is some way to go before SEMs have the necessary 'intelligence' to match the skills of a good security expert."