

Automating Security Consolidation

Enterprises are finding that if principal security functions such as firewall, AV, IPS and content filtering are not sufficiently integrated, then they face the double-whammy of sluggish network/application performance and weakened overall security posture. Hardly surprising then that 90% of European mid-sized and large organisations are seeking to consolidate some security functions in order to reduce opex, lower management complexity and tighten security against blended threats and sophisticated application exploits.

Can encouraging 'teamwork' within your security infrastructure ever be that easy? With the correctly automated approach, it can be. Certainly, this should include a licensing model that doesn't unduly complicate or hinder the evolution of your network, as well as a technology set that brings best-of-breed security capabilities but without the attendant truckload of hardware, and continuing frustrations over network latency.

This advisory describes the process and impact of automating security consolidation to achieve optimum benefits to your security infrastructure and to your business as a whole.

- **Situation Analysis**
 - **Before Automation**
 - **After Automation**
- **The Business Criticality of Automating Security Consolidation**
- **Automation Impacts**
 - **Running Costs**
 - **Time/Labour**
 - **Space & Power**
 - **Decision Making**
 - **Uptime**
- **Implementing Automation**
- **Fortinet Solutions**

Situation Analysis

Before Automation

- Datacentres are overcrowded with multiple security appliances from multiple vendors all taking up valuable space and energy. As well as eating up significant budget, this can be especially detrimental to IT departments meeting CRC (Carbon Reduction Commitments) targets on behalf of the organisation as a whole.
- Despite investing heavily in specialised, high-specification standalone security solutions, organisations are vulnerable to sophisticated, blended threats (such as those derived from Web 2.0 applications) which exploit the gaps in the armoury.
- Multi-vendor infrastructures escalate management overhead by consuming time, distracting IT staff and duplicating efforts on supplier relations.

- Licensing costs are high with per-user licensing models that spring from single vendor point solutions, and the process of ensuring the appropriate level of licensing coverage is an administrative burden.
- Network latency and delays in application response times are the direct results of deploying a large array of layered security systems, creating bottlenecks that provoke expensive investments in higher capacity network infrastructure and connectivity made in an attempt to over-compensate.
- Business scalability is constrained by the complexity of the silo'd security infrastructure and ongoing management/reporting can only be achieved by duplicating these processes.

After Automation

- The datacentre becomes more space and power efficient with elimination of unnecessary appliances, saving costs and increasing the organisation's ability to improve carbon efficiency.
- Vulnerability to new blended threats is decreased, through a tightly integrated and efficient security solution.
- Reducing the number of security vendors means that supplier management is simplified, and more time is freed up to concentrate on innovative projects, whilst any technical issues are identified and dealt with more quickly.
- Replacement of per-user licensing models with a 'per-box' licensing approach results in significant savings for the IT department, as well as reduced administrative burdens.
- Integration of multiple security functions means that performance is optimised, and with each element working in sync with one another, latency is reduced.
- Flexibility offered by consolidated, integrated security means that IT departments gain the ability to scale security infrastructure with the needs of the business.

The Business Criticality of Security Consolidation

With Web 2.0 applications and social media becoming increasingly integral to business communications, the likelihood of businesses falling victim to new sophisticated, blended threats through these new avenues of attack has increased. Adopting a consolidated security solution composing essential security functions that are all tightly integrated, is vital to maintaining ongoing resilience to counter the evolving threatscape.

A security solution that is intelligent, fast and responsive is an essential element needed to maintain business continuity. By consolidating security solutions, organisations can achieve cost effectiveness without impinging on business performance. Consolidation of security solutions means optimum security is achieved as well as carbon efficiency, reflecting cost savings across the board.

Automation Impacts

Running Costs

HIGH 😊

By following a 'per user' licensing approach to security requirements, costs are unnecessarily high. The impact on both budget and time is an expense that can be dramatically reduced by implementing a cost effective per-box licensing model. In addition, with the capability to turn single functions on and off at your convenience and according to business needs, more flexibility is at your disposal.

Introduction of a multifunctional security appliance/s to automate your security needs will in turn reduce the total cost of ownership. By cutting down on number of physical appliances in use, IT departments can reduce costs involved in the running and upkeep of security.

Latency problems can occur when multi-vendor solutions work in silos and out of sync, making vital data slow and inefficient. With a consolidated, well integrated solution this can be substantially minimised. Budgets no longer need to be wasted on attempts to over-engineer faster throughput; IT departments can achieve optimum security speed from the get go.

Time/Labour

HIGH ☺

Individual vendor contracts can mean countless hours spent on managing suppliers. By reducing the number of vendors, management is simplified significantly; one contract, one bill and one training regime, in turn this saves the IT department endless amounts of time to be put to better use.

The process of maintaining multiple systems is time-consuming and complex, requiring a high threshold of skills spread thinly across the IT department. With a consolidated security solution, the skills barrier is lowered, allowing skills to be distributed widely.

It can be hard enough to maintain upkeep of individual security functions as it is, but when they are all in different places, and with each appliance built from entirely different proprietary codes, management becomes extremely complex. With each function communicating with one another, implementation is fast and effective and time that would have been wasted on the upgrading process and other essential maintenance tasks is ceased.

Space/Power

HIGH ☺

Consolidation of point products into multifunctional appliances is an opportunity for security to occupy far less space in the datacentre. If IT departments are using a hosted infrastructure there will be a reduced strain on available space and there may be no need to pay the overheads involved with third party suppliers.

Those that have embraced server virtualisation (studies show 90% of UK organisations are looking to in the next 12 months) need to do the same with their security. The 10% that are left behind may find themselves faces with unnecessary expense that could have been avoided. For example; with CRC coming into play, financial penalties for using up too much space and power and not meeting targets will be high.

Decision Making

MED ☺

Adapting to a consolidated security strategy means that scalability is optimised and IT decision making becomes a lot easier and more flexible.

If you can't measure it, you can't manage it. Consolidation of security solutions gives greater visibility and the ability to monitor and analyse performance as well as potential vulnerabilities. The advantage of management tools that provide a clear view of the goings-on of the entire network is paramount for efficient and effective

IT decision making. Having automated clarity and control of multiple functions will itself prove to be a key decision making tool.

Uptime

MED ☺

Improved security means improved uptime. The benefits of having each individual security element working together at optimum speed, means even less chance of any downtime occurring.

With new and sophisticated blended threats emerging fast, coming from all angles to all networks, IT departments are in need of sophisticated wire speed security solutions to tackle them. Point solutions can often struggle when one fails to keep up with the next. Blended threats require a blended response.

Implementing Automation

Consolidation of tightly integrated security solutions can be established with comparative ease. The ability to try and test each aspect with a few keystrokes means that single elements of the solution can slowly integrate with your existing security infrastructure until your existing licences expire, without impinging on performance. This type of implementation process is almost impossible with any other kind of approach.

Fortinet Solutions

This advisory has been produced with support from Fortinet, a worldwide provider of enterprise network security appliances and the market leader in unified threat management (UTM). The FortiGate product range delivers ASIC-accelerated performance and integrates multiple layers of security designed to provide high-performance protection against dynamic application and network threats, whilst simplifying the IT security infrastructure. For more information, visit www.fortinet.com

Click [here](#) to download the FortiGate-620-B demo

Click [here](#) to download the Beyond UTM - The Value of a Purpose-Built Network Security Platform white paper

Click on the links to download information on the following Fortinet consolidated security solutions:

[FortiGate-110C](#)

[FortiGate-310B](#)

[FortiGate-620B](#)

[FortiGate-3810A](#)