

# Security Consolidation and Optimisation



Are you maximising the return on your IT assets?

Given the proliferation of security applications designed to combat IT breaches, you, like many organisations may be finding that the management of your security systems has become complicated, time consuming and costly. Are your desktops littered with applications for everything from anti-virus to encryption? Do you find yourself reactively deploying new services, which are often proven superfluous following an IT assessment? Are you confident that you're gaining maximum value from your current IT assets? In this article, we explore practical tactics to reduce costs and streamline security deployments through consolidation and optimisation.

## Drivers for addressing security infrastructure

Compliance requirements, mobility and remote access and the threat of malware all require robust security implementations. Typically, organisations have taken an organic approach to their security infrastructure. In response to emerging threats, point products are deployed against point threats. While this ensures immediate threats are managed, it often leads to infrastructures that are heterogeneous, fragmented and inefficient. This disjointed approach typically leads to high licensing, support and operational management costs. In addition, the configurations of many security devices have also evolved organically rather than strategically. Security policies evolve and grow incrementally and often configuration clutter that slows devices down and increases the administrative overhead in terms of operational and change management.

Undertaking a firewall assessment will reveal opportunities to **reduce** the size and **complexity** of the rule bases, leading to **better performance, simplified management** and administration and the **ability to reduce** the overall size of the firewall estate.

According to a recent survey by the ISSA Journal, the average number of rules in a typical firewall has increased sharply over the last seven years, possibly by as much as 500 per cent. In Dimension Data's own assessments, we have found that in many cases, up to 50 per cent of the rules in a typical firewall are not used. The result is a sub-optimal firewall estate with higher than necessary utilisation rates.

Ten years ago many organisations didn't even have anti-virus software installed on the desktop. Today, the typical desktop is cluttered with security software including personal firewall, VPN, anti-spyware, anti-virus and host-based intrusion detection/prevention. Unsurprisingly, this results in high license and support costs, cross-vendor incompatibilities and high software maintenance costs.

So what steps can you take to ensure that your security investment is fully exploited and future investment is optimised, while maintaining and improving your existing security levels?

## Steps towards security consolidation and optimisation

### Unify the desktop

The number of end-point security solutions has increased significantly in recent years as vendors have introduced new products in response to new threats and changing security requirements. Personal firewalls, VPN clients, host-based intrusion prevention, anti-virus and anti-spyware all

proliferate on our desktops, resulting in multi-vendor, multi-agent platforms. This environment leads to various issues which scale proportionally in relation to the number of users:

- Licensing costs are a major component of the desktop total cost of ownership and increase linearly in proportion to the number of users
- Multiple vendors and software agents increase the complexity and risk of incompatibility at the desktop and therefore increases the number of helpdesk calls. Helpdesk calls typically cost organisations between \$10 and \$30 per call and the average user will make 1.5 calls per month to the helpdesk. For a 500-user company, this equates to a startling \$180,000 per year
- Software updates are often a burden on the user, requiring user input and machine rebooting and/or resulting in reduced performance while the software is updating. This has an impact on productivity and can also increase the level of helpdesk calls

Moving to a single, unified client for the end-point can decrease IT costs and improve productivity in all these areas. Many vendors now offer a single security client providing protection against malware infection, personal firewalling and intrusion prevention. This simplifies licensing and software updates, removes the potential for software incompatibility and consequently reduces the number of helpdesk calls.

### **Unified threat management (UTM) and extensible threat management platforms**

Security components within the network can also be consolidated onto fewer appliances, which reduces licensing and support costs and improves operational management. Today's UTM devices are mature and appropriate for the SME market and medium to large enterprises and service providers. While putting 'all your eggs in one basket' may not work for every organisation, UTM devices can now be configured to be highly resilient with built-in redundancy and failover, making them suitable for mission critical, high-availability environments.

Although migrating to a UTM environment requires upfront investment, it can deliver swift returns through reduced licensing and support costs. More streamlined change and configuration management also leads to reduced operational management costs.

The UTM concept may also be extended to consolidate networking and security components. For example, it is now possible to deliver firewalls and intrusion detection/prevention integrated into LAN switches and routers, to deliver secure DNS and DHCP services within a router, and network access control and authentication into the core LAN and WAN infrastructure. A new breed of UTM products is emerging – extensible threat management (XTM) products – that provide a broader range of security capabilities and integrated networking functionality. Consolidation of networking and security provides additional cost saving opportunities and the support of major vendors means security doesn't have to be compromised.

### **Server consolidation**

Server consolidation often goes hand in hand with the discipline of data management and unsurprisingly, consolidating your servers allows for easier and more secure management of data transfer. Dimension Data recently helped the shipping giant, Inchcape, to consolidate its server estate and replaced 200 widely used Microsoft servers with four mega servers in key locations around the world. We have also worked with a large petrochemical company to remove

150 servers and replace them with seven mega data centre. By eliminating complex branch infrastructures and simplifying your network and consolidating servers, you can look forward to cost savings on data centre space and the ability to better manage your resources.

### **Virtualisation**

Migrating your security infrastructure to a virtualised environment is another tactic you can adopt to reduce your total cost of ownership for network security. Although requiring upfront capital investment, virtualisation of firewalls, intrusion detection/prevention systems and anti-virus gateways can significantly reduce licensing and hardware and software support costs. Considerable power, cooling and rack space savings can also be realised, especially in large organisations with extensive security estates. Assessments carried out by Dimension Data for large multi-national organisations have demonstrated savings in electricity costs alone of between \$150K and \$1M over a three year period, depending on the existing architecture. Distributed organisations such as major franchises and large branch networks can benefit from significant cost savings by collapsing per-site security appliances down to a centralised, virtual platform.

### **Firewall assessments**

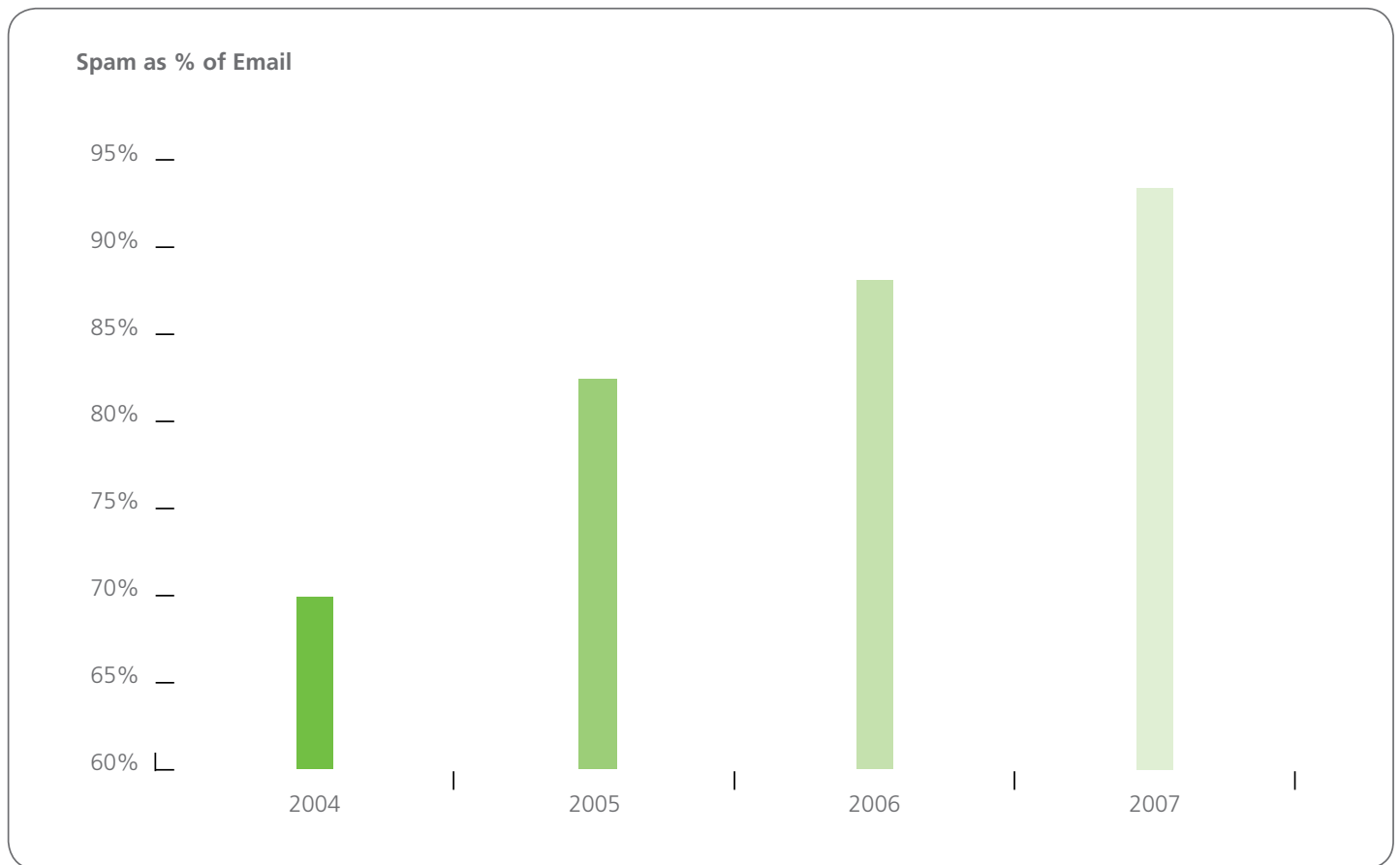
Firewalls are the cornerstone of any robust security implementation and involve

significant maintenance and management costs. Firewall estates grow quickly as new communication channels are opened up to the internet and third parties and firewall upgrades are often necessary to cope with increases in web traffic. However, many of these upgrades are unnecessary, driven by poor firewall performance as a result of complex, sub-optimal rule bases. Research undertaken by Dimension Data indicates that up to 50 per cent of a typical firewall's rule base is redundant. Unused rules are often not purged from the rule base, slowing the firewall down. Duplicate and overlapping rules also clog the rule base leading to a perception that the firewall needs upgrading when, all that is required is some basic 'housekeeping'. Undertaking a firewall assessment will reveal opportunities to reduce the size and complexity of the rule bases, leading to better performance, simplified management and administration and the ability to reduce the overall size of the firewall estate.

### **Security as a service (SaaS)**

SaaS solutions provide cloud-based services as an alternative to traditional customer-owned CPE solutions. E-mail and web security, security event and log monitoring, vulnerability management and denial of service protection all lend themselves well to SaaS solutions. Removing viruses, malware and SPAM from e-mail and web traffic in the cloud rather than on-premise frees up significant bandwidth and may

Vulnerability management and the management of firewalls and intrusion detection/prevention devices is also **often improved** via SaaS solutions **thanks to the 24x7 capabilities** and **highly skilled technical resources** offered by SaaS providers.



Credit: Barracuda Networks

delay, or remove completely, the need for upgrades to internet connections. Analysts estimate that today, approximately 95 per cent of all e-mail is unsolicited. Downloading SPAM over costly internet connections and processing it on-site consumes precious bandwidth and gateway processing cycles. Moving this function to the cloud can eliminate 95per cent of email traffic before it reaches your site – immediately improving performance and reducing the need for high performance e-mail filtering on-premise.

Filtering in the cloud can also improve security by preventing malware from reaching the corporate network edge. Vulnerability management and the management of firewalls and intrusion detection/prevention devices is also often improved via SaaS solutions thanks to the 24x7 capabilities and highly skilled technical resources offered by SaaS providers.

### **Leasing**

Leasing can provide CAPEX reduction benefits similar to those offered by SaaS while providing CPE-based, customer managed security implementations. Many security vendors now offer their own leasing options, enabling you to benefit from the best technology for a fixed monthly, quarterly or annual fee. Several leasing schemes include technology refresh options, future-proofing your investment and providing long term budgeting visibility and control.

### **Bandwidth optimisation**

WAN optimisation technology and security functionality are converging. This new breed of secure bandwidth optimisation products reduces bandwidth demand while maintaining the security of the WAN. Implementing this technology can delay or eliminate the need for bandwidth upgrades. It can also prioritise the performance

of mission-critical applications over less important ones such as web browsers, thereby offering further productivity gains.

### **Conclusion**

Now is the time to re-assess your current security architecture and adopt a strategic, rather than organic, approach to the evolution of your security infrastructure. By enhancing your understanding and visibility of your security estate, you'll be in a position to capitalise on your current assets and realise near immediate benefits through a range of security consolidation and optimisation techniques. Whether it is a simple firewall assessment to remove redundant rules and improve performance or an investment in UTM devices to reduce licensing and support costs, real business benefits and savings are well within your reach.

**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • GHANA • KENYA  
MOROCCO • NAMIBIA • NIGERIA  
SAUDI ARABIA • SOUTH AFRICA  
TANZANIA • UGANDA  
UNITED ARAB EMIRATES

**ASIA**

CHINA • HONG KONG  
INDIA • INDONESIA • JAPAN  
KOREA • MALAYSIA  
NEW ZEALAND • PHILIPPINES  
SINGAPORE • TAIWAN  
THAILAND • VIETNAM

**AUSTRALIA**

AUSTRALIAN CAPITAL TERRITORY  
NEW SOUTH WALES • QUEENSLAND  
SOUTH AUSTRALIA • VICTORIA  
WESTERN AUSTRALIA

**EUROPE**

BELGIUM • CZECH REPUBLIC  
FRANCE • GERMANY  
ITALY • LUXEMBOURG  
NETHERLANDS • SPAIN  
SWITZERLAND • UNITED KINGDOM

**AMERICAS**

BRAZIL • CANADA • CHILE  
MEXICO • UNITED STATES