

Welcome to the cold but clear winter edition of our newsletter — what we're doing and what we see happening.

## Intrusion Protection: Reducing the Cost

As the market for intrusion detection and protection has matured, customers have started to reject the original approach of installing relatively complex software on to separately sourced UNIX or Windows systems. They want a sensor supplied as a ready-to-go appliance that can be put in the rack with a minimum of effort.

### I Don't Want To Be Doing This!

Let's consider some of the issues that arise with implementing a software-based system.

First of all there's the purchase price. Not only is buying separate components inherently more expensive, there's also the likelihood that you end up paying for components that you don't need in a sensor.

Coupled with this is the complexity of procuring software and hardware components, probably from different suppliers and maybe involving different internal teams.

But of most concern is the cost of building a new Solaris

or Windows platform and then installing the intrusion detection system on top of it.

Finally, there is the continuing cost of providing support for a system that doesn't really fit into the rest of the infrastructure — it's a network component that's a bit like a server but with some desktop characteristics.

Only after sorting out all these issues can the implementers start thinking about network security and begin the job of tuning the sensor to do something useful.

In fact, that's really the issue that needs to be addressed: the hassle of setting up and maintaining boxes often distracts people from the real purpose of the IDS.

### Introducing Proventia

To remove some of these hurdles, we are now offering the Proventia range of intrusion detection and protection appliances from Internet Security Systems.



This starts with the A Series, an intrusion detection appliance that does the job of a traditional RealSecure network sensor, but at a much lower cost, in terms of both purchase price and

installation and maintenance overheads.



The G Series is an in-line device that provides intrusion prevention, by automatically blocking malicious attacks. For those who know some of the history of ISS products, this is effectively "Guard in a box".

Finally, the M Series is an all-in-one device that integrates the firewall and the intrusion prevention system.

### Integrated Management

All Proventia devices can be managed by SiteProtector in the same way as existing RealSecure sensors.

This means that the choice is simple when extending RealSecure implementations: Proventia really is the only way to go.

### Idsec's Track Record

Our experience of providing complete, useful RealSecure implementations is unrivalled. Now we are starting to provide our customers with Proventia appliances where they would previously have

had to build sensors from scratch.

### Pricing

As we've said above, the real saving in using an appliance rather than a traditional sensor is in the drastic reduction in staff effort. But the Proventia devices are remarkably good value in themselves.

An entry-level Proventia G100 in-line intrusion protection appliance costs around £8,000, including one year's maintenance. For new deployments, we can supply a starter kit containing a G200, three RealSecure Server licenses, 25 RealSecure Desktop licences, Internet Scanner for up to 10 IP addresses and SiteProtector Fusion to manage the system — all for less than £15,000.

These are just examples: call us to discuss your requirements. ◀

---

## Idsec Develops Training for IDS Informer



We have seen an increase in the number of people looking to test their intrusion detection systems, and have

started selling the IDS Informer product from Blade Software.

This is undeniably a tool for technical staff, but user training is still important when people want to get up and running as soon as possible. Working with Blade Software, we have developed a short training course for the product.

The one-day, on-site course is available to anyone who is considering using IDS Informer. ◀

---

## Web Application Ready To Go Live? Really?

Over the past few months we've seen renewed interest in web application security testing.

Companies are requesting relatively short, focussed tests as part of their product launch cycle. These fit in between normal functional testing and the final decision on whether to go live.

It's fair to say that there is a now a much better awareness of security issues among application developers, perhaps because of the publicity gained by high-profile cases over the past few years.

We do still find some nasties, however: for example, injection of code into SQL queries is a reality out there on the web, not just a textbook case study.

In many cases, simply submitting a mangled URL

will cause an error that results in a stack trace, revealing all sorts of useful information to a potential attacker.

We realise that budgets and timescales are often very tight, but even a short black-box testing exercise can tease out problems that should never make it through to a live system. ◀

---

## About Us

Idsec is an independent consultancy specialising in network security. We have been providing an expert service to a wide range of industry sectors since 1997.

# Idsec

Idsec Limited  
31-33 College Road  
Harrow  
Middlesex  
HA1 1EJ

Tel: +44 (0) 20 8861 2001  
Fax: +44 (0) 20 8861 3433

E-mail: [info@idsec.co.uk](mailto:info@idsec.co.uk)  
WWW: <http://www.idsec.co.uk>