

## FEATURE

# Security with Michelin-star service

Paul Judd, Regional Director, Fortinet

As if understanding and responding to the evolving threat landscape wasn't a challenging enough task, the other equally troubling consideration for in-house IT security professionals, IT managers and indeed business owners is exploring the wealth of solutions apparently best-suited to deal with them.

After determining the scope of threats to your organisation, and specifying the sort of security functionality required to address them, you're confronted with a third hurdle – how would you like this security solution to be served?

Outsourcing the management of your security solution might seem quite appealing. But here you must face an abundance of options because hundreds of Managed Security Service Providers (MSSPs) are ready to answer your needs. Per seat, per month, per function – the idea of the MSSP is that you can get as much security as you want piped into your business, or at the very least have your site-based security infrastructures managed remotely. You're relieved of the nightmare of IT security, and can enjoy the benefits of a secure IT environment that lets you get on with core business operations.

It's like the service in a high-class restaurant where attentive waiters check every detail of your steak-rareness, water-gassiness and napkin alignment. If it's done perfectly, you are more than satisfied. Executed poorly and the effect becomes inappropriate and starts to feel unnecessarily expensive. Sadly, these polar opposites have crept into the burgeoning MSSP market, muddying the distinction between the best and the worst; the most relevant to your particular needs, and the least.

To help businesses through the minefield of MSSP alternatives, the following tips may offer some clarity

when making decisions about individual providers that could dramatically improve the effectiveness of an enterprise's security strategy.

## Who's running the kitchen?

The service available from a MSSP can only reach optimum level when the technology underpinning it is sound, otherwise – to continue with our restaurant analogy – it's like an expert waiter disguising the shortcomings of an errant head chef. It is critical to understand what underlying technology is being used to deliver managed security services, and the degree to which it will protect against future/emerging threats to business customers.

While the latest headline-grabbing security threat may often keep you awake at night, make sure that these actually apply to your business and that you have an actual need to mitigate a particular risk. By the same token, it is a daunting task to examine your entire set of applications and network infrastructure to determine exactly what managed services are needed as your security requirements change.

***"Ensure your managed security service provider can evolve with the dynamic nature of the security market"***

To protect against the unknowable or unknown aspects of your current and future infrastructure, ensure that



Paul Judd

the platform your provider utilises is multi-service and innovation-driven. Security technologies have been consolidating from 'product-orientated' to 'feature-orientated' with such rapidity that your only path to understanding could be reading three months' worth of security publications and distilling the various opinions. However, the matter would be easily settled by an innovative multi-threat security platform operated by your MSSP, mitigating the hype via an instantaneous software upgrade to already deployed units in the field. In short, ensure that your managed security service provider can evolve with the dynamic nature of the security market.

## Can I order à la carte?

You will likely have a range of security requirements that could include some or all of the following: firewall; anti-virus; web content filtering; IPS; anti-spam; etc. The idea that you might be forced to use four or five different specialist MSSPs (for one each security function) is quite ridiculous because many of the principal advantages of the MSSP model (ie, reducing in-house management overhead, complexity, capital investment requirements and skills) will have been defeated. A far more advantageous position would be to have limited managed security service requirements (just one or two functions), but be able to call upon an MSSP with a comprehensive suite of capabilities to 'grow into' if required.

As an example let's suppose you have an impending VoIP rollout planned



## FEATURE

for your organisation and the path you want to go down is a conversion to outsourced VoIP. This shouldn't mean security becomes an afterthought, so how can you implement security effectively?

It is far more cost-effective to implement both solutions from one provider than to go back and add security at a later date. Determine if there is an increase in risk to your infrastructure and if so, look to the bundled VoIP + MSSP option as your quickest route to implementation and most cost-effective solution. The same would apply for other non-security managed services that you are considering.

### Could I use you for all my catering?

Many enterprise organisations are choosing to rationalise their IT partner relationships from a large number of specialised partners to a smaller number of more broadly capable ones. The benefits of reducing the time and effort involved with restructuring partner management in this way are clear, regardless of whether your business objective is to streamline/simplify operations or to grow with the most efficient use of resources.

Often there are multiple components of your business – from security to other portions of the infrastructure such as telecommunications – that make good targets to roll under one managed services provider.

Weigh the trade-offs of enlarging an already complex outsourcing project against the cost of implementing a series of complex projects. Frequently, there will be much to gain by outsourcing the management of several aspects of your infrastructure and many components of your security needs to one provider. Overall this is shown to decrease cost and reduce the time to deploy/upgrade new systems and applications.

### Will you spit in my soup?

The restaurant looks great, the service is excellent and the food tastes won-

derful – so should you be concerned about what's floating on top of your lobster bisque?

The most important factor in considering an MSSP – regardless of whether it is a pure-play MSSP or another managed services provider with a suite of multi-threat security services and many more solutions to offer as well – is, can you trust it? Trust in this instance takes many forms:

- Can you trust the MSSP to provide the appropriate level of risk avoidance?
- Are there enough capabilities to seamlessly protect your most precious information assets?
- Is there an appropriate cultural fit between your organisation and the MSSP?
- Is the MSSP proactive in its approach?

Working with a trusted partner to determine the answer to these questions is the most important first step to make if you want a good experience when outsourcing your security needs to an MSSP.

So, to make your choice, don't hesitate to ask for a taste. Many MSSPs offer a 'free trial' or similar mechanism to test the service before you sign an extended contract.

### Write your own review

At the heart of any managed security service is the reporting, portal and notification that the subscriber receives as a part of the service. Ask the prospective MSSP to provide a demonstration of the reports associated with each of the security offerings. Ensure that the information contained in the MSSP's security reports is easily understood, actionable and segmented to each location where the security services are delivered – a single global report for a multi-location business that does not show where the security events happened is actually counterproductive.

Review the MSSP's notification mechanism and make sure that infor-

mation about major security events is relayed in real time. For example, a DoS attack against your hosting centre could still, while mitigated, impact the quality of your web-based applications. It should therefore be a requirement for any MSSP to notify the appropriate resources within a given end-user's organisation to ensure they can execute additional mitigation steps, should an attack escalate.

A portal that can be accessed anytime and anywhere by selected resources is critical for the smooth running of your outsourced managed services. Ask for a walk through of the portal and all of its capabilities as well. Also look for what is and is not covered as part of the Service Level Agreement (SLA) and get clarification on processes and escalation procedures.

### Five ways to test capabilities

To test the security provider's capacity and true capabilities before taking the plunge:

- Ask for a free trial
- Ask for a portal demonstration
- Ask for a walk-through of the security reports
- Ask for a walk-through of the notification capabilities
- Ask for a demonstration of the SLAs in action

### About the author

*Paul Judd is regional director of Fortinet, responsible for the UK, Ireland and South Africa. Paul has more than 20 years of experience in the technology arena, with an extensive knowledge and understanding of the evolution of the IT networking and security channels. He joined Fortinet in 2007, having learned his trade in organisations including Azzurri Data, Nortel, Extreme and most recently at Juniper Networks where he was responsible for application acceleration solutions.*