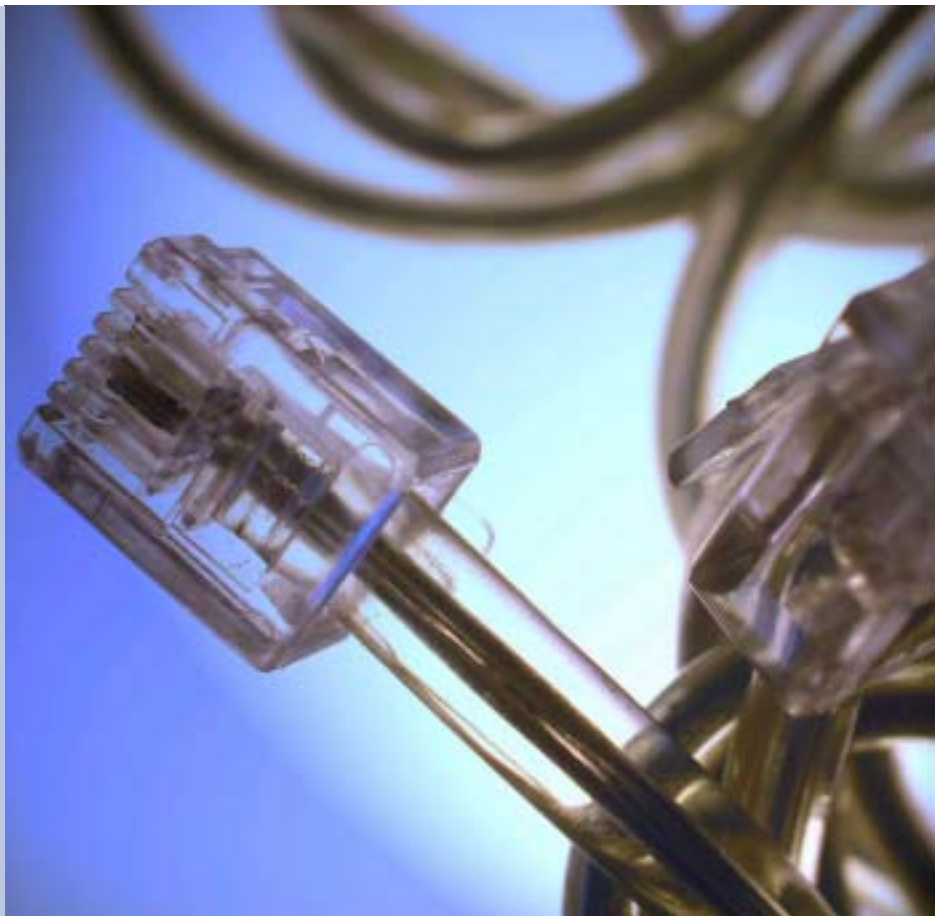


# New working practices and the security-aware network



## How the security-aware network can help IT departments manage the security challenges introduced by new working practices

Working practices are changing and few organisations are exempt. It's becoming genuinely hard to find any business today that doesn't encourage staff to work from home, to share communal or hotdesking areas, or to operate directly on customer and partner sites.

It's a strategy that offers clear organisational benefits but IT and network infrastructures need to respond. And, one thing's for sure – managing the inevitable security concerns is something that's guaranteed to be near the top of any CIO's list.

The emergence of the security-aware network can help. In combination with Identity and Access Management systems, the ability of a network to automatically adjust the way it operates – using knowledge of the roles, responsibilities and location of its users – can go a long way to reducing the risks businesses face in supporting these new approaches to working.

### **A top down approach**

One of the perennial concerns to network and security staff is that posed by laptops and the growing population of other,

portable devices that routinely move large amounts of corporate data outside the confines of traditional office boundaries.

It's not just the fear of confidential data falling into the wrong hands, either. An increasingly common threat is that with staff operating outside of a trusted environment, worms, viruses and other malicious code can more easily infect and damage the entire organisation as soon as the owner of an infected system next connects to the corporate network. The growing use of portable PCs in wireless hotspots or on customer premises – where security policies may not be as rigidly enforced – only serves to compound the problem.

Solutions do exist and approach the problem from different perspectives. As with almost any discussion involving security, though, a combination of countermeasures leading to a *strength in depth* approach is to be recommended.

Policy and education are a good place to start. Clearly, if employees – particularly those working offsite for the first time – are unaware of the potential risks, it's optimistic to expect every one of these

users to work in a totally secure manner. HR and compliance staff will also stress that unless a policy has been well communicated to employees, disciplinary action can be difficult to impose.

Many organisations are now using interactive computer-based training solutions to specifically target users such as home workers that present a higher security risk than others. Solutions not only educate staff in company policy and industry best practice, but can also regularly check that comprehension remains high. Individuals or teams that fall below acceptable levels can be easily identified and remedial actions planned. Such information is also useful evidence to auditors that a company's security awareness procedures are effective in reducing risk.



wireless networking, remote access or through B2B applications using Web Services. This is where technology – and the security-aware network in particular – has a role to play in both risk mitigation and incident response.

Incorporating security intelligence within the network itself introduces a number of key advantages. First, by involving the network in the authentication process of users, the network is able to more accurately identify suspicious network activity based on expected patterns of usage for the type of user involved – and the role they fulfil. It's certainly a major advance over the basic concepts employed in first generation intrusion detection systems.

Secondly, allowing a network to interpret and enforce an Acceptable Use policy

**“Many organisations are now using interactive computer-based training solutions to specifically target users such as home workers that present a higher security risk than others.”**

Interactive training solutions can also help ensure that where incidents do arise, staff are knowledgeable in who to report details to, what information is required and, importantly, how to preserve evidence. Any security professional knows that speed of response and quality of information are all important in minimising the potential impact of a security breach.

#### **Perimeter - what perimeter?**

One of the more fundamental implications of the working practices being discussed has been to question the effectiveness of the traditional perimeter security model. IT organisations are starting to recognise that, whilst a firewall-protected perimeter still has value, it no longer affords sufficient protection against threats that can be introduced from

means that the availability of business-critical network services can be much more closely mapped to identifiable parts of an organisation. This means that a business operating hotdesking areas can now restrict the network access provided at desk positions to basic services only but dynamically enhance these based on the profile of a user once they've been correctly authenticated.

It's a useful capability that affords other benefits, too. With more and more companies employing contractors and temporary staff – or simply needing to provide temporary IT facilities for visitors – being able to provide basic Internet services for non-employees, without the fear of them comprising an organisation's security policy, has significant appeal.

Some network products support even greater degrees of granularity and can, for instance, restrict the use of specific network services based on a user's location, time of day or the type of device in use. This makes it possible to constrain the type of information accessed by portable devices or when an employee is working outside of their normal office location. It all helps to provide a visible demonstration of policy enforcement and compliance.



### Meeting the demands of the 24x7 world

A further advantage of the security-aware network lies in its ability to take proactive steps to reduce the potential disruption an attack can easily cause. It achieves this by automatically quarantining those parts of a network considered to be at risk.

Whilst such an approach may clearly have a localised impact, the advantages of automatically re-configuring a network to bypass infected areas affords major advantages to the organisation as a whole. It can certainly make an

important contribution in helping IT departments meet the service levels that they've committed to business units, partners and customers.

Maintaining the provision of network services in this way is of even greater importance in organisations that have integrated voice and data networking into a single, converged IP infrastructure. Losing a data network would always be bad enough, but losing voice communications as well would have

**“Maintaining the provision of network services is of even greater importance in organisations that have integrated voice and data networking into a single, converged IP infrastructure.”**

catastrophic repercussions. Just imagine the impact on a call centre.

### Conclusions

Technology, of course, rarely solves problems alone. However, in combination with educated staff and best practice procedures, the security-aware network can play a major role in helping organisations respond to changing working practices and, at the same time, help IT and network operations staff overcome the security challenges that are inevitably introduced.

### Key facts

- Speed of response is all important in minimising the impact of a security breach
- The traditional perimeter security model no longer affords organisations sufficient protection
- Involving the network in the authentication process allows it to more accurately identify suspicious activity
- A security-aware network can take proactive steps to reduce the potential disruption an attack can easily cause.

