



Communicating with Confidence: Choosing a Secure, Flexible Working Solution

In today's mobile, highly-networked world, workers depend on access to their office networks to retrieve data about their customers, colleagues and business projects. Whether they are salespeople on the road, organisations collaborating on projects or government departments accessing multi-source data, most professionals in today's workforce share information over the Internet via their office networks.

Along with the benefits of networked systems – easy information sharing and the ability to work wherever and whenever – comes responsibility. Professionals in all industries have the responsibility to protect their customers' (and their own) confidentiality. When professionals access their office networks and exchange information with other organisations, confidentiality is paramount, though not always easy to achieve.

The good news is that sharing information, central services and applications is becoming easier and less expensive for organisations to implement. On the other hand, not all run-of-the-mill networking solutions protect confidentiality as well as they should. In these early days of network communication, companies can become too focused on features and functionality and overlook key security functions. Although the capability to exchange information between agencies and organisations is critical, the security systems and standards involved vary considerably and may permit hackers, insiders and even criminal organisations to access your private data.


Security can be achieved more easily when employees access company networks from a secondary office or from company-issued computers. But that's rarely the norm. Increasingly, workers use equipment that doesn't belong to them, such as computers in Internet cafes, airport terminals and customer and business partners' offices. Even when workers use office-issued computers, it's vital that sensitive information is protected in the event that their PDAs, PocketPCs or laptops are lost or stolen. In this case, it's critical that the authenticity of the user is validated before information is released, and that the confidentiality and integrity of data is assured in transit. In allowing users to access sensitive data, communication routes must not open up other vulnerabilities.

So, what are the primary considerations for choosing the most suitable and effective network solution for your business?

Independent verification is key. To achieve an independent assurance ranking, manufacturers must subject their products to evaluation by an external body. A third-party independent assurance group evaluates the performance and quality of a product. They determine if the security mechanisms and functions achieve confidentiality and fulfil compliance regulations. Examples of trustworthy independent assurance vendors include Communications Electronics Security Group (CESG) in the United Kingdom and the US National Institute of Standards and Technology (NIST) in the United States.

Experience counts. When evaluating network products, consider whether the manufacturer has experience protecting sensitive information. Do they understand the security policies and procedures that the end-user community must meet? Will they provide pre and post sales support necessary to roll out and maintain a mission critical system? Do they have happy customers who are willing to provide references?

Industry knowledge can make a difference. While most network access solutions can be implemented for any business, you may benefit from working with a company that understands



your industry, particularly if you deal with highly sensitive data. For example, security requirements in the financial sector, healthcare and the public sector are often more stringent than in other industries. Ask if the manufacturer has experience developing products for your industry. Do they have customers within your industry area that you can talk to about their products?

Consider implementation and running costs. The cost of a secure networking system will no doubt be a key factor in your purchasing decision. The 'Total Cost of Ownership' of a system includes the implementation and running costs, not just the purchase price. Make sure your IT department has the bandwidth to run your system of choice. Many sophisticated security solutions require constant management and maintenance, so you may want to choose a solution that's easy to maintain. Remember, whichever remote access solution you choose, it must complement existing equipment without increasing overall business costs.

Do your homework. Choosing the right secure network solution is an important decision, so take the time to learn about the available options. Each product, such as Secure Socket Layers VPNs, IPSec VPNs and application layer security gateways, has ideal user scenarios and offers specific benefits depending on your company's requirements. Make sure you understand the technological distinctions between different products (VPNs, firewalls, intrusion detection, virus checking, user authentication, etc.) and take the time to research vendors and their support options. Have a clear understanding of what you will use the product for – secure collaboration and information sharing, data separation, application access, etc.

The emergence of VPNs and networking technology has changed the way we work and makes it easier for professionals to collaborate and share information no matter where they're located. As the number of network products on the market continues to rise it has become more important than ever before to choose the right solution for your business. If your networking solution doesn't facilitate flexible working and protect confidential data, then you're doing a disservice to both your business and your customers.

About Stephen Lewis

Stephen Lewis is a Vice President of Product Management at AEP Networks. AEP Networks manufactures a range of innovative secure networking and application access products that meet the highest confidentiality, integrity and user authentication requirements. AEP products protect sensitive and classified information in large-scale projects with up to 100,000 users in the UK, Europe and North America.

For More Information contact:

David Riley
Director of Marketing EMEA
AEP Networks
Tel: +44 (0)1442 458613
Email: david.riley@aepnetworks.com