

# How to Protect Your Organisation

[ By Sandeep Kokroo, Manager Networks, Alpha Data ]

**I**n today's business environment, access to information is vital in order for companies to remain competitive. As business networks expand thanks to technologies such as MPLS based networks, SSL, VPN's, and wireless access points so too does the exposure to security breaches.



The risk factor for security incidents resulting from any of these threats cost time, money, and possibly an organisation's reputation.

With multiple ways to access information today, end users can bring viruses, hackers, unpatched software, and unapproved applications into your network intentionally or unintentionally.

The risk factor for security incidents resulting from any of these threats cost time, money, and possibly an organisation's reputation. No amount of investment in security products such as perimeter fire walling, content scanning, anti spam, and anti virus can protect your organisation without enforcing end point security policies.

The following steps can help you enforce endpoint security policies to help protect your organisation and your employees:

**Step 1:** Define a detailed security policy, identify what endpoints need protection and define how they can be protected. As with any security guidelines, your initial objective is to reduce risk without having too much impact on your staff or infrastructure. Defining your security policy is an ongoing practice that will change over time along with your organisation.

**Step 2:** Select and deploy tools that will help you enforce your policy. (such as Proxy servers, Internet Acceleration Server ISA) These tools must have a presence on every endpoint (ie. PC's and laptops). Check all your machines for compliance with these tools; machines that do not comply are a breach to your network and security and should be quarantined until they are brought into full compliance.

You need to select the best tool that can allow

you to define and specify automatically, for example, if a user wishes to access and connect to your network wirelessly, then you don't want your administrator to repeatedly install a special application in your machine to allow the access – you need your tools to allow that automatically.

**Step 3:** Provide a self-service correction process – what this means is that you have less of a need for support staff to go to each endpoint to fix problems. Your users can carry on working without too much interruption to their time and relieves a load on your IT support staff.

This self-service process should be easy for individual users to handle on their own (you can send pop-up messages to users with messages such as 'you are not able to connect to the internet right now', or 'a virus has been found on your PC.' As with endpoint security, your correction solution must itself be secure and unable to be bypassed.

**Step 4:** Always monitor compliance and adjust your policy. Use external security auditors to review user compliance to your security policies and security product effectiveness. Questions such as are your users barred due to prohibited applications, is frequent non-compliance of your mobile users due to overly restrictive rules are crucial ones to answer during this step. Remember as in step one, your policies will evolve and change over time.

With the above steps in place you will be on track to greater security for your organisation and users.