# Informative guide to protecting the end point and preventing loss of information And How Symantec solutions can assist.

## Introduction.

This document is designed to provide an insight into Symantec's recent technology releases. And how they can assist an organisation to safeguard confidential information and add extra protection to the end-point (laptops and mobile storage devices alike).

The two topics although seemingly separate, do in fact have overlapping policy considerations, these issues are illustrated below:

## End Point Security (EPS):

Typically staff using devices such as laptops, USB memory keys, PDA's have proved problematic to protect as they face the same threats when operating outside of the corporate network as in, but don't have the protection afforded by the Corporate LAN. Consider that a staff member at a PC will normally operate inside a network protected by a gateway firewall; the firewall will block unauthorised ports, stop unsafe services and restrict sensitive information being passed to the internet. The PC will also benefit from gateway content controls to protect from virus and malicious code infection.

A laptop when operating remotely however will need:

1. Anti Virus protection that is both functioning and up to-date.
2. To ensure the web does not become an open door way for an intrusion.
3. To stop information residing on the laptop from being accessed by an unauthorised party.

Conversely staff with USB memory sticks, provide an unobtrusive route into your business for viruses - and another way out for sensitive company information. Laptops travel with workers wherever they go, providing a vital new line of productivity - and a massive security risk from information theft and from viruses when they come back to base. Most people would agree that  Viruses and information theft are difficult to fight when devices are outside the immediate control of your business for much of the time. Desktop PCs aren't safe either, just because they're within your office's four walls: their USB and Wifi ports are gateway for security threats.

**Data Loss Prevention (DLP):**
Information is the asset that most organisations entrust to IT systems, be it customer databases, financial spreadsheets, customer records or research & development data. The list is pretty much endless and IT is the medium where such data is stored, accessed and manipulated. As such information is not limited by location but by access rights to network resources. Either through ignorance or malicious intent, a staff member entrusted with sensitive information has the ability to manifest an information breach. Just a few examples are: CD with sensitive personal information that is lost in the post, or an email with confidential data sent to a competitor, credit card details, or brand embarrassing information disclosed to the public.

Managing data loss has three concepts:

1. Data at Rest (DAR) – ensuring Information that is residing on a storage medium can not be compromised:  ie protecting the information on a: DVD, CD, USB memory stick, Backup tape, laptops etc can not be accessed even if lost or stolen.
2. Access & Transport – providing safeguards to prevent sensitive information that is electronically sent or received from unauthorised interception.
3. Classification and Control – Its almost useless to have points 1 and 2 above without a system for defining what is confidential and what is not and at the same time a process for educating staff.

As explained in the previous sections the subjects of DLP and ESP are very closely intertwined and addressing one in singularity; one risks excessive expenditure and a less than comprehensive security posture.

Symantec have addressed these diverse requirements with three security solutions that address all such needs.

- **Symantec Endpoint Protection (SEP):** This combines the traditional agent based anti virus scanning and includes a desktop firewall, intrusion prevention and device control. Thus ensuring workstations and/or laptops operating outside of the corporate LAN can be adequately protected. In addition SEP includes policy based attached storage control, which for instance this would allow USB memory sticks to be completely blocked or allowed but with limited access rights. This same policy can be applied to wifi access, multiple NIC cards and in fact any interface. Further more SEP includes host based intrusion detection to defend against spyware, root kits and zero day threats that would otherwise slip past an anti virus scanner. A clever feature of SEP is to automatically recognise its location and apply separate policies accordingly.

e.g whilst out of the office allow WIFI but turn on the desktop firewall. Further more treat any new applications as possible malicious code and allow the ability to only accept pre approved USB memory sticks.

Versus when in the office disabling WIFI (as its not good practice to bridge the corporate LAN with the unprotected WIFI) Also to disable the desktop firewall and restrict any executables from running on any USB memory sticks.

- **Symantec Endpoint Encryption (SEE)**: addresses the DAR requirement as it encrypts hard drives, attached storage mediums (USB keys, hard-drives etc) as well encrypting DVD and CD's. It provides this as a modular suite so you can simply opt for just one part of the encryption if required and as its policy drive with global management console renders this invisible and effortless for the user.

- **Symantec Vontu Data Loss Prevention (SDLP):** Provides a solution for an organisation to classify and distinguish what data assets are of value, rank their importance associate a usage policy. Once in place the solution will scan and locate such data assets no matter where they reside on the network and where such data assets are leaking from, be it at the gateway (email, web, and ftp) or the end point (laptops, USB keys) alike.