

## CSTL's informative guide to End Point Security

Other Guides available are:

- End Point Security
- Network Best Practices

In today's frantic world, mobile technology isn't just for road warriors - we all rely on it, perhaps more than we realise. Every employee has a USB memory stick, providing an unobtrusive route into your business for viruses - and a 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. Viruses and information theft are difficult foes to fight when devices are outside the immediate control of your business for much of the time. And desktop PCs aren't safe either, just because they're within your office's four walls: their network links and drives are a gateway for security threats.

### What is end point security?

The "end point" is any part of a host that is outside or transverses the normal network security controls, either permanently or temporarily. Examples include:

- Laptop
- Home based office PC with remote VPN network access
- USB memory stick or any attached memory device (IPods for instance)
- Internally located PC that allows direct external wifi communication.

### End Point Risks

The traditional IT security posture has been one of a fortress style defence, where the majority of defences were placed at the gateway such as: firewall, access controls, AV scanning, content controls, strong authentication. This style was sufficient as the hosts that were being protected largely resided in the network permanently. The following illustrates why end point security has emerged:

- Companies require greater productivity from staff via enhanced working flexibility, such as being able to move in and out of the network with laptops as required. What happens to the data residing on the laptop if lost or stolen is one issue and another is if laptop is brought back into the network after being compromised whilst on the outside.
- As the cost of memory has reduced, capacity increased and physical format minimalised, devices such as USB memory sticks and media players have become prolific. As such it is not laptops that have the issues above but in fact any memory device that is moved in and out of the network.
- Wifi has emerged from an expensive and generally restricted protocol to one that can be picked up in most cafés, bars and public areas with little or no cost. Combine this with the fact that most new PCs and laptops come pre-enabled with wifi, effectively allows a network based host to communicate with the internet, bypassing the network perimeter controls.
- Remote access for staff has evolved from staff to include third parties such as customers, suppliers and parent company entities. These all require access to the network resources and are all outside the security policy or scope normally attributed to a staff remote access connection, because the IT department can not effectively dictate or enforce the security configuration of the third party's machine.

### CSTL Key Recommendations

#### Data at Rest

Classify data in terms of its value and treat it as an asset. Decide whether it should be allowed outside the network, and if so then identify where the data rests and encrypt such information. The locations may be laptops, home PCs and USB memory sticks. Our recommendation would be to support the use of the device within your network, then encrypt the data residing upon it.

There have been a few high profile media cases recently where organisations failed to protect data at rest. To name just two: the Nationwide building society were fined £980,000 by the FSA and M&S suffered laptop theft containing staff payroll details.

### **Control**

Apply access controls to systems to control and restrict devices such as USB memory sticks. Windows via registry settings can block services such as USB service, but this is problematic, difficult to maintain and unreliable (although still better than nothing). Solutions exist for better granular control and management. Some solutions have the ability to allow only certain memory keys and block others, while ensuring that the information saved on a memory stick is always encrypted. More complicated solutions apply control not just to USB based devices but to PCMCIA and IDE as well as NIC, Wifi and Bluetooth classes as well.

### **Audit**

Consider auditing device and information usage transport as this ensures misuse by staff is pin pointed, as well as allowing potential confidential data leaks to be highlighted early. CSTL provide a device audit service that can quickly and easily audit device usage across a network, its ideal for quantifying the predominance of I-pods, USB memory sticks, cameras, smart phone etc. Ask for the Audit Device fact sheet ([deviceaudit@cstl.com](mailto:deviceaudit@cstl.com)) for more information as it contains extract examples.

### **Enforcement – remote access**

Where remote access is supported and being diversified either to allow third party access or wider accessibility, look to enforce security on the connection prior to network access being granted. A scenario could be that a staff member needs to access an important file whilst half way across the globe from a hotel machine in a lobby kiosk (or a cyber café, or customer's workstation or a supplier's site etc). The issue is that the machine security state is unknown and could harm the network if a connection is permitted with it.

One solution is to enforce a set of security checks as the connection is attempted. This typically involves a scan for viruses, a check that the host has AV enabled and it is active and up to date, that relevant security patches have been applied and that the host is not connected to any other party at the same time of access. If all is verified then access is granted and the security of the network maintained, even though the access and the host is external and outside the company's own security policy.

### **Enforcement – internal access**

Similarly a laptop that is connected to the network after some time outside, should also have security policies verified prior to allowing network access. The risk is that the laptop has become infected or could provide a vulnerable point for attack if access is allowed. One remedy is to use a NAC (Network Access Control) solution. This would identify that a machine has requested access to the network, ensure it did not pose a risk and was in a secure state to connect to the rest of the network, before granting access.

### **Enforcement – protecting remote and mobile machines**

A laptop outside the network is vulnerable to attack from malicious codes (Virus, Spyware and Trojans) and hack attempts. The use of a desktop firewall or client security agent would afford a level of protection to such machines and help to prevent an issue rather than correct it when it next accessed the network.

**Our approach is one of consultative and education and welcome the opportunity to have informative and informal discussion with you, being independent from any single vendor allows us contrast the many options and provide real world insight.**

**You can request a meeting at our city demo suite or at your offices now on:**

**[security-info@cstl.com](mailto:security-info@cstl.com)**

**Alternatively for further information on Endpoint Security Solutions please contact CST on: 020 7621 7832.**