



Piece of cake



Pop Quiz. Do you know how many USB flash drives and other non-sanctioned devices are plugged into your network at this precise moment? Do you know where they are? Where they've come from? Where they'll go when they leave? Do you know what will be on them? Or what they might have left behind?

Thought not.

And for the uninitiated, that's the perfect business case for **Endpoint Security** – the first in iQ's Piece of Cake series...

What's the problem?

- **Intrinsic weakness**

Endpoints – essentially all end-user devices and their ports – are a network's frontier; the least guarded and therefore the most vulnerable places in the infrastructure.

- **Hidden threat**

They're particularly susceptible to removable devices such as USB sticks – which are small (and so easy to conceal), cheap, and abundant; they can also hold huge amounts of data whilst arousing zero suspicion. In other words USB drives are ideal for smuggling data and applications out of – or even into – a business.

Your customer database could leave the network, or a Trojan could enter it, completely undetected having simply bypassed your state-of-the-art and hugely expensive security perimeter, including firewall, IDS, IPS and everything else.

It's like closing, locking, dead-bolting, and alarming all your doors and windows but leaving your back door wide open.

- **Obvious solutions are not finite**

Common solutions include disabling USB ports via the BIOS or even by filling them with glue! These work but tend to be labour-intensive and expensive, and the user can still use alternatives like firewire hard-drives and recordable DVD devices.

- **Unacceptable disruption**

Disable a USB port for the user, and it's disabled for your support staff too. The dilemma becomes even more complex for users who need to use USB devices as part of their jobs.

- **Cultural disconnect**

Secure systems are less flexible than "unsecure" systems, but without continuity and competitive edge there's no business to protect in the first place. It is all too easy for security and line of business departments to end up on opposite sides of this divide.

What do I do about it?

There are several immediate steps the concerned business should take to protect endpoint desktops, laptops, and file servers.

- 1. Up to date anti-malware protection**
Install software patches and anti-malware software updates as soon as they're available
- 2. Stop the threats that bypass the gateway**
Restrict or ban unsanctioned mobile devices such as PDAs, mobile phones, and USB sticks from accessing the network wherever possible
- 3. Install a centrally-managed client firewall...**
... on the endpoint machine to negate any "day zero" threats and prevent hacker intrusion
- 4. Check ALL software before installation**
Including personal and brought-from-home apps. Monitor what software is installed where
- 5. Clamp down on cyber-slacking and unauthorised applications**
Instant messaging clients, VoIP clients, P2P file-sharing applications and the like waste time and bandwidth
- 6. User education**
Teach users about the full scope of the security threat; not just the dangers of opening unsolicited attachments.
- 7. Stop or limit uncontrolled surfing**
- 8. Ensure end-point security dovetails with gateway security**
Endpoint security should always be an integrated part of a broader, enterprise-wide security policy
- 9. Keep your ear to the ground**
Cybercrime is becoming ever more sophisticated, targeted, and rapid. The successful end-point strategy is the one that stays ahead of the game

How do I do that?

1. Develop an endpoint security policy

First get a clear picture of your potential threats and vulnerabilities by reviewing the status of all end-points, internal and remote. What's running? What's being accessed? What attacks are taking place, and where are you most vulnerable to them?

2. Decide on your approach

I. Point solutions

Deploying point solutions may solve the immediate problem, but it doesn't constitute an endpoint security policy. With IT forced implement and manage disparate,

uncomplimentary solutions, it is often very time-consuming and costly too.

II. Least possible user privileges

This provides good short-term security benefits, but carries a number of drawbacks – particularly in terms of flexibility and administrative burden – with end-users often needing special assistance to meet even their most basic needs. Many blanket lock-down approaches fail for this reason.

III. Build a real-world, business-specific model based on live usage data.

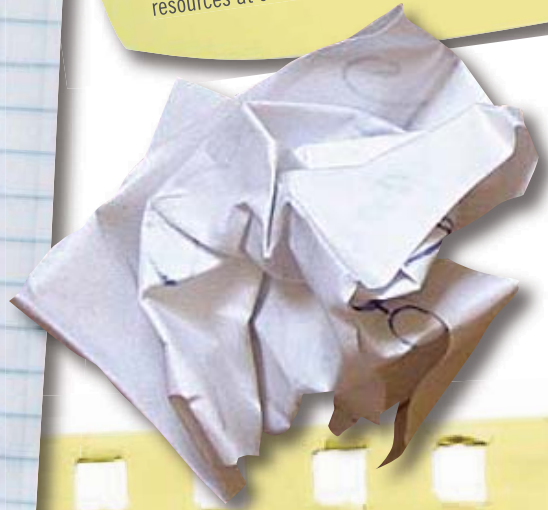
3. Translate your policy into technical procedures and activities...

... which must then be constantly reviewed, refined, and adjusted. Administrators might not like it, but it's good security practice. A one-size-fits-all approach rarely works however, especially with so many different devices now being used for network access.

Then What?

Put policies in place to govern who and what can access the network. Hybrids of the following models are common:

- **End user access control.** The user decides who and what accesses their resources (i.e. who sees their files, accesses their printer and so on.)
- **Mandatory access control.** The administrator or security officer sets the access policy and enforces it across the business.
- **Role-based access.** Resources are made available to users performing particular tasks or functions (only people in marketing can access the marketing file server, for instance.)
- **Rule-driven access.** Rules govern access on a user-by-user, process-by-process basis (for example a particular user may be allowed to access specific resources at one time, but not another.)



4. Enforce and manage these centrally

For true control, your strategy needs to be centrally managed and administered, but it must also be granular, malleable, wide reaching, and as automated as possible in order to reflect changes in the business and its threat profile.

5. Take a stance on user privileges...

... but don't be too miserly. Managing the types of activities performed on a particular machine, and the apps and resources it can access is generally a more sensible approach than total lock down. It tends to be more secure because it actively manages rather than passively disables. It also drives greater asset utilisation and end user flexibility.

6. Enforce them