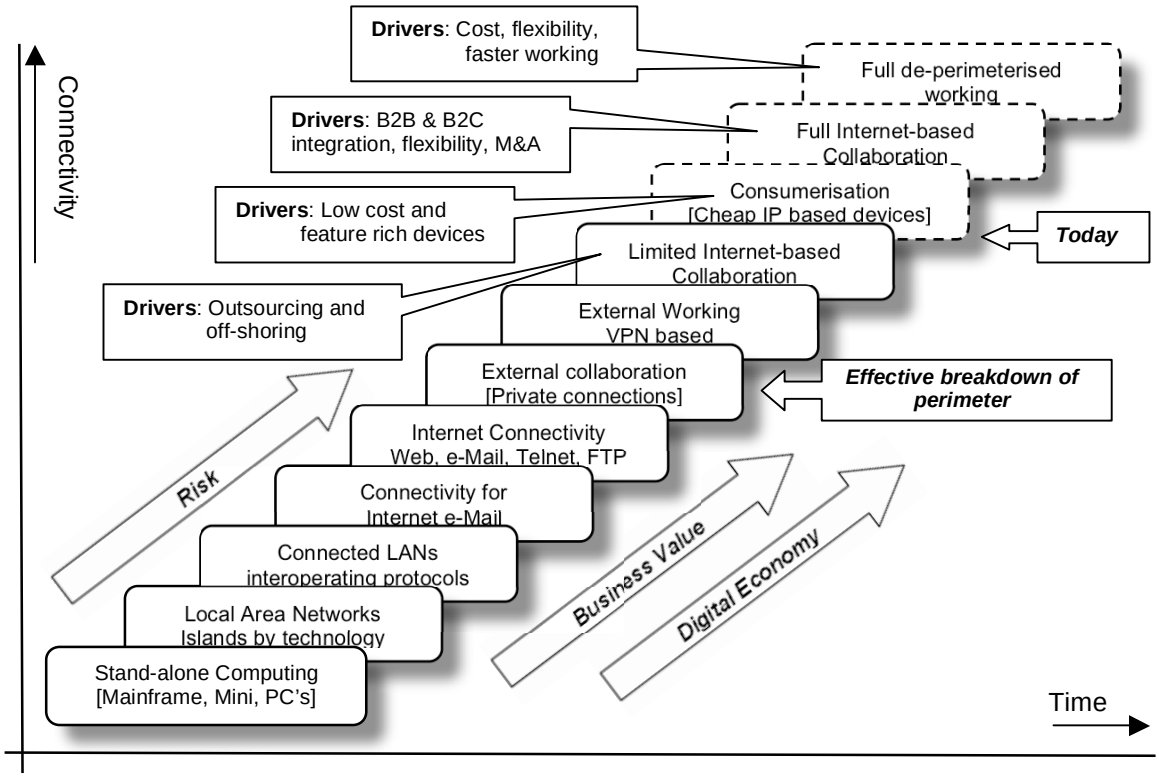
White Paper

Business rationale for de-perimeterisation

History

Computing history can be defined in terms of increasing connectivity over time, starting from no connectivity and developing to the restricted connectivity we currently have today, with islands of corporate connectivity behind their managed perimeter.



Today

Today there are key indicators that every organisation will be seeing within their business that indicate a de-perimeterised future:

- The increasing mismatch of the (legal) business border and the network perimeter as business becomes more integrated and their relationships less clear
- Business demanding to interconnect systems directly where B2B relationships exist
- The need to have good network connectivity and access to all organisations with whom you have a business relationship
- Distributed / shared applications across business relationships
- Increasing number of applications using technology that bypasses firewall security at the perimeter (typically using Web-based techniques that can legitimately traverse the perimeter)
- Increasing inability of traditional firewall and other network perimeter controls to combat malware that uses Web and e-Mail based techniques

The future

Many (and in some cases most) network security perimeters will disappear. Like it or not de-perimeterisation will happen; the business drivers already exist within your organisation, it's already started and it's only a matter of how fast, how soon and whether you decide to control it.

Drivers behind a disruptive technology

Current technology is aimed primarily to secure organisational borders, and then the network, reinforcing a 'perimeterised' perspective; this is at odds with the future business needs of most organisations:

- Business is demanding more connectivity outside the enterprise
- Consumerisation is driving towards an IP addresses on every electronic device, with those devices having ever lower cost with more 'business' functionality built in
- Increasing business 'relationships' of every type, from wholly-owned and partially-owned subsidiaries, to relationships with other business that are also competitors in other areas - all requiring connectivity
- The explosion of pervasive, fast, reliable, cheap Internet connectivity everywhere

Conversely de-perimeterisation will allow the realisation of many business-driven solutions.

Business benefits for de-perimeterisation

The current perimeterised architecture is perfectly adequate for an organisation that simply wants to operate inside its own controlled environment, with e-mail to the outside world. Unfortunately this organisation ceased to exist ten years ago as business mandated wider connectivity; yet most businesses continue to use an architecture adapted from that era thereby exposing themselves to an increasing and often unwise risk.

Worst still, many business and IT leaders, who rightly understand that good security is mandatory to doing business in the 21st century, have become victim to the perpetuated myth that good security starts (and in many cases ends) with a hardened perimeter, and also the fallacy that a hardened perimeter is required by whichever audit regimes they are subject to.

It is essential that businesses and IT leaders relinquish this preconception, and understand what their businesses would be able to achieve if the perimeter was not there inhibiting innovation, wide collaborative working, expansion and speed to market.

De-perimeterisation also enables new ways of working; probably unimagined (or considered and dismissed) by the business. Without the perimeter hindering business new ways of working can be quickly and cheaply implemented.

- Enable direct B2B integration of ERP systems with your major partners enabling better exchange of data and closer co-operative working
- Allow legal, commercial, and quality-of-service borders to align with the network and infrastructure implementation, paying only for the bandwidth and infrastructure the business actually needs
- Allow your partners, joint ventures, contractors etc. to access directly the data they need (and have authorisation to access) as simply as if they were physically connected at one of your offices or sites
- Allow direct electronic interaction with customers
- Move remote offices from slow and expensive managed networks to direct, fast and cheap local network connectivity, with better performance and large cost savings

Why this is a disruptive change

Until recently most device and network security has been additive with, over time, a series of 'sticking plaster' (band-aid) solutions being added. Interim solutions, such as VPN technology, are often applied everywhere as a 'silver-bullet' with little regard for whether doing so is architecturally cost-effective; only with de-perimeterisation are we able to realise an architectural mindset that will address these problems holistically.

Most network based security controls and 'solutions' such as Network Intrusion Detection Systems and Network Access Control are being added to shore up existing corporate networks in the misguided assumption that doing so provides 'defence-in-depth' when an ever-increasing percentage of an organisation's business is operating outside of the traditional perimeter.

Many organisations have tried to segregate the corporate network into security 'zones', each behind their own firewall. While this can provide an interim step in an organisation's transition to de-perimeterisation (we use the terms 'shrinking the perimeter' and 'micro-perimeterisation'), there is a worrying trend that some architects (and sales people) regard this as synonymous with de-perimeterisation. Widespread micro-perimeterisation in fact adds network and management complexity, points of failure, and bottlenecks for network traffic, and is not viable in the long term.

De-perimeterisation requires security to be at the heart of the organisation's distributed technology architecture; consistently implemented in end-user devices, application services, and surrounding the organisation's critical information assets themselves. Thus reinforcing what has been known for years but rarely implemented, that unless security is built-in from the ground up it will rarely be effective.

Architecting for de-perimeterisation

The removal of the border will not be achieved overnight. Alternative security must be implemented if the business is to remain secure while transition takes place. Techniques such as micro-perimeterisation and security services 'in-the-cloud' will enable transition. The good news is that de-perimeterisation technologies will happily co-exist in a perimeterised environment - which will aid transition planning and migration.

De-perimeterisation is simply the concept of architecting security for the extended business boundary and not an arbitrary IT boundary. It is not a solution in itself; however de-perimeterisation, properly implemented, is a set of enabling technologies that promises to:

- Reduce complexity by unifying and simplifying solutions, and generally reduce cost
- Enable business flexibility, cost-effective bandwidth and infrastructure provision
- Provide increased security thereby reduce business risk
- Enable multi-vendor outsourcing, simply and effectively
- Provide a simpler and thus more auditable environment
- Provide true defence in depth, from network through to the actual data

Business opportunity

With de-perimeterisation, as with most change, there are three options:

- Resist the change
- Let the change happen to you
- Leverage the change for maximum business advantage

De-perimeterisation is different to many other (technology) changes. To leverage effectively this level of fundamental change needs a conscious change in architecture. However de-perimeterisation is happening now, so to effect change in the timescale required it is essential that de-perimeterisation is part of strategic planning today.

Timely implementations of business-focused de-perimeterised architectures should result in a lower cost base. This will allow a more agile response to business need while competitors who resisted the change, or consciously (or un-consciously) simply let the change happen, are saddled with a legacy architecture that has a high cost of change simply to play 'catch-up'.