



Mobility In The Cloud: A Gathering Storm

Author: Simon Newby
Lead Architect – Public Sector Cloud



You hold sensitive public sector data – Sentinel protects it.

Sentinel by SCC not only provides faster IT implementation but also keeps your data secure to UK Government security standards, as the most established and cost-effective Cloud solution from the first Pan-Government Accredited provider, SCC.

For 40 years, SCC has been the trusted IT partner for the UK's critical national infrastructure.

Sentinel: keeping public sector data secure.

Contents

Mobility In The Cloud: A Gathering Storm.....	pg. 4
Bumps In The Road.....	pg. 5
The Silver Lining: Sentinel by SCC Mobility Services.....	pg. 6
Unlocking the Cloud, Unleashing the Workforce: Strategic Benefits Overview.....	pg. 7
Need to Know More?.....	pg. 8

Mobility In The Cloud: A Gathering Storm

The goal for Public Sector organisations today could not be clearer: with budget restrictions paramount, institutions around the UK have embarked on a massive drive for efficiency gains, seeking to reduce costs, boost productivity, and find smarter, more flexible ways of delivering frontline services.

Undoubtedly, Cloud computing has a significant role to play in that process – particularly in its ability to create workforce mobility. In tried and trusted systems it has the power to enhance staff efficiency, streamline procedural administration and enable key team members to operate in an environment where work is something you do rather than somewhere you go.

Driving down costs, reducing the requirement for real estate and offering technical departments a flexible, proven solution to key problems, the right Cloud can help public sector bodies meet many of their most pressing organisational goals.

It should be the perfect storm, yet recent fundamental changes in the accreditation scheme for new Cloud solutions have left many organisations uncertain of how to assess the credibility and security of the range of new services now hitting the market.

In such a scenario there can be only one solution. Public Sector departments need an approach with no question marks over it - a guaranteed solution that will not only work safely, securely, and reliably, but will deliver genuine business value at the same time.

The Engine Room Context – Key Challenges for CTOs

SCC has watched the secure remote access market develop and mature rapidly for most of the past 15 years.

Our experience is backed by Gartner research indicating recent trends – particularly in the consumer market - which, when combined with a raft of new ways in which users are leveraging mobility to change their approach to work, have had a disruptive effect. In turn providers across the marketplace have been forced to innovate, develop or even acquire fresh capabilities to meet a new breed of ICT challenge.

In the past it was enough to provide access to organisational systems at set times and set places. No longer. Mobile users today demand ubiquitous access to their data from any mobile device and expect it to work regardless of connection quality, and IT departments are increasingly under pressure to make it happen.

In this shifting mobility landscape, CTOs face a number of significant challenges:

1. Secure remote or mobile access requirements have evolved beyond the traditional 'road warrior' model, which focused solely on external access from remote locations, company provisioned laptops and use of two-factor authentication.
2. Organisations face significant challenges in assuring the identity of users and devices, while also experiencing demand to provide the convenience of single sign-on for access from a growing range of portable computing devices.
3. Long term planning for investments in secure access infrastructure now needs to consider expected changes in usage patterns, in addition to a diverse set of endpoint devices and ownership models.

Bumps In The Road

While the ability to work anytime, anywhere from any device can deliver increased collaboration, greater productivity and improved flexibility for employees, for many organisations, concerns around the expense and difficulty of implementing remote working practices remain.

End-user-driven connectivity in a Cloud infrastructure can often lead to degraded service and minimised benefits when organisations rely on mobile workers to manually establish connectivity. In turn, unbudgeted access costs and security holes only exacerbate the problem when mobile employees make expensive and unsecured connectivity choices from the field.

In this context, security and cost-conscious organisations are focusing on three critical mobility factors as they evaluate and deploy Cloud computing:

End-User Reliance and Connectivity

Delivering the greatest degree of flexibility to the mobile workforce depends on providing easy access to Cloud-based data and applications from anywhere at any time.

Today, users travel between various locations during the course of a work day – switching between a multitude of public, private, wired and wireless networks in order to gain access to corporate applications. This user-driven process requires mobile workers to manually select and connect to the best available network in a given location.

Leaving the connectivity process to end-users creates confusion around what network to select, what policies to apply and a series of how-to questions that often result in support calls to IT. While staff are trying to figure out how to get connected or gain support from their IT help desk, productivity is suffering.

Access Costs

Today's mobile workers typically access Cloud-based data and applications through various technologies like Wi-Fi and 3G either while on the road or working from remote locations such as hotels or home offices.

Unless this connectivity is carefully monitored and controlled, the cost of connecting mobile workers to Cloud-based environments has the potential to significantly offset the efficiencies you expect to gain from the cloud-computing environment.

In many cases these costs are unnecessary, for example paying for LAN or Wi-Fi fees when a mobile worker is in an area covered by their existing 3G subscription, using 3G when roaming internationally or using 3G when a free or low-cost Wi-Fi or LAN alternative is available.

Access Security

Despite many organisations having invested in a portfolio of end-point security solutions and corporate VPNs, data compromise is still a risk because of a variety of threats that stem from network bridging, visits to malicious web sites, downloads of malicious software, and use of open and unencrypted networks.

These threats persist despite existing security solutions when the process of connecting to wired and wireless networks is a manual, user-driven process.

The Silver Lining: Sentinel by SCC Mobility Services

Bridging the uncertainty of the disaggregated service approach currently being adopted across the Public Sector, SCC has been at the forefront of the Government's G-Cloud strategy since its inception.

We were the UK's first Pan-Government Accredited Cloud provider, and because of that experience understand the unique needs, pressures, risk mitigation strategies and deployment methodologies required to help organisations optimise and deliver the services they need.

Secured by design, and built under CESG's exhaustive scrutiny, SCC's Sentinel platform has evolved to meet all of the challenges public sector organisations face when adopting mobility and the Cloud - offering a variety of solutions to the challenges posed by an increasingly mobile workforce.

Remote Access Service

- Choice of department procured or SCC provided managed endpoint device;
- Access to services including:
 - Email
 - Files Services
 - Remote Desktop Protocol
- VPN with strong two-factor authentication and host checker to allow a customer managed device access to the service.

iOS MDM

- A specific process for provisioning the device in a 'known good state' before taking enterprise control;
- Device through-life management capability;
- Passcode Policies, remote device wipe;
- Restrictions on device features (e.g. camera);
- AppSelect that integrates with the MDM solution to provide users the ability to install apps from an organisations approved list.

Sentinel Connect

- Ultra mobile form factor;
- Plugs directly into the HDMI port of a monitor or TV;
- Pre-configured VPN client;
- Pre-configured delivery of VDI.

Virtual Desktop Infrastructure (VDI)

- Access to virtual desktops and applications
- Pro-active monitoring
- Productivity Tools – MS Office
- Decouple the desktop from the device
- Persistent or non-persistent user profiles

Unlocking the Cloud, Unleashing the Workforce: Strategic Benefits Overview

Cost-Effective

Reduced Capital Expenditure: Organisations deploying Cloud-driven mobility solutions can avoid upfront investment, paying for their mobility ICT as an ongoing operational cost.

Significant Cost Efficiencies: Because systems like Sentinel can be consumed as a service on a PAYG basis, organisations typically generate significant cost reductions by only using what they need, when they need it.

Example: In one project managed by SCC introducing high cost workers to mobility and easy data access generated cost reductions of between 25-30%, making an estimated £100m saving in its first year of operation.

Trusted & Secure

Secure by Design: While government accreditation is no longer compulsory, Sentinel by SCC service was built to comply with the Public Sector's strictest guidelines. Everything we've done has been subjected to CESG review, enabling customers to rest assured their systems and information are handled in line with best practice and current security guidelines.

Example: With various organisations across the public sector already utilising Sentinel Mobility Services, we are trusted to securely manage hundreds of mobile devices around the UK.

Enabling Technology

Speed to market: Because Sentinel Mobility services have been tried and tested in the Public Sector's most demanding environments, implementation speeds are far greater. Internal teams have no set up to complete, whilst our history of high-level accreditation status greatly eases the procurement process.

Greater Operational Focus: With background infrastructure operations managed and maintained off site, internal ICT teams are freed to concentrate on delivering refinements and improvements to the front line services they provide.

Example: SCC's work migrating 300 Highways Agency servers and back office infrastructure into the Sentinel environment – supporting almost 4,000 users – has enabled the Agency to focus on a range of current and future digital services.

Enabling Organisational Change

Enhanced Productivity: Because mobile workers can access essential data and services wherever they are, organisations can achieve significant improvements in efficiency.

Improved Collaboration: Always-on connectivity enables workers to stay in touch, participate in conference calls and share information rapidly and more efficiently.

Reduced Footprint: Flexible workforce policies allow organisations to rethink the way they accommodate staff – reducing real estate, energy and carbon costs in addition to removing the need for unnecessary travel.

Example: One healthcare organisation using Sentinel by SCC service has identified that deployment is generating productivity improvements and cost savings in excess of £15m a year – the equivalent to having an additional 400 clinicians per annum.

Need to Know More?

Moving any service to the Cloud takes a combination of expert technology management, strategic service management and solid transition planning to extract and maintain the value offered by Cloud infrastructure services.

SCC is a services company, not just selling servers and other hardware, required to realise the potential that drew the UK Government to the Cloud in the first place.

Engaging with SCC's specialist Cloud team means you will receive acknowledged thought-leadership, together with access to the knowledge and experience gained from multiple engagements with the new disaggregated service approach currently being adopted across the Public Sector.



Why SCC

We enable people to do business by planning, supplying, integrating and managing their IT.

We make IT work through partnership, knowledge and passion: trusted to run IT infrastructure and services for leading business across Europe for 40 years.

- Europe's largest independent technology solutions provider
- The technology division of Rigby Group PLC
- Profitable track record since 1975
- SCC Group revenues: £1.74bn
- UK turnover: £751 million
- Over 5,000 employees
- Supporting more than 5 million users
- Leading strategic partner to all key vendors
- CarbonZero for data centres and recycling operations

People do business. We make it work.

T: 0121 281 8618 E: online@scc.com W: www.scc.com