



Driving Public Sector
operational agility and
improving security with
innovative LAN and
SD-WAN technology



Introduction

Public sector organisations have never been under greater pressure. Whilst commercial organisations were forced to shut their doors during the pandemic, this was not an option for those providing essential services. As life returns to normal the public expectation of a quality service has not diminished.

If anything, there is an expectation that the public sector will now reduce the backlogs created by the recent dramatic events. Additionally, it is extremely unlikely that there will be any extra central funding to help organisations catch up. There are lessons to be learned from commercial organisations that have harnessed technological innovation during the pandemic period to drive efficiency and deliver improved customer service levels. As we emerge from the pandemic the priorities for the public sector are shifting from crisis management to improving the public service experience, reducing costs, rationalising buildings and maintaining staff morale.

Organisations of all types including schools, hospitals and local authorities are finding it challenging to deliver against increased public expectations in a way which is both cost effective and reduces the risk of failure. The communications network architecture of a typical public service provider is now highly complex and needs to facilitate connectivity for a diverse range of information and data sources. From legacy systems to a wide range of data networking end points which now extend to IoT and wireless devices, a new approach is required. There is a clear opportunity to help local authorities lower their operational costs by reducing the level of IT team support required with network multi-tenancy.

Evolution of this type of environment without inadvertently causing communications network outages is essential, as affecting the service experience is unacceptable.

Many traditional networks have been forced to evolve over the last 10 years as the proliferation of network attached devices has shifted from “wired to wireless” connectivity. This presents increased cyber-security threats, which result in a corresponding increase in security solutions overlaying the entire network. This has been further compounded by the trend towards consuming services from the cloud, often in a “multi cloud” environment. All this change creates the perfect storm for networks which simply were not designed to cope with such operational demands.

Although public sector organisations are often burdened with costly legacy infrastructure, this creates a great opportunity to transition to a more efficient future based on new technology.

The challenge is to effect this change in a controlled manner, which harnesses the best of the existing infrastructure and introduces the right amount of new technology to deliver operational efficiency, new revenue streams and greater agility.

Wherever organisations are in their digital transformation journey they are beginning to realise the value technology can add. It now has an important part to play in almost every aspect of the public sector operating model, from improving operational agility, to increasing information security and enabling hybrid working.



Improving operational agility

Public sector organisations are constantly challenged by the need to deliver higher quality while simultaneously expanding their range of services. They are being squeezed financially by reduced central government funding, which decreases operational income in real terms. So, the ability to efficiently react to change, whilst still maintaining service levels is essential. This organisational agility can only be delivered by identifying and executing initiatives that deliver incremental efficiency gains.

At the heart of today's innovative businesses is the digital infrastructure that allows customers and employees to efficiently interact via applications, collaboration tools and networks. This innovation can readily be applied to the public sector,

especially in the area of networking technology. In particular, advances in SD-WAN and LAN technology have allowed ubiquitous internet connectivity to be seamlessly integrated with private networking to create a secure, flexible fabric on which an agile organisation can be operated. According to a recent Cisco survey, 95% of enterprises are using or expect to use SD-WAN within 24 months.

Public sector network infrastructure is typically complex because of the range and age of technologies deployed and the number of services supported. This can be costly to operate and hamper the agility needed to respond to market and customer demands. Additionally, seamlessly integrating new technology can be challenging and expensive.

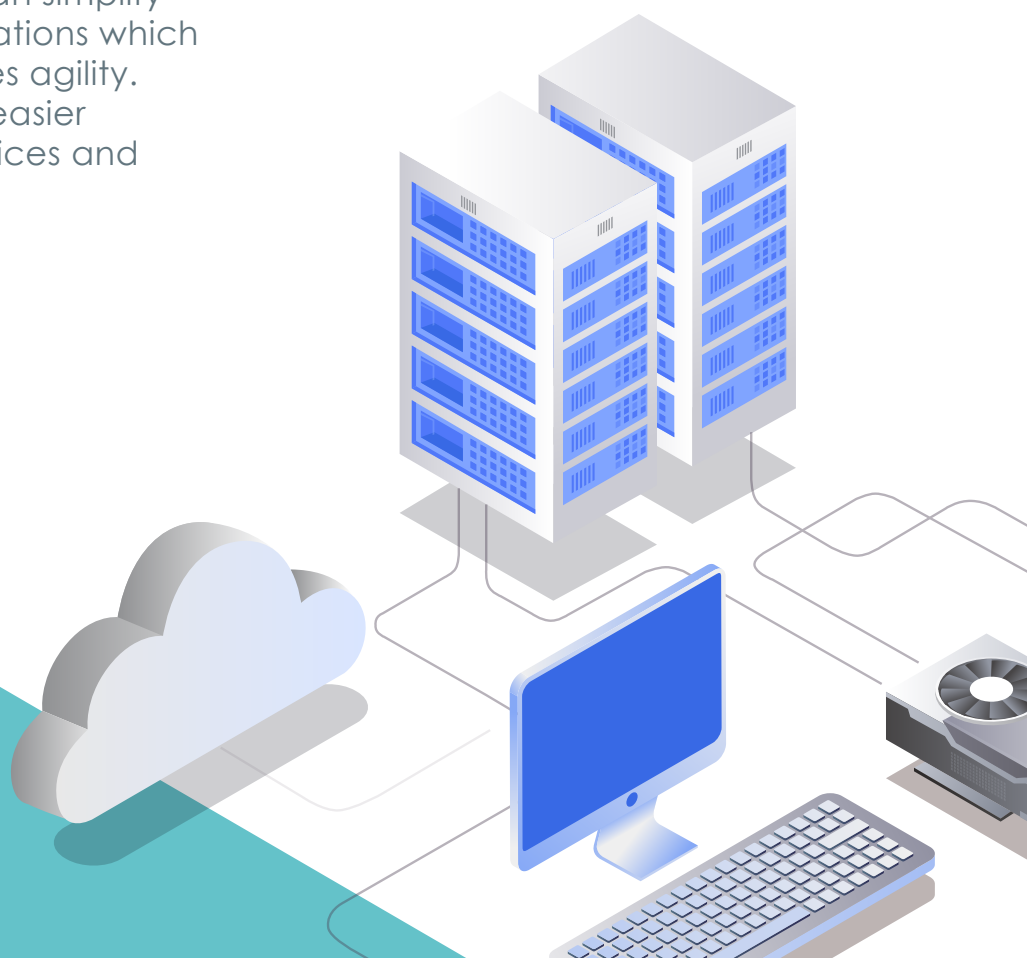


Unnecessary complexity can be overcome by deploying advanced networking technology which simplifies the orchestration and design of the underlying infrastructure. This new approach also significantly improves cyber-security and seamlessly integrates wireless devices by rigorous application of policy, rationalisation of network appliances and reduction in manual configuration. Through automation and service elasticity there is an immediate benefit in form of efficient management of new devices, users, locations, services and applications.

Implementing software defined networking together with advanced network orchestration can simplify management and operations which lowers cost and increases agility. This results in faster and easier deployment of new services and

improved application performance by delivering more bandwidth at a lower cost. In addition, software defined networking delivers advanced analytics which enables even better efficiency and greater application performance.

Maintel, in partnership with global network vendors Cisco and Extreme, are transforming critical network infrastructures for all types of public sector organisations. Now, you can deploy exciting new networking technology which meets the need to provide flexible, wired, or wireless access to public or private cloud services, without compromising cyber-security.



How to ensure flexible network access and protect sensitive information

Public trust in local government organisations is generally high, so any loss of personal data is unacceptable. Ensuring that there is protection from today's vulnerabilities and tomorrow's threats is essential. Network security, protected data, intrusion protection, virus detection and removal are essential if public information is to be secured. A recent Cisco survey highlighted that 68% of branch offices and roaming users had been compromised in recent attacks.

There is an accelerating transition to an ever more mobile and remote workforce, which is causing the boundary between the LAN and WAN to become blurred. The new priority is to carefully manage the security of this combined entity as a Campus. Technology such as hyper-segmentation can improve security by ensuring that each endpoint has its own fully isolated path to a specific application on a server.

Teams now need to be able to access all their applications and data wherever they are, which means there is a significant increase in the use of public networks and much greater risk of data loss and network penetration. SD-WAN networking solutions from Maintel in partnership with Cisco have embedded security architecture which ensures that information and applications are protected even when data is carried over the public internet.

Balancing the demand for remote access with the need to protect personal and sensitive data is challenging. This can be effectively achieved by defining role-based network and application access, then centrally managing all policies and configurations, with zero-touch provisioning to streamline policy enforcement and increase threat protection.

Having the flexibility to deploy the security that is needed by location and by user, combined with the ability to easily scale and centrally manage that protection across the LAN and SD-WAN is essential. Maintel have extensive experience of working with public sector organisations to design secure communications solutions that not only address the key challenges they face today but also help them quickly respond to future changes. Maintel deliver more agile communications solutions by bringing together state of the art LAN, Wi-Fi and SD-WAN technology, then seamlessly integrating it with existing infrastructure.

Managing hybrid working in the new normal

The pandemic caused a radical re-think of work as being only office or premises centric. As we return to a more normal working pattern it is likely that most roles will continue to be wholly or partly carried out remotely. This will result in sustained hybrid working and a significant corresponding change to the networking infrastructure that is needed to support it.

Over time organisations have industrialised the workplace to increase security and enhance productivity, to the extent that quality of the office environment is being taken for granted.

A recent Gartner report identified that pre-pandemic a typical enterprise might have had 5,000 people working across five offices. Now, they have 5,000 mini offices in people's homes.



So, the problem for the public sector is how to bring the security and reliability of the office working environment to potentially thousands of remote locations. Ensuring that remote workers have reliable network connectivity, secure access to applications and the ability to effectively interact with the public is essential. This problem can be solved by applying pre-set policies to users, to allow them rapid access to the applications they need.

There are two additional challenges for public sector IT organisations when managing widespread hybrid working:

1. How to connect staff securely to the applications and data that they need to perform their roles?
2. How to ensure that they have sufficient bandwidth and network performance?

SD-WAN solutions from Maintel allow you to overcome these challenges by providing encrypted access to applications over any public or private network. They also ensure that quality of service is maintained by dedicating bandwidth to key applications.

Maintel, in partnership with Extreme Networks and Cisco, have a proven track record of designing and implementing secure hybrid working solutions for public sector organisations. From auditing the existing infrastructure to planning network transformation, we can help you harness the power of innovative networking technology at scale.



Conclusions, case studies and recommendations

There is a great opportunity for public sector organisations that are willing to embrace new technology to improve operational agility and securely enable hybrid working. However, the key challenge is to introduce technological change in a controlled manner. Attempting to upgrade infrastructure too quickly can often result in unplanned outages and extensive service disruption. Conversely a slow transition can result in benefits not being realised quickly enough to have the desired impact.

The ideal network transformation retains the best of the existing infrastructure and combines it with innovative new technology to deliver a right-sized outcome for the organisation.

Liverpool City Council (LCC) chose Maintel and Cisco as trusted partners to assist with their data centre network transformation. Faced with the challenge of legacy infrastructure and business demands for increased resilience, flexibility and agility, they identified the need for an overhaul of the network core infrastructure.

LCC were developing new business applications to deliver to the workforce, including the deployment of a new virtual desktop solution which could not be supported by the existing infrastructure. Utilising Cisco's software defined Application Centric Infrastructure, they benefitted from operational simplicity, high availability, central network management and greater visibility of network performance.

This delivered increased agility, enabling LCC to meet the needs of their users, including the significant increase in remote workers because of the Covid-19 pandemic. Additionally, the solutions allowed them to take advantage of Cloud applications such as Office 365 and unified communications.

One of the largest social housing providers in the UK are Incommunities, they provide and maintain affordable high-quality housing for rent, shared ownership and for sale to across 22,000 households in the West Yorkshire region. Their corporate networking infrastructure needed to be upgraded to deliver new business critical applications.

Maintel, utilised their experience in deploying best of breed networking solutions to design and implement a new secure, resilient, core and edge Extreme network solution, including cloud-based Wi-Fi. This enabled both Incommunities staff and customers to access business critical data more effectively and improved the existing staff and customer experience.

Richard Frank the ICT Security and Communications Manager at Incommunities was delighted with the project:

"We approached Maintel to discuss the replacement of our legacy network. Throughout the process, Maintel's sales and engineering teams worked in partnership with us in a flexible, efficient and effective manner. They delivered a high speed, robust, secure Extreme network solution, that we and our customers can truly rely upon, now and in the future."

Maintel have over 20 years' experience of designing and implementing innovative public sector networking solutions. By thoroughly understanding our customers organisational goals, operational constraints and appetite for change, we ensure that benefits of new technology can be fully realised whilst at the same time minimising service disruption.



For further information about how Maintel can help you [click here](#) or reach out to us direct below:

+44 (0)344 871 1122
info@maintel.co.uk
www.maintel.co.uk
twitter.com/maintel
linkedin.com/company/maintel

