UK GOVERNMENT, GCHQ AND THE NATIONAL CYBER SECURITY CENTRE ADVISE UK BUSINESSES TO USE AN MSP FOR CLOUD AND CYBER SECURITY PROTECTION

With 90% of businesses having already migrated to the Cloud or Multi-Cloud the significant rises in cyberattacks mean that securing data has become a huge issue for every business as costs of attacks escalate and reputations are damaged. SD-WAN cloud, SASE security and data encryption are fast becoming essential technologies across all sectors.

Therefore, in January 2023 the National Cyber Security Centre (part of the UK governments GCHQ) have issued their advice for businesses to take proactive steps to protect themselves from cyberthreats – namely, by engaging a Managed Service Provider (MSP) for both cloud and cyber protection services.

Industries at the **top** of cyber-criminals' lists include:

- Healthcare
- Construction
- Manufacturing
- Legal
- Finance & insurance
- Energy providers
- Supply chain across all sectors nationally and internationally
- Multiple areas of the public sector, educational bodies, government departments and all areas of national infrastructure

However, predictions are that SMEs are also a growing target based on the cyber-criminals' assumptions that SMEs are less prepared or have less budget to incorporate technological protection, and that they face a growing risk of attack. We at SDWAN Solutions -an expert MSP and Service Integrator – strongly believe that every business should have affordable access to both progressive technologies that make business more efficient, such as SD-WAN Cloud as well as robust protection, such as SASE security and data encryption that makes all data unreadable to anyone without authorised access to it.

With the NCSC recognising the need for MSPs to supply these technologies to businesses it has issued guidance on how to choose an MSP for both Cloud and cybersecurity services.

A summary of the NCSC's key advice:

What your business needs to know before engaging an MSP

Before engaging an MSP, businesses need to have a clear understanding of their cybersecurity needs. They should identify the systems and data that are critical to their operations and the level of protection required for each. This will help them choose an MSP that can meet their specific needs.

Choose a reputable MSP with best practice methodologies

The NCSC advises businesses to choose MSPs with a proven track record in providing cloud and cybersecurity services.

Conduct due diligence
When considering an MSP, conduct thorough due diligence to ensure that they have the necessary technical and organizational capabilities to meet your requirements. Check their certifications, accreditations, and security controls.

Check the MSP's security practices
businesses should ensure that the MSP has robust security practices in place to protect their systems and data. This includes measures such as access controls, encryption, and monitoring. The NCSC also recommends that businesses ask the MSP about their incident response procedures to ensure that they can respond quickly and effectively in the event of a cyberattack.

Clarify responsibilities
Businesses should clarify the responsibilities of the MSP and themselves in relation to cybersecurity. This includes identifying who is responsible for what aspects of cybersecurity and ensuring that there are clear lines of communication in the event of a cyber incident.

Define service level agreements (SLAs)
Work with the MSP to define clear SLAs that outline the services they will provide, the expected service levels, and the responsibilities of both parties. SLAs should also include details on how the MSP will handle security incidents and breaches.

Monitor the MSP's performance
The NCSC recommends that businesses regularly monitor the performance of their MSP to ensure that they are delivering the agreed-upon cybersecurity and cloud services. This includes regular reporting on cybersecurity incidents and ongoing assessments of the MSP's security practices. Regularly monitor the MSP's performance to ensure they are meeting their SLAs and delivering the expected level of service. This will help you identify any issues early and take corrective action as needed.

Maintain oversight
Remember that **ultimately, your organisation is responsible for the security of your data and systems.** While the MSP can **help** you manage this, it is important to maintain oversight and ensure that your security requirements are being met.

In conclusion, the NCSC says that engaging an MSP for cybersecurity services can be an effective way for businesses to protect themselves from cyber threats and get their ideal cloud provision. Overall, using an MSP can be a valuable way to enhance your organization's cloud and cyber protection capabilities. The NCSC believes that by following their guidance, businesses can choose an MSP that will meet their specific cloud and cybersecurity needs and help them protect their business and their data against attacks.

How SDWAN and SASE Solutions Global can help you
We are a specialist SD-WAN, SASE, SDWAN Cloud and Data Assurance managed service provider, who deliver start to finish, on-budget solutions designed to your individual requirements using our multi-vendor ecosystems. We are regarded as being way above your average IT provider / reseller for expert knowledge, technologies and innovation, having developed 6 world-first innovations to date and are the only company on the planet with 2 MEF double accredited SD-WAN Subject Matter Experts. We keep companies of all sizes connected, protected and data assured, and work with all

types and sizes of businesses from SMEs to Enterprises and corporates, in both the public and private sector.

Right now, many companies are looking to reduce costs and complexity via outsourcing to specialist expert MSPs, who can help consolidate their network, cloud and security technologies. Other benefits of using an MSP include:

1. Free up IT teams' time
2. Bring free training and upskilling
3. Act as a highly skilled extension of in-house IT teams
4. Help retain & recruit customers who are increasingly checking security of data held by 3rd parties
5. Keep companies compliant on having robust cyber- protection as new laws roll out in 2023

Finally, we leave you with some cloud and security facts and stats and some links, to help you decide your course of action to protect your data and ensure your cloud operations continue without risk to your margins and reputation.

CLOUD & HACK FACT AND STATS

- **By the end of 2022 60% of all corporate data was stored in the cloud, up from 30% in 2015**
- **In 2023 90% of businesses are already using the cloud**
- **34% YoY growth of cloud services**
- **88% of UK businesses have suffered a cyber-attack in the last 12 months**
- **Just 11% of organisations have encrypted between 81-100% of cloud-stored data**
- **60% of SMEs do not survive beyond 6 months after a data breach and**
- **78% of UK enterprises have been attacked more than once**

Here are some links to our products that will assist in many areas raised by the NCSC:
https://www.sdwan-solutions.global/solutions/sdwan-cloud/
https://www.sdwan-solutions.global/solutions/security/
https://www.sdwan-solutions.global/solutions/sdwan-complete/sdwan-data-assurance/
https://www.sdwan-solutions.global/solutions/sase-select/

You can find out more about the NCSC's guidance, advice and compliance at
https://www.ncsc.gov.uk/
https://www.ncsc.gov.uk/blog-post/using-msps-to-administer-your-cloud-services
https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles/protect-data-at-rest-and-in-transit