MAINSTREAM digital
Cyber Security Solutions

Managed IT, Cyber, Telecoms and Network Services: Options For Consideration

Our Vision

Mainstream Digital Ltd, is here to be your business partner. With our years of experience and technology partners, we are able to take care of all of your IT, Cyber and Telecom needs to allow you to focus on your business. We are here to be your partner and help you succeed.

We do Tech and let you focus on your organisation.

Personalised Solutions and Support

We know your time is valuable and your technology has to be appropriate. That's why we take time to visit with each client and understand their business.

One Stop Shop

We can help deliver all of your technology needs, whether it be computer or network security, cyber, phone and voice, or cloud services.

Experience

We have over 275 years of experience in both large and small environments. We can listen to your requirements and match appropriate solutions to them, that meet your budgetary, compliance and cultural objectives.

A Customer Centric Approach

We want to partner with you long term. We are here to provide practical solutions, based on a consultative approach to ensure that we understand your needs and do our best to meet them.

Support

Helping you through your working day and addressing any disruptions.

Configuration Management and Monitoring Via RMM

A major component of the security and reliability of your systems, is the ability to identify issues as soon as they arise, to recognise when software is unpatched, and ensure compliance in all aspects of its operation. We utilise an RMM product as part of our portfolio of tools to allow us to give you the best calibre of support and monitoring, and in the most efficient way, keeping costs to a minimum and allowing us to offer you a number of ways of engaging with us.

Network Operation Center (NOC)

Our Network Operations Center (NOC) is watching your entire network, your servers, your internet connections, all of it. If a problem is detected we start remediation activities immediately minimizing any impact to your business. The NOC also proactively supports your environment, deploying security and software updates, and performance testing. You don't have to worry about if you are up to date.

Support Desk and Ticket System

Your technology is critical to your business success. We are here to support you when you need it. Available via phone, email and desktop app. Our team of 1st and 2nd line engineers utilise Freshdesk, the Gartner leading Help Desk solution, which enables you to contact us and raise a ticket via phone, email or portal. It also allows us to inform you of just how much we are doing for you and perhaps suggest areas of training.

AppGuard AGMS and Cybersmart Active Protect

Our AppGuard Management Console, allows us to monitor your deployed agents, gather logs, analyse and modify policy where necessary. Our Active Protect console allows us to monitor your Cyber Essentials compliance on up to 4 devices per user, inform you of issues and if required, address them. All this whilst monitoring your teams progress through Cyber Compliance training and policy adherence.

Included Benefits

Out of Hours Telecoms Call Logging and Support

If you have a Telecoms or connectivity issue out of hours then our OoO service will call you back to understand the nature of the issue and if possible triage at that point, whilst also lining up the traditional channels of support to follow as soon as we return to normal office hours.

Our ACS Network Monitoring Service

As a network or telecoms customer of Mainstream Digital, and user of our our Routers, you benefit from a free of charge network monitoring service, which can tell the status of your network at any given time and can flag with us that you are having a problem, even before you are aware. This allows us to give you the best possible response and remediation.

Our Offerings

Office 365 Tenancies with License Advice to Suit Your Requirement

Microsoft licensing is a complex subject and you need advice to ensure that you select the right product and with an eye for your requirements and your budget. We can assist you with this, and would normally do this a result of a discussion about your office functional requirements.

Sharepoint Services

Many organisations have need for a cloud based document database. In particular, council organisations have a common requirement for council document management. Sharepoint, as part of the standard licenses from Microsoft Office 365 is a powerful tool, that can be tailored to offer role and geographically controlled access and document version control, whilst minimising budgetary outlay.

Office Desktop Software (Office 365)

Your business relies on email and office documents. That's why we include a solution which includes, business email, file sharing, and encrypted email options.

Backup

Just because some of your data is in the cloud, it doesn't that you have no need of backup. We can include a solution to backup both cloud and on prem important data and we can offer advice on data recovery and business continuity.

A Framework For Cyber Compliance

As a fundamental starting point on your journey towards Cyber Threat Compliance and helping you to meet the requirements of the NCSC CAF (for local government), we offer Cyber Essentials and Cyber Essential Plus delivered in a helpful and assistive portal. Once achieved, we can help you to maintain it with Active Protect, to flag, train, provide self help or MSP delivered help on up to 4 devices per user.

The Peace of Mind You Need for Your Cyber Threat Landscape

NCSC and other government agencies are advocating a new paradigm in antimalware, as traditional detection based method lose effectiveness. Many Councils have already adopted this new approach. We offer the new paradigm - AppGuard - in use with MOD primes, developed by the US intelligence services and widespread in the US Department of Defence.

Looking for MSP services tailored to your business?

Think Mainstream Digital. Whether you're a small business or a large enterprise, managing a single system or multiple networks, we've got you covered. Get in touch today to find the perfect solution for your needs!

MAINSTREAM digital
Cyber Security Solutions

Mainstream Digital Ltd
Cirencester Business Park
Love Lane
Cirencester
Gloucestershire
GL7 1XD

T 0800 169 6000

E sales@msdigital.com

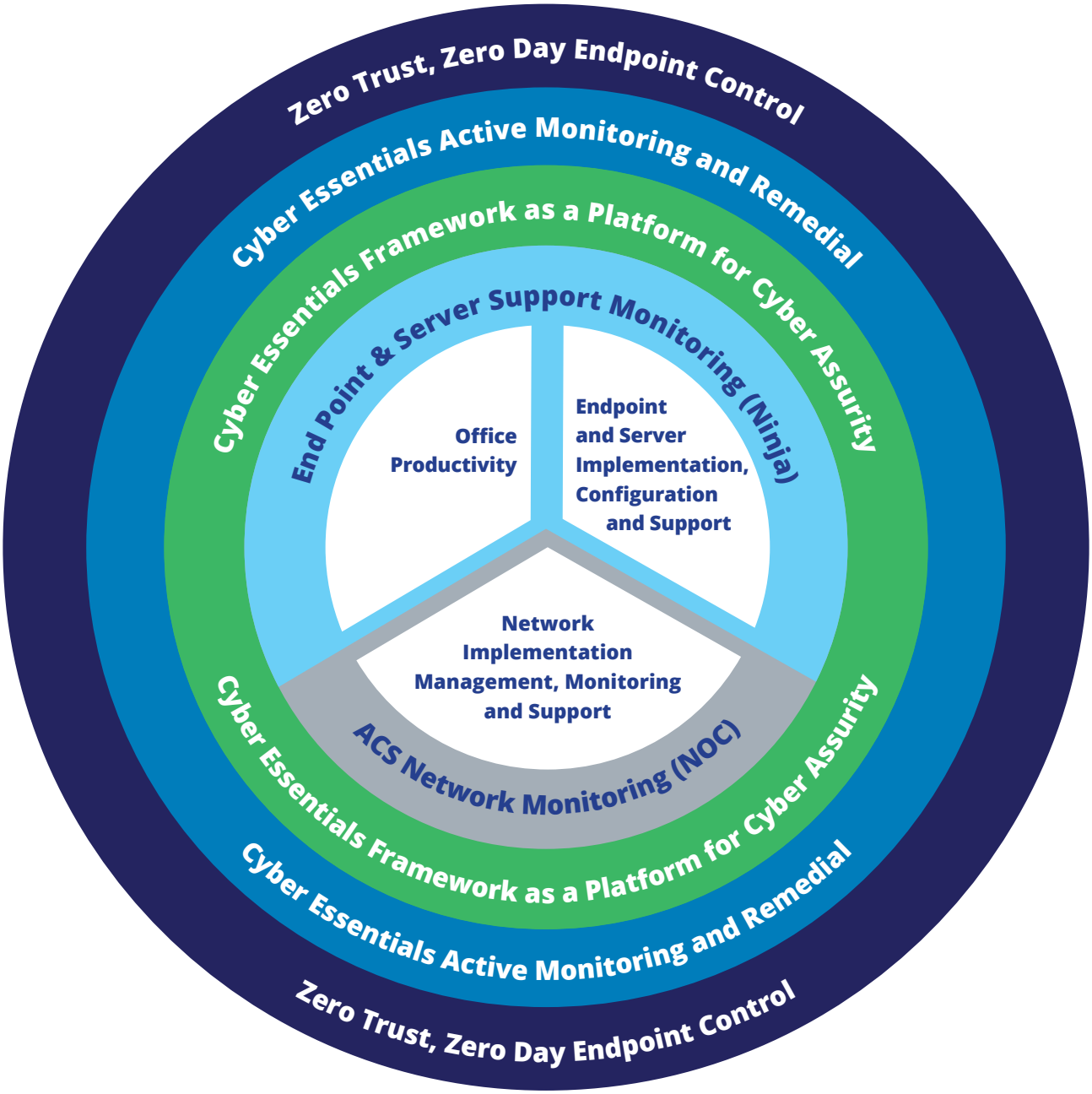
www.msdigital.com

MAINSTREAM digital
Cyber Security Solutions

IT Managed Services Portfolio

Our Layered Approach to IT Managed Services

The Mainstream Onion



ninjaOne CyberSmart APPGUARD

What does it mean?

In an ideal world, this is what we would roll out to ensure we provide the best, most robust, cyber safe and reliable solution.

We know that this not what suits every business, and very few are a green field. We can work with each business to identify their needs, the risks and the existing infrastructure, to ensure that we provide a complementary and effective solution to your needs.

We have an array of tools in our toolbox and we are not limited to a finite set, although we do have a core of approved products.

The Three White Areas

Represent our core managed server offerings.

The Pale Blue Area

Represents the equivalent monitoring services for PC/Servers, patch status, and operational status implemented with NinjaOne, which allows proactive remediation and monitoring of IT resources.

The Grey Area

Represents our overarching Network Operating Centre, which monitors the routers and intelligent network devices we have in place with our clients for proactive identification of issues.

The Green Area

Represents the basic fundamental framework for cyber threat preparedness. This is typified by a CyberSmart Cyber Essentials approach.

The Bright Blue Area

Represents the monitoring, management and remediation framework which we apply to ensure that the basic fundamental framework is maintained and audited throughout the year, rather than just taking the "MOT" approach, of being right on the day.

The Dark Blue Area

Is the provision of suitable antimalware to protect the organisations endpoints from active cyber attack. Our preferred route to this is a zero day capable, zero trust antimalware, although we can work with other products and services as required by the client, although we strongly advocate AppGuard.

PAGE LEFT INTENTIONALLY
BLANK

Gap Analysis

- Commitment Free.
- Cost Free.
- Let us give you an idea of your state of preparedness.

The three layers of Gap Analysis

VULNERABILITY TO CURRENT TRENDING CYBER ATTACKS

END POINT THREAT CONCERNS

COMPLIANCE IN A CYBER SECURITY CONTEXT

What does it mean?

Vulnerability to Current Trending Cyber Threats

This provides a Breach and Attack Simulation to enable you as an organisation to real time test your current state of cyber preparation against any threat or class of threat that you think is relevant – for example the Top 10 Ransomware attacks. This will deliver a status as to whether your configuration would have survived and will produce a list of the measures that would need to be addressed to ensure survival.

End Point Threat Concerns

This ensures that we know what is running on our endpoint(s) and what we would be controlling on that endpoint and why. An insight that shows stealth software, dangerous practices and illegal accesses. This provides a log for analysis to see what is actually happening on your end point and whether it needs to be addressed.

Compliance in a Cyber Security Context

Ensuring that the basic foundations of Cyber preparation have been addressed, such as would be encompassed by a Cyber Essentials compliant organisation. Cyber Essentials compliance tackles 80% of cyber risk. We can provide a gap analysis free of charge and with no commitment, to ensure that your foundation for Cyber preparedness is intact.

MAINSTREAM digital
Cyber Security Solutions

Mainstream Digital Ltd
Cirencester Business Park
Love Lane
Cirencester
Gloucestershire
GL7 1XD

T 0800 169 6000

E sales@msdigital.com

www.msdigital.com

In 2025,The Cyber Security and Resilience Bill will be introduced which will be the UK equivalent of the European NIS2 which has just been introduced.

For some types of organisation, local authority, Critical National Infrastructure, Health and Digital services being a few, the legislation will have teeth and be targeted at ensuring that the NCSC CAF is adhered to. We as a company are well prepared for this and will be soon joining the ranks of NCSC organisations accredited to audit and advise on compliance with NCSC CAF.

Below are some of the questions that you need to be asking yourself in preparation for this, and these questions come from the Local Government site https://www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-digital-and-technology-policy-team/government-cyber and 10 Questions on Cyber Security | Local Government Association and as such are not our questions, but your own advisors. We furnish you below with an explanation of what the question means, and incidentally, how we could help.

Question	What does it mean	How could we help	Some of Our Options that we can employ to assist.
What cyber security mitigation has been done in your council?	Do you have a Cyber Security Posture – Have you considered the risk, put any measures in place, assessed your level of threat?	We could provide an audit of existing measures	Our people, Our Gap Analysis
Can you demonstrate Due diligence on the matter of cyber security?	If you were to be successfully attacked, could you defend your position and the responsibility placed in you with respect to cyber risk?	We can offer Vulnerability checking and compliance gap analysis to show you your current state of play	CyberSmart Vulnerability check Validato BAS check CyberSmart Service Agent Gap analysis AppGuard discovery mode
Can you Evidence all staff members have the cyber skills and knowledge ?	Every member of the team contributes to the size of the attack surface area. Are they prepared, are they trained	We could offer a service that allows you to automate the training, policy dissemination and monitoring burden	CyberSmart Active Protect

Can you deliver a Current assessment of cyber security posture against good practice?	Do you have any means of assessing whether what you have in place would measure up as adequate?	We can provide at the very least, GAP analysis. If something more detailed is required, we can offer vulnerability checking	CyberSmart Service Agents Ninjaone Agents
Does your council have a centralised asset management system?	Do you track your resources, in terms of computer hardware, software and infrastructure. If you don't know what you have you don't know if it is protected.	We can offer agent based support and management tools very competitively, that report to an automated asset register, which tells us when your systems need updating, maintenance, are obsolete and NOT COMPLIANT	NinjaOne Agents CyberSmart Audit List
Are you awre of the Risks in your organisaton, and the processes used to manage procedures	Do you have an appreciation of where the risks to your organisation are? People,suppliers Systems, external threat, obsolescence, dependencies?	Spread the understanding of risk by vulnerability and gap analysis and by training your staff with courses and policies so that they are more aware of risk and are more diligent	CyberSmart Agent Gap Analysis CyberSmart Vulnerability Check Validato BAS AppGuard Discovery Mode
Are the Risks identified and managed in your supply chain?	Your suppliers are an extension to your attack surface area. They are the route of choice for attackers – why?	We can offer to Gap analyse your suppliers to give you peace of mind. Why would they not agree?	As above
Is your data secure?	Is it protected? From exposure, from deletion, from ransomeware, from disaster?	We can advise on best practice for data backup, data protection and protection of your data resources	NinjaOne backup
Response, recovery, and continuity plans for when cyber incidents occur?	If the worst happens, can you recover from it. Would it all just click into place if the mire hit the fan?	With a compliance and Cyber framework in place, we can advise on a business continuity plan with a recovery time that suits your organisation.	Our People An existing, proven, effective strategy in place.