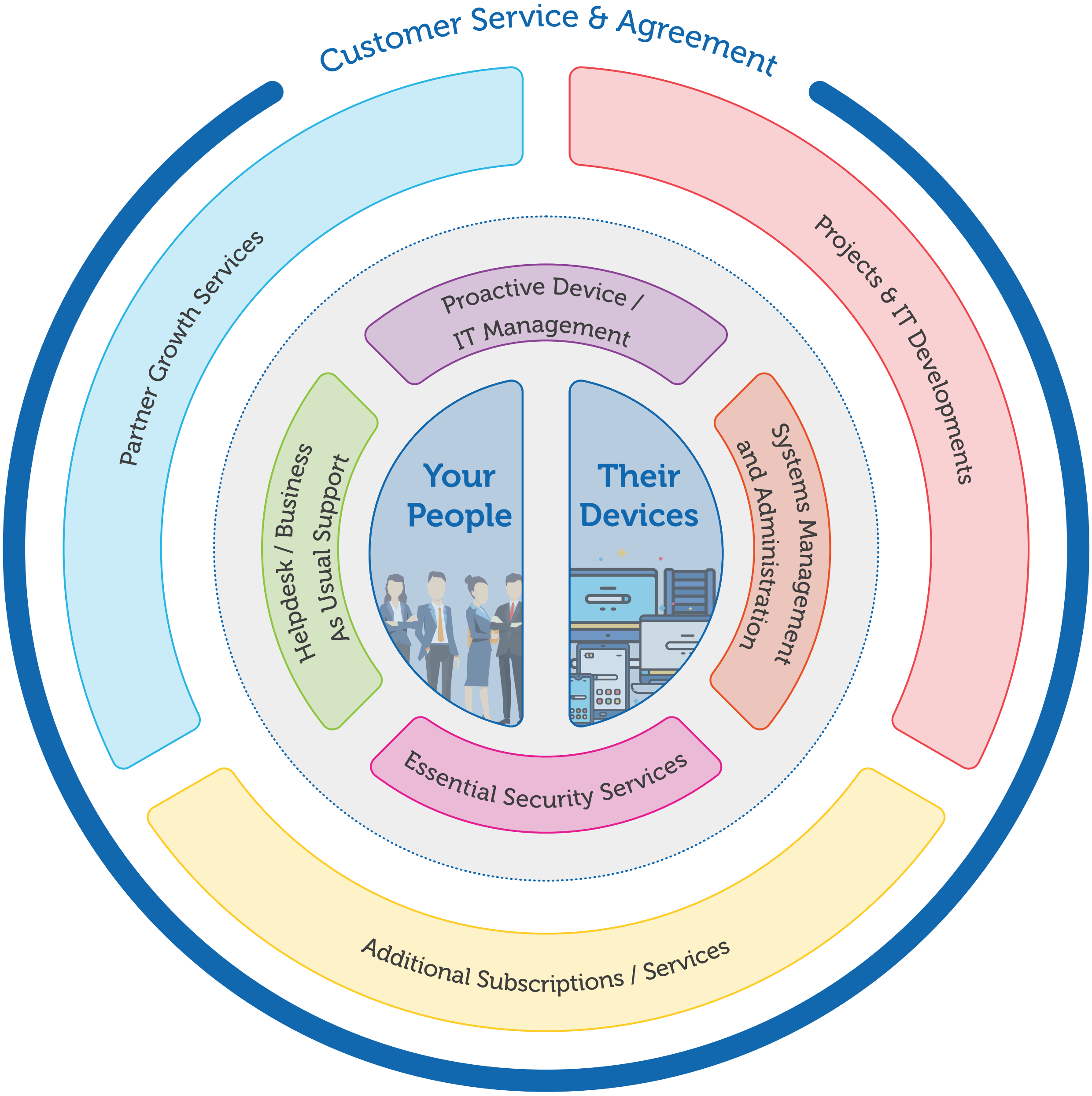
grantmcgregor
technology · people

The GM Difference | Explained

One Single Gold Standard


Customer Service & Agreement
Partner Growth Services
Projects & IT Developments
Proactive Device / IT Management
Helpdesk / Business As Usual Support
Your People
Their Devices
Systems Management and Administration
Essential Security Services
Additional Subscriptions / Services

Item	MSP Service Benefit		The GM Difference	📄
Customer Service & Agreement				**6**
1	Initial Contract Term - 12 Months		✓	7
2	90-Day Money Back Guarantee		✓	7
3	Professional Platform for Service Delivery Tracking & Management		✓	8
4	Guaranteed SLA - Response/Resolution Times & Rebates		✓	9
5	Measurement & Metrics for Service / Contract Management / Success		✓	10
6	Customer Satisfaction Scoring every user, every ticket tracked for success & feedback		✓	11
7	Additional IT	"Supported" EUDs catered for - more EUDs than Users	£26.65 / EUD / Mth	12
8		"Supported" Users catered for - more Users than EUDs	£26.65 / User / Mth	12
Helpdesk / Business as Usual Support				**13**
9	Extended Service Coverage Times & Hours for Support (Mon - Fri = 50 hrs)		0800-1800	14
10	GM ServiceDesk / Helpdesk / Remote / Tel Support Time		Unlimited	15
11	GM On-Site Support Time where GM attend your main site if required to hasten resolution		Unlimited[1]	15
12	Mobile Device Support (Smartphones/Tablets)		✓[2]	16
13	Dedicated ServiceDesk Team of Qualified Technicians for Business As Usual Support		✓	16
Proactive Device / IT Management				**17**
14	Remote Monitor & Manage	"Supported" Server/VM/NAS System	✓ Includes up to 4 servers	18
15		"Supported" EUDevice (not Mobile Devices)	✓	18
16		"Supported" Network Device	✓ Included[3]	19
17	Software Update Service	Server & EU Device GM Standard App List	✓ See Standard App List	19
18		Non-Standard Software & App List	✓ Extra	20
19	Dedicated RMM Team for handling your RMM Alerts and Human Intervention Support		✓	20
Systems Management and Admin				**21**
20	Software Application Install / Uninstall Service Time		2 hours / Month[4]	22
21	On- / Off-Boarding New/Old User Accounts in AD / Server System		✓ Included[5]	22
22	Provision / Re-provision Existing End User Devices for new Users		✓ Included[6]	23
23	Frequent Review of Supported Users v. Active System Accounts		Monthly	23
24	IT 'Supported'	Hardware Asset Register & Warranty Management (lifecycle report)	Assisted by GM quarterly, managed by customer. Reviewed quarterly.	24
25		User Asset Register & Housekeeping		24
26		Application Asset Register & Housekeeping		25
27	Hardware Update Service	(Server) - Manufacturer BIOS, Drivers & Firmware	✓ Included[7]	25
28		(EUDs) - Manufacturer BIOS, Drivers & Firmware	✓ or Extra (on-site)[8]	26
29		(Network Devices) - Manf BIOS, Drivers & Firmware	✓ or Extra (on-site)[9]	26
30	Server Out of Hours Maintenance Window & Reboot Service		✓ Automated Overnight	26

<table>
<tr><th>Item</th><th colspan="2">MSP Service Benefit</th><th>The GM Difference</th><th>📄</th></tr>
<tr><td colspan="4"><b>Essential Security Services</b></td><td><b>27</b></td></tr>
<tr><td>31</td><td colspan="2">GM Server / EUD Managed Essential Security Services (NB not Tablets/Smartphones)</td><td>Essential Package
(see below)</td><td>28</td></tr>
<tr><td>32</td><td rowspan="3">GM Managed</td><td>Antimalware & Antivirus Service</td><td>✓</td><td>28</td></tr>
<tr><td>33</td><td>Threat Prevention & Zero-Trust Service</td><td>✓</td><td>29</td></tr>
<tr><td>34</td><td>Web Threat Protect & Content Filter Service</td><td>✓</td><td>29</td></tr>
<tr><td>35</td><td colspan="2">GM Device Control (USB) on End User Device Only</td><td>✓</td><td>29</td></tr>
<tr><td>36</td><td colspan="2">GM Desktop Firewall on End User Device Only</td><td>✓</td><td>30</td></tr>
<tr><td>37</td><td colspan="2">Privileged Access Management (PAM)</td><td>✓</td><td>30</td></tr>
<tr><td>38</td><td colspan="2">Endpoint Detect Response and Advance Threat Security</td><td>✓</td><td>31</td></tr>
<tr><td colspan="4"><b>Partner Growth Services (IT Strategy & Planning)</b></td><td><b>32</b></td></tr>
<tr><td>39</td><td colspan="2">Service & Partnership Health Reviews (QBRs)</td><td>✓
Quarterly</td><td>33</td></tr>
<tr><td>40</td><td colspan="2">Technology Strategy Consultations (vCIO)</td><td>✓
Quarterly</td><td>33</td></tr>
<tr><td>41</td><td colspan="2">Video Tutorials and Courses for the Modern Workplace</td><td>✓</td><td>34</td></tr>
<tr><td>42</td><td colspan="2">3rd Party Systems / Supplier Support & Liaison Time Included Per Month</td><td>2 Hours / Mth[10]</td><td>34</td></tr>
<tr><td>43</td><td colspan="2">Additional IT Consultancy Services; e.g. IT Policies, IASME etc (beyond QBRs)</td><td>£ Extra</td><td>35</td></tr>
<tr><td colspan="4"><b>Projects & IT Development</b></td><td><b>36</b></td></tr>
<tr><td>44</td><td colspan="2">End User Device / Laptop / Desktop Installation Service</td><td>From £85.28 / hr</td><td>37</td></tr>
<tr><td>45</td><td colspan="2">On-Site IT Floor-walking or Dedicated Technician Service Time</td><td>From £85.28 / hr</td><td>37</td></tr>
<tr><td>46</td><td colspan="2">Dedicated Project Delivery Team for your Change and Development Work</td><td>✓</td><td>38</td></tr>
<tr><td colspan="4"><b>Additional Subscriptions / Services</b></td><td><b>39</b></td></tr>
<tr><td>47</td><td colspan="2">Managed Data Backup and Restore Services</td><td>⊗
Charged per server / EUD</td><td>40</td></tr>
<tr><td>48</td><td colspan="2">Office 365 / Microsoft 365 Subscriptions & Support</td><td>£ Extra</td><td>41</td></tr>
<tr><td>49</td><td colspan="2">Managed 365 Account Cloud-Cloud BUDR (per 365 account backed-up)</td><td>£ Extra</td><td>42</td></tr>
<tr><td>50</td><td colspan="2">Managed Email Security Plus Services (per email account protected)</td><td>£ Extra</td><td>43</td></tr>
<tr><td>51</td><td colspan="2">Enhanced Security Suite (beyond GM Essential bundle)</td><td>£ Extra</td><td>44</td></tr>
<tr><td>52</td><td colspan="2">Advanced IT Security Services (beyond GM Essential or Enhanced bundles)</td><td>£ Extra</td><td>46</td></tr>
<tr><td>53</td><td colspan="2">Cyber Essentials Certification GoldAssist Annual</td><td>£ Extra</td><td>47</td></tr>
<tr><td>54</td><td colspan="2">Cyber Insurance & Basic Forensic Investigation Service</td><td>£ Extra</td><td>48</td></tr>
</table>

Notes

1 Additional charges for travel and time may apply. GM decide if site visit is necessary & frequency/time spent. Only for hardware we have supplied or that is under approved warranty. N.B. SLA hours only. OOH charges otherwise apply.

2 Covering Mobile App support for these Apps only: Microsoft 365 Email & SharePoint; Microsoft Office 365 OneDrive, Outlook, Excel, Word, PowerPoint, Teams; Microsoft Authenticator. Mobile Device OS Support and Management available only via GM-supplied Microsoft InTune or GM-supplied MDM software. Mobile Device Hardware support or maintenance is not included.

3 Basic SNMP monitoring only included for compatible Network Devices (e.g. Wireless, Router, Firewall, Switch). GM can add provision of additional 24x7x365 Network Device Monitoring, self-healing and performance automation for an additional charge. Incompatible or Manufacturer End of Life network devices will not be monitored.

4 Subject to the same 2 hour time limit but for assistance with the installation or uninstall of 3rd party IT assets, devices and applications. Note the total time limit is across both aspects for 3rd party support AND for software application install/uninstall service time.

5 Formalised audit trail documentation for on-/off-boarding. Limit of 10% of existing staff count per year. Review at QBR if excessive. If more than 10% of User numbers in any quarter, you may be charged.

6 Includes all standard applications plus GM Managed Services, updates etc. Additional charges will apply for 3rd Party applications e.g. Sage, Adobe Creative, AutoCAD to be installed/set up.

7 If GM supply the Server and the Server has current Manufacturer / GM-Approved Warranty. Conducted quarterly out of standard SLA / working hours. Existing client Servers not capable of running our Hardware Update system or without a GM-Approved Warranty will incur additional time & fees to perform this service.

8 GM-supplied devices will be updated via the Manufacturer's update automation. Otherwise, bespoke quote for extra on-site chargeable time. Typically conducted every 3-6 months.

9 GM-supplied devices will be updated via the Manufacturer's update automation. Otherwise, bespoke quote for extra on-site chargeable time. Typically conducted every 3-6 months.

10 For troubleshooting & liaison with any other supplier to the client or any self-purchased IT asset, device or application. Any time above the limit will be chargeable. *N.B. This 2 Hour limit is a combined 2 hours for 3rd Party time AND for Software Application Install / Uninstall Service together.*

Customer Service & Agreement

1 Initial Contract Term - 12 Months

We can be flexible for 24/36 months. Rate will be increased on 1st January each year or on your contract annual renewal date. Underlying service rates can also increase with 30 days notice.

Grant McGregor charges a fee for professional off-boarding to cover the work involved. This equates to £995 for approximately 1.5 days for up to 25 users; £1995 for approximately 2.5 days for 26-50 users; and £2995 for approximately 3.5 days for greater than 50 users.

Why (does it have to be) a 12 month arrangement? What other options are there? Monthly commitment only? 36 months?
The standard initial contract we offer is for 12 months so that the initial 2-way commitment is not too onerous. Thereafter, we typically extend to 24 or 36 month terms. We use this minimum term so that both parties can commit to resource it appropriately and put the requisite effort into establishing and building a 'partnership' together. As part of ongoing reviews, we seek to evaluate the relationship, the contract delivery and the terms so that both parties can ensure it is mutually-beneficial or adjust where & when necessary. No other tailored term lengths are available.

What is the notice period or why do we have to give 3 months notice if we wish to quit?
This is simply a natural part of our ongoing Quarterly Business Review routines and we will confirm any changes, updates or continuation of the contract 90 days before the end date. Where the existing arrangement is not working for either party, a 3-month period offers sufficient time for either party to prepare for a replacement provider and for professional handover.

2 90-Day Money Back Guarantee

Our Promise & Service Guarantee - within 90 days, you'll enjoy a smooth transition experience and a better, more responsive IT service, all delivered at the price you expected to pay - or your money back!

GM Client On-Boarding Process is completed by both parties; GM Steps 1-5 complete within 90 days; GM Care & Manage Packages complete & in place; GM Phase 1 recommendations are in place; All supported Client Devices & Users are documented on GM systems; Users follow GM Support Process.

Measures: Critical Systems Availability >95%; SLA Met >90%; CSAT Response >70%; Score >85%; Monthly Spend Rates; Requests to invoke this Service Guarantee must be made in writing within 90 days of Contract Start Date. Your money-back applies to Support Fees only, not Project or any other Subscription or Equipment Fees.

Your Service Contract will be terminated and we will professionally off-board you.

What is this and why is it of any value to me?
We understand that changing IT provider can be stressful and worrying. That's why people often put up with poor service for way too long. To make that step less scary, we offer our straightforward promise and service guarantee that: within 90 days, you'll enjoy a smooth transition experience and a better, more responsive IT service, all delivered at the price you expected to pay - or your money back!

What's the catch? Or what are the terms of this?
Well, we do expect both parties to commit to making this a success so there are a few conditions to meet and some metrics that we'll score in the early stages of our relationship together. After all, if it turns out that we're not a good fit then both parties need a way out. However, no-one has yet invoked this guarantee but its there to demonstrate to you that we recognise your risk but that we mean to make a success of your decision to partner with us, hopefully for the long-term!

3 Professional Platform for Service Delivery Tracking & Management

All GM teams integrate and coordinate together via our IT Service Management or PSA System (ITSM) which we've had in place for, and evolved phenomenally, for over 10 years. This system 'glues' together information about your IT systems, configurations, users, help requests, system alerts, patterns and anomalies. It informs our ability to provide the right advice to a recurring problem rather than 'sticking tape over it'. This enables our various teams to see a technical context for any client's situation as well as to ensure they understand the business or organisational context. Think of it as an intelligent database, record-keeping and CRM system through which all of our people (and our clients' people) can request help, record details of actions, plus track, measure and report on all support, project and development activity that we carry out for clients and their users.

What is a PSA Platform and why is this important to me that you have this?
A mature, professional IT Service Provider or MSP will use one of the main Professional Services Automation (PSA) platforms in our industry to manage their business operations effectively and efficiently and to ensure quality in everything that they do for clients. The main professional systems used are ConnectWise, Autotask and Kaseya and, of these, we use ConnectWise to manage your IT devices, your IT infrastructure, your service requests, your projects, your products and services and everything to do with all of that. It's a purpose-built system for our industry - and we have employed it for over 10 years now - so much time, effort and money has been invested into developing it to create 'the Grant McGregor Way' recipe of policies, processes, procedures, checklists and systems information to ensure we can do our best work for you so that, in turn, you and your employees can do your best work for your customers and other stakeholders. It ensures that everything can be measured, resulting metrics can be used to drive improvement, things do not get lost or forgotten and we can track everything that we have done – or need to do – for you to keep everything running smoothly. Some IT providers have 'built' their own ticketing system or use a basic tool or have only just begun to use such a system so they will still be learning how to do this on your time, and will be years away from being the mature partner for you that ConnectWise affords us the ability to be right now.

How does this PSA Platform help you to help me and my staff?
By not just having such a tool in place but having invested heavily with our time, effort, money, blood sweat and tears (OK, maybe not blood) this PSA system ensures we can predict patterns of pre-cursor IT events and proactively prevent them before they cause you downtime or disruption. It ensures we can be proactive in management and updates to your devices to keep them secure, operational and available to be used by your staff when they need to get the most out of them to be effective in driving sales and profits or delivering your why. Our PSA also enables our team to be highly responsive when your people need our help and anyone in the team can get secure access to the info they need to help your employee without asking difficult questions about IP addresses or other things that they shouldn't need to answer. We can connect directly to your device, diagnose and identify any technical issue and, where possible, to resolve it there and then. Our PSA also enables us to track how quickly we manage to get to that end-goal of problem resolution every time meaning that we can identify areas to improve for you (maybe with the device, an application or connectivity) or for us with education, learning and sharing of knowledge to every member of our team. From all of this, it simply speeds up and makes flexible the way your team can log a request for help, organise when best to get that help or help us to escalate it quickly to a more experienced technical colleague where necessary. Critically, it helps us to get to the resolution of the problem or issue faster thus reducing the disruption or distraction that means your people can get back to what they do best or need to do to achieve to move forward your own organisation's mission and outcomes.

4 Guaranteed SLA

Response/Resolution Times & Rebates

From the beginning, GM decided only to offer ONE single “Gold”-Standard SLA and not to provide a better (or worse) level of service to different clients according to the money they pay. The information derived from our PSA client reports also openly shows you how we are performing against our SLA. This means that every request you log with us starts a shared clock that then measures if we have met the terms of our SLA arrangement with you. It’s very transparent. GM’s ServiceDesk team work to some target response, plan & - most importantly - resolution times (your SLA) wherever feasible and within your standard SLA hours. Our PSA system and SLA monitoring reports and gauges will alert us to any incomplete or more ‘complex’ tickets that have passed 80% of their expected SLA time for you. Amongst many other procedures and processes (SOPs) to ensure Quality Control, GM has a documented process (SOP) for escalating faults, requests and other workflows.

What should we expect from our Service Level with GM? Response times? Resolution/Fix times?
GM’s Unlimited Remote System Support and On-Site Reactive Support is provided across Monday to Friday from 0800 to 1800 (and excludes Christmas/Boxing Day and two New Year’s Day public holidays). Our Standard Service Level Agreement (SLA) works to the following timescales. GM will aim to meet the following priority 1 to 5 timescales each month for tickets logged through our ServiceDesk.

5 Measurement & Metrics for Service / Contract Management / Success

As part of our comprehensive Managed Service and SLA, GM provides monthly reports as standard on Server status, performance and availability. However, this is also part of a broader monthly service performance report with an Executive Summary Report that shows service stats and KPIs. Our PSA platform also offers instant, transparent access to information on service requests opened/closed, server status info, KPIs on patch updates, systems availability, backup trends and so on.

How does this type of measurement and these metrics aid me and my team?

It is often quoted and is credited to Peter Drucker as saying "If you can't measure it, you can't improve it…". Many of the measurements and metrics we gather around response, resolution, service delivery and effectiveness truly are for internal improvement and help us to follow our growth values of Quality, Commitment, Accountability and Innovation. You can read more about all of our Company Vision and Values **here**. Some of our key Customer delivery metrics are around Service Delivery such as response and resolution times for every service request, proactive device management & security measures, device health and early warning alerts and fixes, project delivery milestones and timelines, individual and company-wide customer experience and satisfaction ratings, billing accuracy and customer issues and resolution tracking. In measuring what and how we do for you specifically – plus delivering such stats to you in a periodic report and making them available to you anytime - we serve two key purposes. The first is to demonstrate that what you are paying for is actually being done – that problems encountered by your people are being addressed and satisfactorily resolved. You'd be surprised how often we find that many IT providers say they're monitoring your systems & reacting to alerts when, in fact, those alerts have been bleeping away and have been ignored or that they're updating the security on your systems when they've not been updated for months. The second reason is we can ensure you have a true reflection of the service being provided and enjoyed by your staff – their service experience, speed of resolution, trends with issues, who is seeking the most help and more. Measuring service remove any doubts and provides evidence of your overall customer experience.

6 Customer Satisfaction Scoring

every user, every ticket tracked for success & feedback

GM seeks genuine feedback at the end of every service request or ticket (from users) and at the end of every project. Using a tool called *Customer Thermometer*, this takes the form of a 4-choice rating survey to rate the quality of service experienced: Great, Good, OK & Bad with free text comments to augment the feedback. This feeds into our client and employee reviews. Any low scoring results are followed up by the Team Manager for the ServiceDesk or Projects to understand the reason for the rating and to learn if we could do something better next time or if the customer expectation is out of kilter with the SLA or Deliverables.

How do I / you know if you are providing good service to my company and my staff?
Quite simply because we measure it. GM tracks customer experience (CX) through a tracking tool using a range of mechanisms. First, for all ServiceDesk requests, all Projects and all Change Requests, clients and individual staff are encouraged to complete a short Customer Satisfaction (CSAT) survey to score their experience out of 'Great', 'Good', 'OK' or 'Bad' and also to offer comments. If the survey is scored either 'OK' or 'Bad', then these survey results are recorded into our Customer Improvement board for our ServiceDesk Manager to follow-up on. The aim is to understand the 'why' behind that score and to improve the experience for that user next time with an improvement task to follow. Second, we survey every Client every six months with a Customer Engagement Survey to rate our recommendation score. This is also recorded into the Customer Improvement board. Third, a monthly report is generated showing a range of metrics including SLA metrics, CSATs, service request categories and time spent supporting your people. Finally, we review this data alongside you at our Quarterly Business Review meetings to discuss contract performance, service delivery and any adjustments required.

What if my team score the service poorly or less than satisfactory? What do you do about this?
Any review that is not Excellent or Good (so the OK and Poor ratings) is sent immediately to our internal Customer Improvement Board and the Service Desk Team Leader is alerted. They will contact the person who gave the rating to find out more and to understand what lessons or experiences we can learn from this. This is then all noted in our PSA system for review by our Service Desk Manager to assess and to then contact the end user themselves. Hopefully, if there's something for the ServiceDesk Engineer to learn, amend or take feedback on, then this is carried out quickly and shared out in the weekly team meeting for all to learn any broader lessons. Occasionally, a poor rating can be down to the end user expectation not being met or being too high in the first place and so we seek to tactfully adjust those expectations or to follow-up with the client lead contact. An example where a recurring situation has helped us to improve our process is where we struggle to get hold of the end user who has raised a request for help despite us trying to reach them 4-5 times in the initial 24 hours. This can be frustrating for both parties, so rather than simply leaving it for the end user to come back to us when they are ready, we have implemented a time-booking App to organise a mutually-agreeable slot. This came from direct Customer Satisfaction feedback and has helped us to innovate our service.

7 Additional IT 'Supported' EUDs catered for
more EUDs than Users

Charged if authorised when supported EUD number is greater than the number of Users with 1 included EUD. £26.65 per EUD allows for EUD RMM, Software Update Services plus Essential Managed Security Services.

Will I be charged for having two computers or 'spare' PCs with no dedicated user?
Yes, if they are to be protected, updated and managed. You will be charged if your authorised, supported number of End User Devices (EUDs) is greater than the number of Users. Each User is already assumed to have 1 included EUD. The additional fee of £26.65 per extra EUD allows for EUD RMM, Software Update Services plus Essential Managed Security Services.

What if I don't want to include any spare PCs in this?
You have a couple of options here. If the PC / EUD will be used within a month or so then we recommend that it is maintained, updated and protected as a functional device ready to be redeployed to another user. During that time, it will be charged as an 'orphan' device or spare / additional PC without a specific user. If, on the other hand, you are confident that this machine will not be used at all for a period of 2 months or more, then you formally notify our ServiceDesk team and we will 'off-board' it (this includes the removal of monthly subscription services & essential security services). It will then be unprotected and unsupported. Of course, before this device can then be re-employed and supported, subscriptions & essential security services will need to be re-installed and software updates applied - as such we ask for a minimum of 7 days notice for this.

8 Additional IT 'Supported' Users catered for
more Users than EUDs

Charged if authorised, supported User number is greater than the number of Users with 1 included EUD. £26.65 per User allows for unlimited support for that User.

What if some of my staff / computer users share a PC or device?
If you do have more users than machines, you will not be charged the full Per User Fee. However, since we still need to support that additional person, this Additional User fee is charged for every authorised, supported User that is is greater than the number of Users with one included EUD. This charge is £26.65 per User and allows for unlimited support for that User.

Helpdesk / Business As Usual Support

9 Extended Service Coverage Times & Hours for Support

Telephone, LiveChat & Remote Support during these hours. Any request logged outside of these hours will only be reviewed and actioned within the SLA times i.e. from the start of the next working day.

What if I (or my employees) need support outside of these times? Or need help at the weekend?
We have a Priority Support model that is always based on the impact & severity of an issue. High Impact and/or High Severity will merit a Priority 1 reaction/response to achieve a resolution as quickly as possible. When our normal ServiceDesk operation is closed, Clients can reach their key GM contacts by mobile phone to deal with any High Impact/High Severity emergency issues outside of the standard SLA hours.

Why don't you offer support 24x7?
Simply put, our 7-Step proven process ensures that the way we design, configure, monitor & manage your IT systems should mean that unexpected faults or issues are genuinely minimised. Our 24x7 advanced monitoring systems offer alerts reacted to by our ServiceDesk team and with a degree of self-healing for devices. Users can still log service requests with us around the clock and these will be dealt with once the ServiceDesk reopens. Experience has shown us that the perceived demand for 24x7 support is virtually eliminated with the right IT planning, quality processes and proactive support and device management.

10 GM ServiceDesk / Helpdesk / Remote / Tel Support Time

ℹ

Unlimited within SLA hours. For agreed IT Asset list of supported Users, Devices and Applications only. These will be centrally-held on GM's IT Service Management System. Not for Project or Tech Services / Change Services or 'Floor-walking' Support. Fair Usage limits apply. Reviewed by both parties at QBR.

?

How do we contact you to get support when we need it? And what response / resolution times should we expect?

Every time you request support (or it might be us telling you about an issue you're unaware of yet), we record that into our Professional ServiceDesk system. Your people can reach us by dedicated support phoneline, specific email account or on an online service portal. Logging everything ensures that every request is tracked (including those generated by our system monitors) until successfully closed so we can ensure we meet our Service Level Agreement (SLA) commitments to you. And for us, it's not about response time, it's all about the end-goal of resolving the issue and enabling your employee to get back to what they do best. Since we can, and do, measure all of these results, every user and your management can see on your monthly report just how we're tracking against SLA metrics specifically for your company: how many tickets; how long each type takes to resolve and pick up on any patterns to be discussed and actioned at quarterly review.

Is there any limit to how often our staff can call you or log a request?

No, that's why we have an Unlimited service. We hear too often of other IT providers telling clients they ask for too much support. Referring to our Service Coverage Times above, it's our job to design, build and manage IT that works and, if we do that properly, we should be able to minimise the number of headaches that are caused. We're pretty robust in guiding you to replace outdated hardware and software, to get training for those who need it, or to swap-out 3rd party providers (e.g. printing, internet connectivity or phone systems) if they are your real headache.

11 GM On-Site Support Time

(where GM attend your main site if required to hasten resolution)

ℹ

Additional charges for travel and time may apply. GM decide if site visit is necessary & frequency/time spent. Only for hardware we have supplied or that is under approved warranty. N.B. SLA hours only, out of hours charges otherwise apply.

?

Will you come on site to provide support if required?

Yes, absolutely. It's in our best interests and yours to get your staff back to work quickly so, if we believe it will speed-up resolution, then we'll send an Engineer out to you. There are some caveats, of course, the main one being based on the impact & severity (therefore the priority) of the issue. This is strictly not for installing new equipment or project work but for supporting what you already have.

Is on-site time chargeable?

Generally no, it's not. Today, with the technology investments we've made and thanks to thorough on-boarding of you as a client, we can truly conduct support remotely 99% of the time. If it's in both of our interests to attend your site to achieve a more efficient or effective resolution then we'll have factored this in. However, as detailed in our Service Agreement, this is not for any type of project or change work and also that charges may apply for travel and out of hours on-site support.

12 Mobile Device Support (Smartphones/Tablets)

Covering Mobile App support for these Apps only: Microsoft 365 Email & SharePoint; Microsoft Office 365 OneDrive, Outlook, Excel, Word, PowerPoint, Teams; Microsoft Authenticator. Mobile Device OS Support and Management available only via GM-supplied Microsoft InTune or GM-supplied MDM software. Mobile Device Hardware support or maintenance is not included.

Will you support our Mobiles too (Smartphones and Tablets)?
Yes. We provide Mobile Application support for these Apps only: Microsoft 365 Email & SharePoint; Microsoft Office 365 OneDrive, Outlook, Excel, Word, PowerPoint, Teams; Microsoft Authenticator. Mobile Device OS Support and Management is available but only via a GM-supplied Microsoft InTune subscription or GM-supplied MDM software subscription. Support and/or maintenance for the hardware device itself is through the original Manufacturer or your Device Vendor (e.g. Apple, Samsung, Vodafone, EE, Currys). Mobile device protection (e.g. Antivirus) is not provided.

13 Dedicated ServiceDesk Team of Qualified Technicians for Business As Usual Support

GM has separate teams for Support, IT Developments, Tech Services and Cyber Security. The advantage to our clients is that our Technical delivery people are focussed on their own role meaning that you will not be calling a technician for support whilst he/she is in the middle of installing a server, conducting a security assessment or quoting for new laptops for other clients.

How will you properly resource the help my people need?
Many companies (or individuals) who provide support are very small, often 1-2 or fewer than 5 people companies. Their support line is often a mobile phone to a person who is also trying to install new IT equipment, assess security needs and react to system alerts to many other customers. That's an impossible task for anyone. GM has a dedicated team of skilled engineers who operate our Support ServiceDesk across 8am to 6pm to offer ready availability for your people but who are also focussed only on supporting you and your employees. They can give all their attention and knowledge to your troubled user and they are set up to deliver as fast a resolution as possible so as to get your team back to what they do best. Our qualified ServiceDesk people capture every request in our Professional Service IT Management System and will actively follow-up with your staff until the issue is resolved. Every request is recorded to provide us - and you - with data on how swiftly we are able to react and resolve your IT issues.

Will your people ask for our passwords in order to access our systems?
No. We do not need your people's passwords to be able to do our work and they should never handover their passwords to anyone, and that includes us.

Do you ask for permission before remotely accessing my people's laptops or PCs?
Yes. Our system will request access to a person's laptop or PC before we connect. That way they have time to remove any confidential company information from their screens before we login. To ensure that our people can effectively do their work in a timely manner, if there is no response to a request within 30 seconds, our system will automatically accept the request and our technician will be granted access. This allows your people to get on with other tasks away from the computer while still allowing our people the required access to assess and solve the issue.

Proactive Device / IT Management

14 Remote Monitor & Manage ‘Supported’ Server/VM/NAS System

Provision of 24x7x365 Server Monitoring, self-healing automation where possible and human reaction to alerts within SLA if not. Covers up to 4 Servers, VMs and/or NAS servers per client. Additional Servers chargeable at £42.64 per Server/VM/NAS per month. Includes attendance to diagnose & escalate hardware faults where protected with a Manufacturer/Approved Server warranty. Incompatible or Manufacturer End of Life Servers will not be monitored.

What exactly do you do to remotely monitor and manage our servers / virtual servers / NAS servers?
We conduct 24x7x365 Server RMM Monitoring & Alerting. Within our Network Operations Centre (NOC) we actively monitor your core servers (which run your main applications & house your data) to check uptime, availability and performance. We aim to ensure your systems are available to your staff as much as possible so this allows us to pre-empt problems that might cause disruption or downtime. We have a dedicated ServiceDesk NOC team to provide self-healing automation where possible and human reaction to alerts within your SLA if not. As standard this covers you for a total of up to 4 Servers, Virtual Machines (VMs) and/or NAS servers per customer. Additional Servers are chargeable. Includes attendance to diagnose & escalate hardware faults where protected with a Manufacturer/Approved Server warranty. Incompatible or Manufacturer End of Life Servers will not be monitored.

Yes but everyone says they do this. How can I see the value of this?
You’re right! Remote monitoring is only a small part of this service. The value ‘effects’ or real benefits of this is the NOC staff we employ to swiftly react to the alerts and warnings that the monitoring throws up to prevent a problem escalating. Around 66% of all of our ServiceDesk tickets are raised by our carefully-tuned monitoring and these are then dealt with by our team through coded ‘adaptive healing’ or by human intervention. We can evidence this by reporting and showing you every incident raised by monitoring/alerts and handled on your behalf to show you the work we do for you behind the scenes seeing off problems before they grow. That’s part of the GM difference!

15 Remote Monitor & Manage 'Supported' EUDevice (not Mobile Devices)

Provision of 24x7x365 PC / Laptop Monitoring, self-healing automation where possible and human reaction to alerts within SLA if not. Assumes 1xEUD / User only. Not including Mobile / Tablet devices. Unassigned and/or secondary devices are charged extra at £26.65 per EUD per month. Incompatible or Manufacturer End of Life End User Devices will not be monitored.

What exactly do you do to remotely monitor and manage our End User devices?
We conduct 24x7x365 EUD RMM Monitoring & Alerting. Within our Network Operations Centre (NOC) we actively monitor your End User devices to check uptime, availability and performance. We aim to ensure your devices are available to your staff as much as possible so this allows us to pre-empt problems that might cause disruption or downtime. We have a dedicated ServiceDesk NOC team to provide self-healing automation where possible and human reaction to alerts within your SLA if not. As standard this covers you for one EUD per user. Additional EUDs are chargeable. Does not include Tablets, Mobiles or non-Company devices. Includes attendance to diagnose & escalate hardware faults where protected with a Manufacturer/Approved Device warranty. Incompatible or Manufacturer End of Life Devices will not be monitored.

16 Remote Monitor & Manage 'Supported' Network Device

We will perform basic SNMP monitoring only included for compatible Network Devices (e.g. Wireless, Router, Firewall, Switch). GM can add provision of additional 24x7x365 Network Device Monitoring, self-healing and performance automation for an additional charge. Incompatible or Manufacturer End of Life network devices will not be monitored.

Can you add more value by monitoring my network beyond basic SNMP monitoring?
Yes, we can. Depending on the specific make and model of devices, we can provide much more thorough 24x7 monitoring for your Wi-Fi systems, your security Firewall, your internet router using proprietary monitoring applications. However, we can also provide a 24x7 network monitoring and management capability that speeds up fault-finding, hunts down bottlenecks and aids with uncovering root-cause conditions for network faults and slow-downs. There is an additional cost for this advanced network monitoring and this can be quoted separately.

17 Software Update Service (Patch Mgt)
Server & EUDevice GM Standard App List

The following Software / Applications is considered "Standard Software": Support for Windows Server OS for in-life support by MS; Support for Windows Desktop OS for in-life support by MS; Support for Apple Desktop OS for in-life support by Apple; Support for MS Office platform for in-life support by MS; Support for Exchange Email/Outlook for in-life support by MS; Support for Microsoft Browser software for in-life support by MS; Support for Browser software Chrome for in-life support by Google; Support for Browser software Safari for in-life support by Apple; Support for Browser software Firefox for in-life support; Basic Support for SQL Server for in-life support by MS; Support for Adobe Reader application for in-life support by Adobe; Support for non-MPS Printing (excluding >A3, plotters)

What is patching and why is it so important to keep our software up to date?
After an Application is first released to the market for use, bugs or flaws in the software as well as security vulnerabilities or weaknesses are discovered. The software manufacturer will then release an update from time to time (can be annually or even daily depending on the issues detected) to resolve these flaws. The update may be a small or large incremental change to the software that affects a small part of the code or the entire version running. These updates are commonly called software patches. The process of patching is another cornerstone of good cyber security as it closes known vulnerabilities before criminals can exploit them. It is vital to perform patching quickly and best practice is to do so within 14 days of the update being released to the market.

What software do you include for patch management?
There are millions of current and aged software applications and operating systems (OS) in the world. It is estimated that there are over 100,000 software companies today. That's why there has to be some sort of sensible list of applications & OS that we are able to update and those that must be updated by the software provider. See the info section in 17 for details of all standard software supported for patch management by GM.

18 Software Update Service (Patch Mgt)

Non-Standard Software & App List

Firstly, any unsupported / End of Extension (EOE) or End of Life (EOL) Applications will strictly NOT be patched or updated. No updates are provided for these and it is strongly recommended that you urgently replace them or discontinue use.

What about the software that is not on your list?
See note above on unsupported / End of Extension (EOE) or End of Life (EOL) Applications. For other client applications there are two routes. If the client-specific Application can be updated via GM's Script/Automate tools, then GM will perform these updates as additional, chargeable Tech Service time at applicable rates. Otherwise, the client should seek update support directly from the Application provider or their approved agent.

19 Dedicated RMM Team for handling your RMM Alerts and Human Intervention Support

GM has separate teams for Support, IT Developments, Tech Services and Cyber Security. The advantage to our clients is that our Technical delivery people are focussed on their own role meaning that you will not be calling a technician for support whilst he/she is in the middle of installing a server, conducting a security assessment or quoting for new laptops for other clients. For the RMM, this means we have someone dedicated to reacting to, addressing and managing all alerts and warnings that this important system monitoring provides. That dedicated RMM person can help advise the Project team of a failing device to alert the customer of the need for a replacement or can repair and fix issues such as low disk-space quickly without bothering the client or can write a script to address a repeating alert or a security flaw. Most importantly, these notifications don't get lost in the noise of hundreds of alerts some of which could be critical or highly disruptive. This is unfortunately so common amongst less mature, well-staffed IT providers and their distracting monitoring becomes pointless as it gets increasingly ignored.

What exactly is RMM and what difference do you provide?
We conduct 24x7x365 Server Remote Monitoring & Management (RMM) & Alerting. Within our Network Operations Centre (NOC) we actively monitor your core servers, desktops and devices (which run your main applications & house your data) to check uptime, availability and performance. We aim to ensure your systems are available to your staff as much as possible so this allows us to pre-empt problems that might cause disruption or downtime. We have a dedicated ServiceDesk NOC team to provide self-healing automation where possible and human reaction to alerts within your SLA if not. Whilst other IT providers will 'monitor' your network 24x7, if they don't have people dedicated to this task to understand the cause or react swiftly to the alerts and resolve any issues before they grow, then there's really no point to it.

Back to contents

Systems Management & Admin

20 Software Application Install / Uninstall Service Time

Subject to the same 2 hour time limit but for assistance with the installation or uninstall of 3rd party IT assets, devices and applications. Note: the total time limit is across both aspects for 3rd party support AND for this item.

Will you include installation of my applications such as Sage or AutoCAD? (Or any non-Standard Application)
Yes. However, it depends if this falls under unplanned change or project work. For occasional installations, this is subject to the same 2-hour 3rd Party time limit and includes assistance with the installation or uninstall of 3rd party IT assets, devices and applications. Note that the total allowance of time is across both aspects.

What if I or my 3rd Party provider needs to install or change non-standard software?
During the on-boarding stage, we'll identify your 3rd party applications and providers. (This can be added to at QBRs). We'll work with you and/or them to design a suitable agreed process. As and when you or they require access to perform such work, we'll ensure this follows that process and then restores access back to our standard supported level.

21 On-Boarding New / Off-Boarding Old User Accounts in AD / Server System

Formalised audit trail documentation for on-/off-boarding of users. There is a limit of 10% of existing staff count per quarter. We review these numbers at QBR. On-/off-boarding more than 10% of User numbers in any quarter, may incur a charge. There is a minimum 5 day notice period for informing us of new users and users being off-boarded. All notifications should come via the form located in our portal. Emergency off-boarding will be dealt with on a case by case basis, we will use best endeavours to support your request.

What is all this on/off-boarding of users and AD / Server systems about? It sounds confusing!
When your employees join or leave, (and subject to your software licensing) we typically activate/deactivate software licences, then create or cease a Login User account, a mailbox, Office 365 set-up and protection, appropriate file access permissions and membership of groups on your systems. This process is very client-specific but takes approximately 30-60 minutes to conduct per person. Although it is change, we include this work type under support, up to a fair usage limit of around 10% of your employee numbers. And why this limit? Metrics from our range of clients show this level of turnover to be typically 8%. If you have some unusual changes because of e.g. closing or opening a new office; buying another company; or making redundancies then this limit will, naturally, be waived. However, if your staff turnover rate is frequently higher than this then we either need to adjust your overall agreement to allow for more time for this or to charge for additional time as and when used for this purpose.

...and why is this so important for us?
One of the cornerstones of data and systems security is maintaining appropriate user access controls. User accounts for data and systems should only include current employees or application accounts that are 'live' and documented with permitted access. This is often neglected but it is best practice for cyber security hygiene and an essential part of good systems administration & management.

22 Provision / Re-provision Existing End User Devices for new Users

Includes all standard applications plus GM Managed Services, updates etc. Additional charges will apply for 3rd Party applications e.g. Sage, Adobe Creative, AutoCAD to be installed/set up.

When someone joins our team, will you set them up on an existing PC or laptop? Or is this charged?
Yes, we've allowed for this under supporting that person and getting them ready to work. We typically have to ensure that device is suitably updated with software patches; is protected with our essential security services; standard applications (see list for details) are set up; organisational shortcuts & links are configured; and printing to company devices is set up and tested. Again, this work takes a resonable amount of time per user/device and so is subject to the same fair limits as for on/off-boarding users.

What happens to a PC/Laptop if an employee leaves and not immediately replaced?
You have a couple of options here. If the PC will be used within a month or so then we recommend that the PC is maintained, updated and protected as a functional device ready to be redeployed to another user. During that time, it will be charged as an 'orphan' device or PC without a specific user. If, on the other hand, you are confident that this machine will not be used at all for a period of 2 months or more, then you formally notify our ServiceDesk team and we will 'off-board' it (this includes the removal of monthly subscription services & essential security services). It will then be unprotected and unsupported. Of course, before this device can then be re-employed and supported, subscriptions & essential security services will need to be re-installed and software updates applied - as such we ask for a minimum of 7 days notice for this.

23 Frequent Review of Supported Users v. Active System Accounts

Send IT User Asset List Report monthly showing all 'Supported Users' (CW) versus Microsoft 365 User / Licence list for client to adjust accordingly. GM will then adjust from updated Client report.

How do we check our list of users and MS365 accounts is up to date? How often?
During the on-boarding process, an agreed/approved list of supported employee/IT users will be input into our ConnectWise support systems for authorised support. Then when users join or leave, the ConnectWise system is updated from an on/off-boarding form. Each month, a report is generated and emailed to you showing any supported users that have been active during the prior month. This report enables you to review, check and adjust any further changes required for the following period via an on/off-boarding form.

24 Hardware Asset Register & Warranty Management (lifecycle report)

We will gather a Hardware asset list during on-boarding, including computers, servers, and network devices. This will then be updated by us for GM-procured devices, and then shared for QBRs. Unless formally notified to us via ServiceDesk ticket, any other Hardware sourced elsewhere will not be recorded and will be unsupported. Device on-boarding fees will then also apply. You'll receive a monthly lifecycle report of future end-of-life (or out of warranty) based on the hardware asset list. Allowing us both to put appropriate warranties in place.

How do you define what is a 'supported' hardware device (Server, User Device, Network Device)?
An authorised, supported device is: Monitored, Managed & Essential Protection by GM; has a ConnectWise Automate Agent installed by GM; is on the client-curated/shared IT Hardware Asset Register; and is on GM's ConnectWise Configurations Tab for the Client company.

25 IT 'Supported' User Asset Register & Housekeeping

The Customer remains responsible for this and curates all IT asset inventories. GM will gather a User asset list during on-boarding. This will then be updated by GM using the User On-/Off-Boarding forms, and then shared for QBRs. See Review of Supported Users v. Active System Accounts for details of monthly update process.

How do you define what is a 'supported' IT user?
An authorised, supported user is: on the Client's Approved IT User Register; is on GM's ConnectWise as an Approved, Active User for the Client Company.

Who is responsible for updating this list and maintaining it?
The Customer remains responsible for this and curates all IT asset inventories.

26 IT ‘Supported’ Application Asset Register & Housekeeping

The Customer remains responsible for this and curates all IT asset inventories. GM will gather an Application asset list during on-boarding. This will then be updated by GM for GM-procured applications, and then shared for QBRs. Unless formally notified to us via ServiceDesk ticket, any other applications sourced elsewhere will not be recorded and will be unsupported.

How do you define what is a ‘supported’ application?
An authorised, supported Application is: on the Client’s IT Application Register; AND is on the list of GM-supported Applications; OR is a GM-provided Application/Service; otherwise it is not supported by GM. Any application that is EOE/EOL is STRICTLY NOT supported. See list of GM-supported-applications.

Who is responsible for updating this list and maintaining it?
The Customer remains responsible for this and curates all IT asset inventories. GM will gather an Application asset list during on-boarding. This will then be updated by GM for GM-procured applications, and then shared for QBRs. Unless formally notified to us via ServiceDesk ticket, any other applications sourced elsewhere will not be recorded and will be unsupported.

27 Hardware Update Service (Server)

Manufacturer BIOS, Drivers & Firmware

If GM supply the Server and the Server has current Manufacturer / GM-Approved Warranty. Conducted quarterly out of standard SLA / working hours. Existing client Servers not capable of running our Hardware Update system or without a GM-Approved Warranty will incur additional time & fees to perform this service.

What on earth is a Hardware Update Service for servers and why do I need this?
Like software, hardware also needs to be updated and maintained in the form of the ‘control software’ for the various components, peripherals and interfaces - these respectively are called firmware, BIOS updates and drivers. Bugs or flaws are found over time along with security vulnerabilities or weaknesses. The hardware manufacturer will release updates from time to time (less frequently than software updates) to resolve these flaws. The updates need to be applied to the server or hardware timeously before bugs can be exploited but the difference with such hardware updates on a server, for example, is that the hardware will be unavailable whilst it is updated and then often must be rebooted or restarted. In practical terms, this means conducting this update work out of normal working hours to minimise disruption and downtime. The process of hardware updates is another cornerstone of good cyber security as it closes known hardware vulnerabilities before they can be exploited.

Why do you place such importance on doing this work as part of your support?
Not only is this a required cornerstone of your cyber security - indeed Cyber Essentials certification requires it - it has performance and practical benefits for your server hardware. Like any machine, it needs to be maintained to remain reliable and available to you to use. Any hardware manufacturer will only support a machine of theirs that has all the latest updates applied and if it is up to date (of course it needs to be in warranty too). Because of the expertise required, the time it takes and the reboot/restart required, this is an often-overlooked task and can cause many unnecessary and unexpected problems downstream if not done.

28 Hardware Update Service (EUDs)

Manufacturer BIOS, Drivers & Firmware

GM-supplied devices will be updated via the Manufacturer's update automation. Otherwise, a bespoke quote for extra on-site chargeable time may apply. Typically conducted every 3-6 months.

What about for End User Devices such as my laptop, do I need this service for them?
It is still important for all the reasons cited as for servers. However, there's not a straightforward solution for every hardware device variant that exists - Dell, HP, Fujitsu, Lenovo etc all have different updates applied in different ways. That's why we standardise on supplying a small number of device Manufacturers and only on a certain business-quality level of device. In this way, we can largely automate the process for applying updates for you to our GM-supplied devices meaning that it is included as part of our standard service level. Otherwise, for your existing user devices, this is conducted as a bespoke additional, chargeable service.

29 Hardware Update Service (Network Devices)

Manfacturer BIOS, Drivers & Firmware

GM-supplied devices will be updated via the Manufacturer's update automation. Otherwise, a bespoke quote for extra on-site chargeable time may apply. Typically conducted every 3-6 months.

Which network devices need to be updated and do you cover this?
Hardware updates also need to be applied for appropriate Network Devices such as Wireless Access Points, Routers, Firewalls and Switches. Any new GM-supplied devices will be updated periodically via the Manufacturer's update automation with some human intervention as required. Otherwise, a bespoke quote for extra on-site chargeable time may apply.

30 Server Out of Hours Maintenance Window & Reboot Service

Server reboots must be conducted as security or other updates demand. Reboots will be scheduled to be performed automatically and in line with Software & Hardware Update Service requirements. The agreed maintenance window for reboots and other automated maintenance tasks is typically Mon-Fri 2300-0300.

Why does my Server need to be rebooted/restarted and when will you do this?
Server reboots must be conducted as security or other updates demand. Reboots will be scheduled to be performed automatically and in line with Software & Hardware Update Service requirements. The agreed maintenance window for reboots and other automated maintenance tasks is typically Mon-Fri 2300-0300 to minimise disruption and downtime to your team. Anything outside of this process will be a bespoke, chargeable service.

Essential Security Services

31 GM Server / EUD Managed Essential Security Services (NB not Tablets/Smartphones)

Contains Managed 'Essential' Protection Services: Antivirus & Anti-Malware; Threat Prevention/Zero-Trust; Web Threat Protect & Content Filter; Device/USB Control; and Desktop Firewall. All managed by GM's Service team including set up and updating plus human reaction to system alerts when appropriate.

What is this Essential Security services bundle and what is included?
As the name suggests, it's a bundle of essential security services that you must have in place to provide adequate protection and defence against 80% of cyber threats. This is aligned to the UK Government's own Cyber Essentials security certification. The bundle contains: Antivirus & Anti-Malware; Threat Prevention/Zero-Trust; Web Threat Protect & Content Filter; Device/USB Control; and Desktop Firewall. These are all managed by GM's ServiceDesk & RMM teams and includes set up and updating of the subscriptions for each protected device plus any human reaction required to deal with system alerts when appropriate.

What if I already have AV etc? Can't I just keep using that?
There are literally hundreds of providers of security solutions but no IT provider can master them all. That's why we carefully select, partner with and then undergo staff training to master and maintain a small number of best of breed technologies that are suitable for our clients needs, for their affordability and for our ability to readily manage, monitor and update them. Critically, our solutions are tightly integrated into our IT Service Management platforms to ensure rapid reaction to alerts and updates. As such, these solutions are only delivered as part of our core, managed solution and we don't operate any other method such as employing your own procured AV solution. Depending on your level of security risk and industry requirements (e.g. FCA regulations), we do offer some advanced security solutions to meet specific client or industry needs over and above this essential set of tools.

32 GM Managed Antimalware & Antivirus Service

Complete Antimalware and Antivirus – GM's service provides an advanced combination of Antivirus/Antimalware so you only need one security solution, mitigating security breaches, simplifying deployments and reducing expenses. Exploit Defence - detects exploit techniques, stops known and zero-day exploits. Automated Disinfection & Removal - automatic actions to block, disinfect or delete threats.

What is this and what's different about this from any other AV solution?
This is complete Antimalware and Antivirus combined. GM's service provides an advanced combination of Antivirus/Antimalware so you only need one security solution, mitigating security breaches, simplifying deployments and reducing expenses. It also provides Exploit Defence - which detects exploit techniques, stops known and zero-day exploits - and Automated Disinfection & Removal - automatic actions to block, disinfect or delete threats.

33 GM Managed Threat Prevention & Zero-Trust Service

Machine Learning Threat Prevention – With more than 10 years of experience and 7 patents, Bitdefender has perfected Machine Learning algorithms to block elusive new threats with minimum false positives. Zero-Trust Continuous Behaviour Monitoring - monitors all running processes, detects and stops malicious ones automatcially.

What is this and why do I need this?
This service provides Machine Learning Threat Prevention with clever algorithms to block elusive new threats with the minimum of false positives. Zero-Trust Continuous Behaviour Monitoring monitors all running processes, and detects and stops malicious ones automatically.

34 GM Managed Web Threat Protect & Content Filter Service

Web Threat Protection - Web Traffic Scan (inclusion of SSL), Anti-Phishing, Search Advisor. Content Filtering & Control - Restrict User Access to websites or web categories such as gambling.

What is this and why do I need this?
This essential service provides an always-on Web Traffic Scan (including SSL), Anti-Phishing, Search Advisor. Content Filtering & Control service. It works beyond straightforward user browsing to restrict User Access to malicious websites or web categories such as gambling.

35 GM Device Control (USB) on End User Device Only

Device Control - Control which USBs or other external devices can run on user systems.

What is this and why do I need this?
This Device Control service allows control over which USBs or other external devices can be run on end user systems.

36 GM Desktop Firewall on End User Device Only

Desktop Firewall - Host Firewall with Intrusion Detection System (IDS) protecting endpoints inside and outside the network.

What is this and why do I need this?
We move around a lot more with our laptops and PC today from office to office and to working from home. A Desktop Firewall provides a Firewall on the End User Device with Intrusion Detection System (IDS) to protect the computer both inside and outside the business network.

37 Privileged Access Management (PAM)

As a Cyber Essentials certified body, and for good security hygiene, you should not be logged in as an administrator when carrying out non-administrator tasks. This is because if the device is compromised malicious software can be easily installed as you have admin rights. PAM software allows you to remove those local Admin rights and secure your devices by logging in as a standard user without frustrating them when they need to install approved software and updates.

What do I need to do to implement this?
We work with you to create a trusted software asset register. From this an agreed, automated software approved list is generated and can be installed and updated automatically as your users require.

What about unapproved software that needs installed?
If a user requires software to be installed that is not recognised, an approval request is sent to your key contact automatically to decide whether to allow the installation.

38 Endpoint Detect Response & Advance Threat Security

Cyber-criminals are growing ever more sophisticated, and today's advanced attacks are increasingly difficult to detect. Using techniques that individually look like routine behaviour, an attacker may access your infrastructure and remain undetected for months, significantly increasing the risk of a costly data breach.

Our Endpoint Detection and Response capability extends EDR analytics and event correlation capabilities beyond the boundaries of a single endpoint computer, to enable you to deal more effectively with complex cyber-attacks involving multiple endpoints. This technology provides focused response by providing threat visualisations at organisational level enabling more effective reaction. It is an integrated part of GM Enhanced Security suite

What is the EDR Module?

The Endpoint Detection & Response (EDR) module enhances your Essential Security and ATS defences to detect, investigate and respond to attacks. EDR is a cloud-delivered solution built on Bitdefender's GravityZone (BDGZ) platform with EDR agents deployed on your organisation's endpoints. Each agent has an event recorder that continuously monitors the endpoint computer and securely sends insights and suspicious events data to the BDGZ platform.

The EDR Continuously monitors your computers activity such as running processes, network connections, registry changes, and user behaviour. This metadata is collected, reported, and processed by machine learning algorithms and prevention technologies that detect suspicious activity on the system, and generate Incidents.

What is the Advanced Threat Security Service (ATS) Module?

The Advanced Threat Security module protects against enhanced threats and block attacks with next-generation, machine-learning technology. Combines a powerful Hyper Detect module with an integrated Sandbox Analyzer to grade and act on suspicious files and behaviours – to analyse, alert, block & eliminate threats – around the clock.

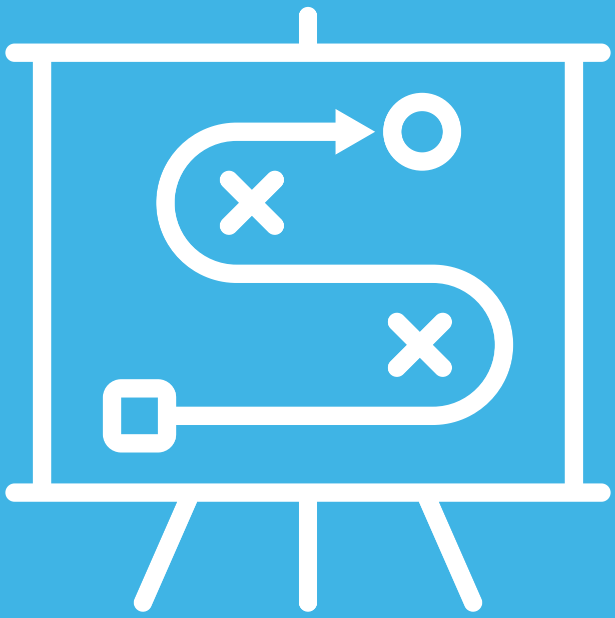
These additional layers of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage, and it is an integrated part of GM's Advanced Security suite.

How is the Hyper Detect protection level configured?

There are 5 protection layers to control targeted attacks, suspicious files and network traffic, exploits, ransomware and greyware. Each is configured with the normal level rather than Aggressive or Permissive. The standard action we will take is to move any files to a quarantine and block network traffic.

What is the Sandbox Analyser?

Content Prefiltering scans files, command-line arguments, and URLs for suspicious behaviour. This module automatically determines the objects that require further analysis and submits them to Sandbox Analyzer to test in isolated remote computer.



IT Strategy & Planning

39 GM Initial Business IT Planning & Advisory Reviews (QBRs)

Quarterly Business Review meetings (QBR) to be held for business-as-usual service and relationship review. Held 4 times per year. Can be reduced to 6-monthly for smaller sites/user numbers.

What is this QBR service and why is it of any value to me?
GM offers you, through our Quarterly Business Reviews meetings, the opportunity to review your service over the preceding and future 90 days. Discussing with you the service provision reports that you have received. Talking about our service together and feedback from your people. To continually improve our partnership.

So, does this mean you'll handle everything related to IT for us now?
No. It's only appropriate that someone in your organisation remains responsible for the oversight of IT and for managing the relationship with us and other 3rd party providers for printing, internet and so on. Just like an outsourced Accountant does not provide every single aspect of the accounting function for you, neither will any IT outsourcer be truly able to be responsible for some day-to-day aspects and decisions. For example, during our Quarterly Business Review meeting (QBR) we would prompt you to update the IT asset registers (people, devices and applications) that you curate but that we use to authorise against for essential support, security and updates. We'll also guide and help you to review maintenance planning.

40 Technology Strategy Consultations (vCIO)

These consultations provide you and your organisation with insight and guidance to help you better prepare and plan for technology trends, organisational changes, the security landscape, compliancy challenges, and to help remove obstacles.

How do you deliver this service to me?
Working in partnership with you, the process is overseen through a shared advisory platform that manages security and operational health, identifies technology gaps and creates a technology roadmap to ensure you can make informed budget decisions.

What is this vCIO service and why is it of any value to me?
Imagine you had/could afford a full-time IT person. They wouldn't just be responsible for support and fixing things. They would also be responsible for planning and developing your IT to invest appropriately in keeping you up-to-date, competitive and to ensure that your IT is strategically transformational and enabling. So, way beyond support alone, this is what GM offers to you through strategy meetings. We'll help you to develop your IT and budget for it appropriately, steering investments where they can provide most impact. We'll look for potential problem areas before they reach a critical point and help you to navigate through them. Yes, this means ongoing investment but better that this is done in a planned rather than piecemeal or reactive way.
Critically, troubleshooting/liaison does not provide for us to perform their duties for them or to manage them on your behalf.

41 Video Tutorials and Courses for the Modern Workplace

Our video library comprises of an education portal which includes tutorials course covering a broad range of subjects including Microsoft 365, Microsoft Teams, Mental Health and Wellbeing, Personal Cyber Security, Customer Care, Selling Skills and much more.

Why is this important and what benefit will it have on my organisation?
In the ever-changing modern workplace, poor team members are required to understand and work with technology applications, as well as navigate the workplace and WFH environments. To ensure they keep up with the demands ongoing, quality training is beneficial. Our comprehensive (and growing) library of short video tutorials teach key skills for the software your people use every day as well as important personal development and wellbeing practices.

How do some of your customers get the best value out of it?
With our support, customers have created an IT competency programme that ensures their people have baseline of skills to use the software on their devices for their everyday needs. They have then developed higher grades of proficiency to help boost productivity and ensure the organisation is future-proofed for further technology developments.

42 3rd Party Systems / Supplier Support & Liaison Time Included Per Month

For troubleshooting & liaison with any other supplier to the client or any self-purchased IT asset, device or application. Any time above the limit will be chargeable. * N.B. This 2 Hour limit is a combined 2 hours for 3rd Party time AND for Software Application Install / Uninstall Service together.

Who or what is a 3rd Party? What if I don't know who to talk to? You or my other provider(s)?
A 3rd party is another company (not GM) providing an IT-related product or service to you directly or indirectly. For example, your internet line may be provided to you by BT or Virgin. We will provide a limited amount of time and effort each month for troubleshooting of and/or liaison with this service/provider to investigate an IT issue in order to determine where the issue lies and report back to you. You can then take up further support (including progress reports) with the 3rd party. Alternatively, we can assist you further thereafter but this will be chargeable at our standard Tech Service rates. Critically, troubleshooting/liaison does not provide for us to perform their duties for them or to manage them on your behalf.

What happens if I exceed my fair usage limit because of 3rd party provider/service issues?
For example, if your internet line is provided by another party and keeps suffering from outages or performance issues. GM will help you to identify the core issue wherever possible and enable you to liaise with your other provider appropriately. This has to be limited as we have no control over another party's quality of service or delivery but we would encourage you to review or replace constantly-failing service providers and can assist you with this process. If you decide to take no action, any time expended above your limit will be charged.

43 Additional IT Consultancy Services

e.g. IT Policies, IASME etc (beyond QBRs)

Additional Consultancy Services charged separately: e.g. GM supply IT Policy Templates to Client to tailor and develop. Current Rates - £133.25/Hr, £1039.25/day, £527.67/half day.

Does this include IT Consultancy advice for improving our IT and/or for help with IT Policies or Compliance?

We aim to help you to plan and develop your IT, to invest appropriately in keeping you up-to-date and competitive, and to ensure that your IT is strategically transformational and enabling. Beyond support alone, this is what GM offers to you through our initial planning and Quarterly Business Reviews / IT Development meetings. See above. However, it's virtually impossible to scope for every client's needs within the one service fee. If you need help with enhanced security, risk assessments, compliance work, creation of policies or any other additional Consultancy Services then these are charged separately. Current Rates are £133.25/Hr, £1039.25/day, £527.67/half day.

Projects & IT Developments

44 End User Device / Laptop / Desktop Installation Service

Quoted with price of supplied, installed device(s). Standard rate is £85.28/hour for Technical Service time.

When I buy a new PC or laptop, is installation and set up of it included in my monthly fee?
As we cannot readily predict how many or how often you may need to buy new equipment, it isn't part of your predictable monthly cost. Instead such fees are quoted along with the price of a supplied, installed device(s). Wherever possible, we can combine the set up and installation of several PCs to make better use of Tech Service time. The current rates are £666.25 per Day, £330.46 per half-day or £85.28 per hour.

...and what if we buy our own computers? Will you install them?
We apply the same rules as for GM-supplied hardware save for two caveats: - the first is that any device must be of a suitable business hardware specification to be supported and protected for your needs using our standard bundle and toolset. We would not wish you to compromise the intergrity or performance of your network with a sub-standard, poor-quality or unknown hardware device. It must also come with an appropriate, currently-supported business-class Operating System and licenced software. For this reason, GM avoids low-cost, low spec, 'gray imports' or end-of-life and refurbished models as these are unlikely to last for a standard 3-4 year lifetime in a business-use environment and invariably cause additional support time and effort. The second caveat is that for any client-supplied PC, we apply an additional Assessment/Device On-Boarding fee to provide you with an objective assessment of the device and its suitability as well as to manage, protect and ready for support this machine on our systems and the IT asset list. We also remove all non-business software such as adware, bloatware and trialware. The Assessment/On-Boarding fee in this case is £52.23 per device.

45 On-Site IT Floor-walking or Dedicated Technician Service Time

For support purposes only, not for Project time or Change time. Day equivalent of £666.25, Half-day equiv. of £330.46.

Will you come out to our offices to spend time supporting my people?
Over 95% of the support we provide is delivered remotely by phone/chat/email. And, in fact around 65% of our proactive service deals with IT issues before you or your users are even aware of them. If you require it, we can offer a One-to-One Support service for a dedicated time slot for a Technical Service team engineer to visit your premises or to conduct a one-to-one session over the internet (via Teams). This may be beneficial for those users who don't readily call or email the ServiceDesk for whatever reason. However, note that this time is for support purposes only, not for Project time or Change Management.

46 Dedicated Project Delivery Team for your Change and Development Work

GM has separate teams for Support, IT Developments, Tech Services and Cyber Security. The advantage to our clients is that our Technical delivery people are focussed on their own role meaning that you will not be calling a technician for support whilst he/she is in the middle of installing a server, conducting a security assessment or quoting for new laptops for other clients.

When I want to procure new IT equipment or conduct projects, how does this work?
Dedicated people, focussed on development, standardised quality equipment & best breed solutions, lifecycle management, key vendors, buying power, project planning, forward planning (QBRs), thinking for you/best interests, downtime/weekend work, project success handover, project quality reviews and metrics plus CSAT.

Additional Subscriptions / Services

47 Managed Data Backup and Restore Services

Server BUDR - Charged at £99 per Server including up to 1000GB of Data Backed-Up Per Server; Charged at £99 per EUD including up to 200GB of Data Backed-Up Per EUD; 10p per Additional GB Backed Up Data for Servers & EUDs; Cloud Stored Data for both; Data also stored to Local Speed Vault Device NAS for Servers (NB Device is Extra Cost); Data Integrity Check Daily & Remediation of Faults; Server / Data Restore during SLA Hours only; DR Test during Service OnBoarding; Additional DR Tests charged extra. Any other aspect of BUDR such as regular testing, DR policies is an additional, chargeable service.

Will you backup my data as part of this service?
These backup services are charged separately since it depends on exactly which data (and where it is) that needs to be backed-up. Our Server backup is charged at £99 per Server which includes up to 1000GB of Data backed-Up Per Server; For PCs and/or Laptops, it is charged at £29 per EUD including up to 200GB of Data Backed-Up Per EUD, If you exceed these quantities, there is an additional fee of 10p per additional GB Backed Up Data for both Servers & EUDs. Your Data is stored in the Cloud and also on a local Speed Vault Device NAS for Servers (NB this Device is an extra cost). We will perform a Data Integrity Check daily & remediate any Faults. Any Server / Data Restore is conducted during your SLA Hours only. We will conduct a DR Test during the set-up and OnBoarding of this Service; any additional DR Tests or OOH restores are charged extra. Any other aspect of BUDR such as regular testing, production or assistance with DR policies is an additional, chargeable service.

Backup is great but will you restore my data if required?
As part of our managed service we will also restore your backup data to the same device it was backed-up from. We will conduct this restore remotely where possible and within your standard SLA service hours. If hands-on service or on-site restore is required then travel time is excluded but any reasonable out of pocket travel / other expenses will be charged.   If data restore must be conducted outside of your SLA hours, then additional evening or weekend charges will apply. If the original hardware source has a fault and we are unable to restore to it then we will invoke hardware warranty for a repair/replacement to be carried out as appropriate. If there is no warranty or we must restore to a different / replacement device then any Technical Service time taken to prepare this alternative device for the data restore is not included and will be charged separately.

48 Office 365 / Microsoft 365 Subscriptions & Support

Month-to-month Subscription only. Unlike with Microsoft direct, GM does not force each user licence into a 12-month tie-in saving you money when an employee leaves. Subscription includes GM support for 365 / Office 365 subscribed-services. All GM MS Cloud Subscriptions are priced and invoiced separately from this Support Services Fee

Is Microsoft 365 (and other Cloud Subscriptions) included with this?
These Microsoft 365 subscriptions are charged separately since it depends exactly how many and which subscription types you have. Microsoft has a vast and ever-changing array of subscription options which you typically can buy on a 12-month minimum subscription per user via a credit card. GM provides these only on a month-to-month subscription to offer complete flexibility for you. With Microsoft direct, you are forced into a 12-month tie-in for each licence so we can save you significant money if & when an employee leaves. Your subscription through us includes GM support and administrative changes (e.g. people changes, licence management and permission changes), for your 365 / Office 365 subscribed-services. All GM-supplied Cloud Subscriptions are priced and invoiced separately from this Support Services Fee.

Can I keep my own MS 365 subscription direct with Microsoft or with a 3rd Party?
Yes you can. When you need or request any administration support/change around that 3rd Party-supplied service, we will use your time-limited 3rd Party support agreement for this. That’s why it’s often more cost-effective and efficient for you to move these subscriptions to us so that we can manage and administer them within one simple subscription fee.

49 Managed 365 Account Cloud-Cloud BUDR
(per 365 account backed-up)

Microsoft 365 / Office 365 subscriptions do not include any data backup. Data is only stored with Microsoft for between 2 weeks and 90 days depending on the data type. This service provides a back-up and restore facility for all 365 data for Email, SharePoint and Teams per 365 account. The subscription quantity depends on the accounts and type of data selected for back up, hence it is separately priced.

Why do I need this? Doesn't Microsoft already store and backup our cloud data?
Microsoft are quite clear about this and so we need to strongly convey this too. They say: *"...Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."*

Note that this is not just for your email but also for SharePoint content & data, Teams data and data held in any other Microsoft 365 App. So, it ought to be clear that they DON'T backup or store this data for you. Hence GM strongly recommends a separate 365 Data backup and recovery service that we manage for our clients.

What exactly is included in your 365 Backup Service?
Eliminating user error and other causes of data loss is unlikely. However, it is possible to minimise its cost and disruption to your organization. Our 365 Managed Backup Service for Office 365 ensures that the data used in an organisation's instance of Office 365 is backed up, restorable, and protected. The service can be used to perform backup and restore of Office 365 emails, contacts and calendar (Exchange online) and files, folders and document libraries in sites, subsites in both: the classic site collections (SharePoint) and the modern Teams sites, communication sites (SharePoint online and OneDrive). Organisations that deploy our 365 Backup service for Office 365 can rest assured that all of their critical Office 365 data is backed up to the encrypted, tamper-proof systems within our provider's Cloud systems. It is, therefore, cloud-to-cloud backup only and requires restore from across the internet.

50 Managed Email Security Plus Services
(per email account protected)

Four Service options available depending on Client situation, hence separately priced. Can include standard email security, enhanced security, encryption, archiving and all of the above.

What is this and why do I need this service? Doesn't Microsoft already filter for spam?
Microsoft's own built-in online protection provides a basic degree of defence from spam and malware though it doesn't go far enough against today's persistent level of email attacks - which are the number one vector for cyber criminals. It also does not have any form of business continuity function for disruption or disconnection to the 365 service. So when 365 suffers an outage, your inbound and outbound email would bounce or be lost. GM's Managed Email Security Essentials service for business offers the best protection for Microsoft Office 365 accounts. It secures your people and data with superior protection against email-borne threats and offers key differentiators that complement Office 365 by: Protecting against malware and non-malware threats with industry-leading efficacy; Preventing impostor email threats with dynamic classification; Sandboxing malicious URLs and attachments in case your users click on them unwittingly; Protecting against compliance violations and information loss; Providing 24x7 emergency continuity inbox in the event of an 365 outage; Social media account protection; Policy-enforced encryption and data loss prevention (this last one is only available in our Enhanced version for an additional cost).

...and what exactly is included?
The Email Security Essentials service is priced per mailbox and includes: Real-time Email Spam Filtering; Virus-Blocking; Attack-Blocking; Traffic-Monitoring; Content Filtering. Additional features available in our Enhanced service level include: Email Archiving; Email Encryption & Data Leak Prevention. A protected mailbox is charged if it is a User Mailbox (secures inbound & outbound email and gives control over security preferences) or a Functional Mailbox (also secures inbound & outbound email but has no control over security preferences).

51 Enhanced Security Suite (beyond GM Essential Bundle)

The Enhanced Security Service is a 12 Month term

Cyber Awareness Training

The managed Security Awareness Training includes several services which are targeted at increasing your people's awareness of cyber security threats and how to help them stay safe.

What is included with the Security Awareness Training month to month?
Access to a wide range of cyber training materials for all End Users, with automated training campaigns and scheduled email reminders. Also, fully automated, configurable simulated phishing attacks, with reporting of results. 'Virtual Risk Officer' which provides risk scores which can be reported by End User, groups of End Users or the whole organisation

Will there be ongoing management once the training has been set-up?
There will be a professional onboarding of the system provided by a GrMc partner. If you ever require to be retrained on the system this can be arranged. The service is constantly being updated in the background for you. Those who fall for phishing emails will be guided for additional training as well as reports of phishing email passes and fails reports will be sent.

Continuous Cyber Essentials Compliance

Cyber Essentials is not just a one point in time excise to receive a certificate but is continuous all year-round Compliancy. The Continuous Cyber Essentials Compliance Service allows you to demonstrate compliance against the standard all year round.

How does the Continuous Cyber Essentials Compliance Service differ from the once-a-year Cyber Essentials Service?
GM will make available a project manager as appropriate to act as a single point of contact for the Client for the duration of this Agreement. This will be provided in 15 to 20 mins blocks each month, totalling no more than (3 to 4 hours per year).

At the start of the service GM will provide the Client with a set of documentation and provide a single one-on-one briefing on Cyber Essentials to a representative of the Client. Following the briefing, Grant McGregor will provide access to the Self-Assessment Questionnaire, which the Client will complete with assistance from Grant McGregor.

Throughout the year GM will help the customer to keep the asset management register up to date for devices that are in scope each month. The project manager will also guide the customer within the CE framework, assessing the current compliance level and providing assistance with the assessment. All within the 15 -20 mins provided each month.

What policies are included and how often are they updated?
Grant McGregor will provide 10 Cyber Essentials Polices at the beginning of this agreement. They will be tailored per customer needs, but not rewritten. The policies will be updated when and if internal and external variables change to keep them update. All within 25 mins pe month or 5 hours per year. At the beginning of the new agreement year this will be repeated. The policies are as follows: -

- Information Security Policy
- Acceptable Use Policy
- Password Management Policy
- Joiners / Movers / Leavers Procedure
- Asset Management Procedure
- Asset Register / Software Register / Admins / Open Ports
- Access Control Policy & Register
- Patch Management and Vulnerability Policy
- Backup and Restore Policy
- Computer and Mobile Device Policy

What is included with the Computer Vulnerability Service?
GM will provide a 12-month licence for the Vulnerability Tool which will be downloaded to every endpoint in scope. During the month GM will provide remote device audits and software vulnerability management. Continuously scanning of the Endpoints to centrally report on vulnerabilities, allowing GM to gather and then address such vulnerabilities if software fixes are exist , all within 5mins per end point each month

What happens at the Cyber Essentials Renewal Anniversary date?
Prior to the customers Cyber Essentials expire date. The custom must complete the Self-Assessment Questionnaire, GM will Assess the completed Self-Assessment Questionnaire and report the result of the Assessment. If the Assessment result meets the criteria of the Scheme, GM will issue a Scheme Certificate. If an Assessment fails to meet the Scheme's criteria, the customer may submit one further Self-Assessment Questionnaire for Assessment.

Will there be an extra cost for the Submission of Cyber Essentials to IASME?
There will be, as normal, a separate certificate cost as charged to us by IASME.

Password Management

i

Password Management is a critical most important aspect of Cyber Essentials and good security hygiene. It allows you to manage and maintain all your passwords in one place, so that they are not all over the place in spreadsheets; word documents and located within peoples' personal browsers.

?

Will this help when people are off/on boarded?
This is a great solution for when people come and go. As you don't need to reset or locate who had what username and password. You just stop access to the one user account and reassign to another.

Advanced Threat Protection and Managed Detect and Respond Service

i

Think of MDR as having a house alarm system connected by a telephone line to a respond centre. They will know when the alarm is sounding to enabling them to respond and alert you. By having the MDR service they can provide you with a team of experts who monitor your computers and networks and respond to cyberthreats 24/7.

?

What is the Managed Detect and Respond Service?
The MDR Proactive Protection, includes a 24 x 7 x 365 security operations centre which proactively researches the cyber-threat landscape and constantly updates the capabilities of the Advanced Threat Protection service. The Automated Response, which detects attacks in real time and mitigates their effect through the use of highly customisable pre-approved actions that are executed by security experts. The reporting, the provision of breakdowns of all threats detected in your infrastructure and actions taken in mitigation.

52 Advanced IT Security Services
(beyond GM Essential Bundle)

i

Advanced Security Services charged separately: e.g. Security Risk Assessment; Security Risk Analysis; Endpoint Detection & Response; Advanced Threat Protection; Managed 2FA; NextGen Antivirus; Security Awareness Training & Testing; Penetration Testing; Vulnerability Scanning; Smart Security Compliance; Data Loss Prevention; Mobile Device Management; Microsoft InTune Device Management etc.

?

What is the difference between your Essential Security and Advanced Security services?
Enhanced Package or Advanced Security Services are all charged separately: e.g. Security Risk Assessment; Security Risk Analysis; Endpoint Detection & Response; Advanced Threat Protection; Managed 2 Factor Authentication (2FA); NextGeneration Antivirus; Security Awareness Training & Testing; Penetration Testing; Vulnerability Scanning; Smart Security Compliance; Data Loss Prevention; Mobile Device Management; Microsoft InTune Device Management etc. Details of what's included and the charges are available separately.

53 Cyber Essentials Certification GoldAssist Annual

Subject to IASME Submission Fee and paid-for GM Cyber Essentials / Plus Consultancy as/where required. May be additional charges for Smart Cyber subscription if required.

Will my systems, my staff and my data be protected and fully secured by you?
GM would love to offer you a 100% security guarantee but we simply can't. Not even the US Government can guarantee to fully-secure its systems, staff and data from attacks, ever-evolving threats or data breaches.

What we WILL do to provide an appropriate level of protection for your business is to recommend you put in place appropriate security measures to readily certify your company against the UK Government's (NCSC) Cyber Essentials standard for security preparedness. And we can help you to prepare for - and get certified to - this standard as we are one of a small number of qualified and recognised Certification Bodies for this scheme in Scotland.

Certification is subject to an IASME Submission Fee and additional, chargeable GM Cyber Essentials / Plus Consultancy services as and where required. Organisations sign-off their own Security Readiness statements at Board level as this is not an IT-driven programme but needs support from the top. Additional charges for further security tool set subscriptions may be required to expedite your preparation and certification. A growing number of businesses are valuing Cyber Essentials and it is proving useful to gain contracts and to win tenders. However, it is still a baseline and is not objectively tested nor is it currently a 'continuous compliance' service.

CE Plus is the independently-verified step beyond certification and a suitably-qualified Security Tester will check your systems and processes are, indeed, in order. The annually-recertified scheme is currently considering the need to remain constantly vigilant and some form of continuous testing or monitoring against the standard is likely to be included. Even with Cyber Essentials Plus, your business may still be vulnerable to determined or persistent attackers but CE/CE Plus is designed to prevent the most common 80% of threats and attack types from everyday cyber criminals.

54 Cyber Insurance & Basic Forensic Investigation Service

IASME Cyber Insurance and basic Forensic Investigation (3rd Party-delivered service) is included if the client certifies (and maintains certification) to Cyber Essentials / Plus using GM CE / Plus Services and if they qualify for the IASME CE insurance scheme conditions. Details on request.

What do you do if I have a data breach? Or need post-attack forensic support?
The start point here must be prevention and it begins with preparation to be well ahead of any data breach. This means in practical terms that your organisation needs to conduct a Data Information Audit (so that you first understand where exactly your data is), then construct your own Information Security Policy and Action Plan (for your staff and stakeholders to know how to behave). You should also have registered your business with the Information Commissioner's Office (ICO) in readiness to report any breach and create (and test) your own Data Breach Procedure to follow in such an event. If you certify to (and maintain certification to) the Cyber Essentials / Plus schemes using GM Services then you may qualify for IASME Cyber Insurance. This includes a 24hr helpline to report a cyber incident, which will provide crisis management and incident response to the total liability limit of £25,000. (this is a 3rd Party-delivered service). Terms and conditions apply - see https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/ for further details. GM may be able to assist you with any of these preparations - or assistance with/reaction to a breach - as chargeable Consultancy services.

What are the conditions of Insurance and the Forensic service?
Being compliant to Cyber Essentials has been shown to significantly reduce the likelihood and severity of a data breach. However, the risk still remains, especially if there is human error, a malicious insider or a concerted external attack. The presence of cyber insurance will provide vital incident response services and cover your costs in your hour of need. The insurance provided with certification gives you £25,000 limit of indemnity so you may want to purchase a higher limit of cover in case you suffer a severe breach. When a UK-domiciled organisation with a turnover under £20m achieves self-assessed certification covering their whole organisation to either the basic level of Cyber Essentials or the IASME Standard, they are entitled to Cyber Liability Insurance, terms apply. You can find out more about the details and terms of this arrangement at https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/

Abbreviations and Frequently Used Terms

2FA (MFA)	Two Factor Authentication (Multi-factor Authentication)
BUDR	Backup and Disaster Recovery
CSAT	Customer Satisfaction
CW	ConnectWise
Cyber Essentials (CE)	A Government backed scheme to help organisations put in place basic controls to combat the most common cyber security threats
DR	Data Recovery
EOE	End of Extension
EOL	End of Life
EUD	End User Device
GM	Grant McGregor
IASME	A not-for-profit organisation who oversee Cyber Essentials accreditation
MS	Microsoft
MS365	Microsoft365
NCSC	National Cyber Security Centre
OOH	Out of hours
RMM	Remote monitoring and management
QBR(s)	Quarterly Business Review

Back to contents