GM Enhanced Security Suite

Effective cybersecurity requires more than a single solution.

A multi-layered approach is now essential, combining advanced technology, regulatory compliance and ongoing training for your team.

GM Enhanced Security Suite
brings together 7 critical services to help your organisation defend your people, data and systems from modern cyber threats.

- **GM Cyber Awareness Training**
  Empower your team to identify suspicious activity, reduce risk and build a culture of cybersecurity awareness with continuous reinforcement.
- **GM Continuous Cyber Essentials Compliance**
  Stay compliant and audit-ready with expert-led Cyber Essentials support, keeping your business aligned with regulatory and insurance requirements.
- **GM Cyber Essentials Policies and Policy Management**
  Ready made policy templates that are required for Cyber Essentials. A central and easy way to distribute these policies to your staff to ensure they are seen.
- **GM Vulnerability Management**
  Continual monitoring and resolution of software vulnerabilities across your devices, ensuring they are Cyber Essentials compliant and secure.
- **GM Password Manager**
  Secure account access with strong, centralised password management, even through staff changes.
- **GM Encrypted Microsoft Connect**
  Protect Microsoft 365 access with encrypted, Zero-Trust controls that ensure your business data isn't intercepted.
- **GM Managed Detect and Respond**
  Control and stop emerging threats with proactive endpoint monitoring, real-time threat protection and immediate response from a 24x7x365 Security Operations Centre.

GM Cyber Awareness Training

Part of GM Enhanced Security Suite

POWERED BY KnowBe4 Human error. Conquered.

GM Cyber Awareness Training is essential for bolstering your organisation's cybersecurity defences, transforming employees into a human firewall - helping them work safely and protect organisational data and money.

With professional on-boarding, consultation and guidance, you'll get the most out of the training from day 1.

The training covers critical topics like phishing, social engineering, and safe browsing, using interactive modules that ensure knowledge retention and practical application.

With phishing, spear-phishing and vishing simulations you get to see who is retaining the knowledge and taking appropriate action and who isn't. In-depth reporting shows which of your people are and aren't actively enaging with the training.

What sets GM Cyber Awareness Training apart is its commitment to up-to-date, customisable content, aligning with the latest cyber threats and organisational standards. This not only educates employees but also cultivates a robust cybersecurity culture, making them vigilant and proactive.

By enhancing employee awareness and response capabilities, GM Cyber Awareness Training significantly reduces the risk of cyber incidents, protecting your organisation's assets and boosting its reputation for data security.

Enhanced Cybersecurity Awareness
This knowledge helps them recognise and avoid potential threats, enhancing the cybersecurity posture of your organisation.

Risk Reduction
Reduces the risk of successful cyber attacks, minimising potential financial and reputational damage to the organisation.

Compliance and Regulatory Adherence
Training assists organisations in complying with industry regulations and standards by ensuring employees' knowledge

Empowered Employees
Employees become active participants in the organisation's cybersecurity efforts, with the knowledge to make informed decisions.

Customisable Training Content
Customisable training modules that can be tailored to the specific needs and policies of your organisation

grant mcgregor
technology · people

GM Continuous Cyber Essentials Compliance

Part of GM Enhanced Security Suite

Cyber Essentials is a UK government-backed scheme that helps organisations protect themselves against the most common cyber threats.

It is important to remember that it is not an exercise for a single point in time - it expects compliance year round and puts the onus on you to demonstrate such. GM's Continuous Cyber Essentials Compliance helps you do just that.

Grant McGregor will provide you with a dedicated project manager who will guide you through a briefing on Cyber Essentials and the certification process.

They will also provide you with all the documentation you need to complete the questionnaire, including 10 customised policy documents:

- 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

Throughout the year, we'll help you keep your asset register up to date. Your dedicated project manager will guide you within the CE framework, assess your compliance level and provide assistance with the assessment.

Simplify recertification
With continuous monitoring of your devices, and expert help, recertifying for Cyber Essentials becomes easier than ever.

Maintain a secure environment
Our clever monitoring tools help ease your mind by ensuring your devices are as up to date as possible.

Demonstrate your secure credentials
Cyber Essentials certification helps you show your customers and your supply chain that you take cyber security seriously.

Expert help to ensure you're secure
We'll provide you with everything you need to submit your assessment and help put things right if they go wrong.

One Single Point of Contact
We'll assign you a project manager who'll be your helping hand to guide you through the assessment and our continuous monitoring.

GM Vulnerability Management

Part of GM Enhanced Security Suite

Reduce cyber risk with continuous asset visibility, risk-based prioritisation and built-in remediation tools to address the most critical vulnerabilities - keeping you in continuous compliance with Cyber Essentials

POWERED BY Microsoft

Assess and remediate vulnerabilities across your assets

Over 25k CVEs (common vulnerabilities and exposures) were published by CISA in 2022. As organisations accelerate adoption of digital transformation and hybrid work models, CISOs are tasked with securing their multicloud and hybrid environments against ever-evolving threats.

Uncover risks and prioritise what matters

Vast assessments are available to uncover vulnerabilities and misconfigurations across endpoints and multicloud workloads. Prioritise the biggest vulnerabilities on your most critical assets using Microsoft's threat intelligence, breach likelihood predictions and business contexts.

Leverage Microsoft threat intelligence to prioritise vulnerabilities

See the list of common vulnerabilities and exposures (CVEs) in your organisation and in the broader landscape, and view events that may impact your cyber risk.

Track and report on vulnerability management progress

Get a view that shows current statistics and vulnerable device trends over time. Access APIs with rich data for custom reporting on vulnerability management progress. Grant McGregor will make these reports available on a monthly basis.

GM Password Management

Part of GM Enhanced Security Suite

POWERED BY N-ABLE

GM Password Manager is a solution that seamlessly addresses the complexities of password management in today's digital landscape. Passwords are our digital keys but they aren't all locked in the same cabinet. They are in the heads, devices and notes app of our people.

What happens if someone leaves? Do the passwords and accounts leave with them? Are organisational accounts just forgotten?

This robust password manager ensures that your employees can securely store, manage and retrieve passwords. And importantly, means operationally important access information stays within your organisation.

With features like secure password sharing, automated password updates, and advanced encryption, it significantly reduces the risk of data breaches and cyber attacks.

Moreover, GM Password Manager's integration capabilities mean it can effortlessly fit into your existing security framework, enhancing your overall cybersecurity strategy.

By choosing GM Password Manager, you're not just adopting a tool; you're embracing a culture of cybersecurity awareness and resilience, safeguarding your organisation's digital assets against evolving cyber threats.

Enhanced Security
Employing advanced encryption to safeguard passwords, reducing the risk of data breaches and unauthorised access.

User Friendly Interface
Designed for simplicity, it offers an intuitive interface that enables users of all technical levels to easily manage their passwords.

Secure Password Sharing
Facilitating secure sharing of passwords, ensuring that sensitive information is accessible only to authorised personnel.

Automated Password Updates
Generating strong, unique passwords and automates the process of updating them, helping maintain robust security postures.

Seamless Integration
Integrates effortlessly with existing systems, providing a cohesive and streamlined experience that bolsters overall cybersecurity.

GM Encrypted Microsoft Connect

Part of GM Enhanced Security Suite

GM Encrypted Microsoft Connect is a powerful tool designed to help organisations securely access Microsoft 365 data using Zero-Trust principles.

Zero Trust Principles is a security model that assumes breaches are inevitable, and focuses on verifying every access request as if it came from an open network.

POWERED BY Microsoft

Identity-Centric Security

GM Encrypted Microsoft Connect integrates identity and network access controls to secure access to any Microsoft 365 application or resource from any location.

Conditional Access Policies

Leverages conditional access policies, including multi-factor authentication (MFA), to validate both device and user identities.

Seamless User Experience

Provides a fast, seamless, edge-accelerated access experience that balances security and productivity.

Direct Access to Microsoft

Facilitates speed and security when accessing Microsoft 365 applications by routing your traffic directly to Microsoft over an encrypted connection.

Enhanced Security

By implementing Zero Trust principles, GM Encrypted Microsoft Connect ensures that only authenticated and authorised users can access sensitive data. The solution minimises the risk of unauthorised access and potential breaches by continuously monitoring and validating access requests.

GM Managed Detect and Respond

Part of GM Enhanced Security Suite

POWERED BY Bitdefender

Advanced 24x7x365 Service to meet today's evolving cyber security needs

Do you have or wish you had a house alarm connected to a central control centre? One that can alert the authorities should an intruder be detected?

Think of our Managed Detect and Response (MDR) service like that.

With this service, a team of security experts monitor your computers, other devices and networks. If they detect something untoward they can react in real-time and respond to cyber threats 24/7.

Other advantages of GM Managed Detect and Repsond

24/7 Security Operations Centre
Providing continuous monitoring and analysis for real-time threat detection and response.

Threat Management
A systematic process of identifying, assessing, and mitigating cyber risks effectively.

Tailored Response Playbooks
Customised security protocols for specific threat scenarios for efficient incident resolution.

Expert Recommendations
Specialised advice for enhancing security postures and remediating threats.

Root Cause and Impact Analysis
Determines the origin of threats and assesses their potential or actual damage.

Monthly Service Report
Details security incidents, actions taken, and insights to improve your organisation's security

Risk-based Threat Hunting
Proactively identifies hidden threats by prioritising risks to your business.

GM Managed Detect and Respond

Part of GM Enhanced Security Suite

Our managed, advanced security prevention, detection & response service defends your business from today's elusive and harmful cyber threats.

It augments GM's Essential Security Suite baseline with two advanced modules - all wrapped with a 24x7x365 Managed Detect & Respond (MDR) plus Security Operations Centre (SOC) overwatch service.

Why we've chosen to partner with BitDefender

They gather threat intelligence across several of their products. There is more threat data fed to them every minute than there are Google queries. The sheer volume of data actually means competitor solutions often use some of BitDefender's technologies in their own products.

Tamper-proof ransomware mitigation - they've developed their own proprietary solution that ransomware can't corrupt or destroy.

No other cybersecurity vendor has been consistently rated as high as BitDefender in independent testing for prevention, protection and detection & response.

GM Enhanced Security Suite

Bringing together 7 vital services to keep you, your people and your data safe.

The best way to ensure that your business stays safe from evolving cyber threats is to create a multi-layered defensive posture.

With GM Enhanced Security Suite you get technology, training and compliance in one simple package - putting in place the crucial layers you need.

Four invaluable services and technologies to keep you and your business safe from evolving cyber threats. One simple price.