



# The Dynamic Security Lifecycle Framework

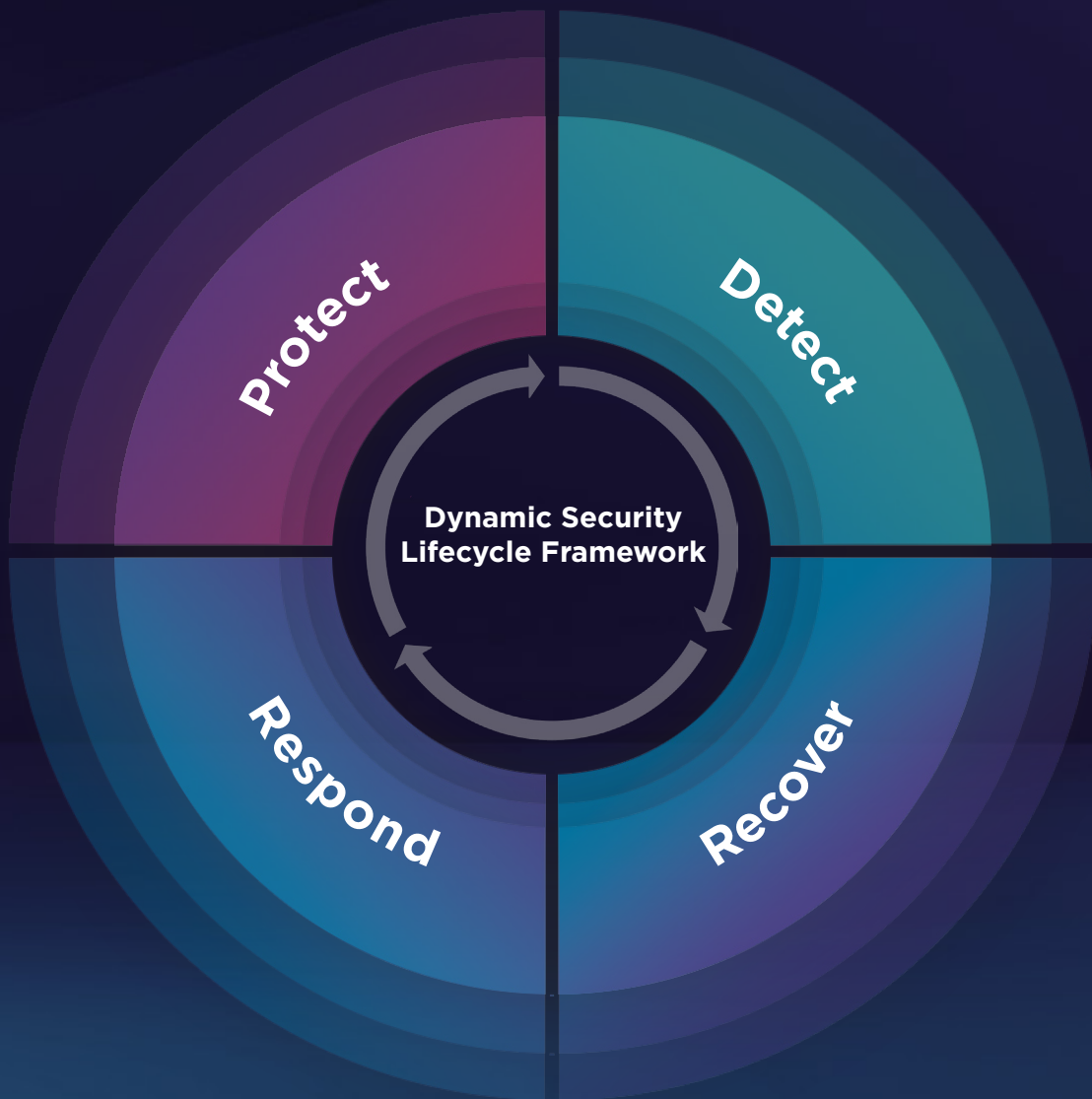
**A guide** for finance decision makers, procurement teams, CIOs, CTOs and technology analysts in SME organisations

# Keep it simple

Security breaches and legal compliance are the top two current concerns for the boardroom as 'mission critical' protection becomes vital for business survival.

Governments across the globe are actively encouraging greater awareness and action.

In the race to guard against the devastating damage to reputation and loss of revenue that can occur following a cyber incident, our Dynamic Security Lifecycle Framework can help to simplify the way you think about your security solutions and vendor management.



Whether you are tackling lack of bandwidth to investigate alerts or lack of budget to purchase more mature solutions for the post-Covid world, protection, detection, and a suitable plan for response and recovery are key considerations.

# Protect

Protection of IT infrastructure, systems and information is essential and should be your first port of call.

This can be achieved by looking at:

- **Dynamic system protection**

Real time protection for critical infrastructure by detecting, alerting and taking immediate corrective action against a breach - and stopping an attack 'dead in its tracks'.

- **Managed firewalls**

This is one solution most businesses understand well. A managed firewall helps monitoring network traffic, assessing the live cyberthreat landscape, and providing around-the-clock management, support and protection for your network, systems and end-points.

- **Distributed Denial of Service (DDoS)**

Advanced protection against criminal cyber extortion through dynamic threat detection at your perimeter, where a third party can identify and block malicious traffic.

- **Email Protection**

More than 90% of cyberattacks infiltrate organisations via email. Scanning, filtering and backup services will ensure your email systems are fully protected.

- **Advisory and design**

Pick a partner with extensive cyber security expertise and specialist consultants to help you audit existing infrastructure and processes - identifying current vulnerabilities, recommending and implementing robust security solutions that meet your specific requirements.

## Top three lifecycle priorities and business outcomes

- Evolving cyber security strategy
- Mitigating cybercrime and adapting to evolving malware and cyber threats
- Unifying protection across networks and cloud environments

# Detect

**Detection, identification and removal of breaches is vital, including detailed reporting to support investigations and meet compliance requirements.**

Keeping ahead of the cybercrime threat is a massive challenge for in-house IT departments who have many other priorities to deal with. It's why a growing number of companies prefer to rely on managed security services, rather dealing with it internally.

**This can be achieved with:**

- **Detect and respond**

Continuous and dynamic protection and mitigation against malicious cyber threats including automated defensive actions and real-time behavioural data analysis.

- **Intrusion detection**


24/7 monitoring - keeping your data and systems safe by alerting you to attacks on network and systems, malicious activity and violations of behavioural policy.

- **Managed threat detection**

A cyber security operations centre (SOC) always protects your infrastructure and systems, including secure access service edge (SASE) models, threat intelligence reporting, data collection and on-going risk analysis.

- **Security, Information and Event Management (SIEM)**

SIEM solutions provide next-generation incident detection, along with detailed analytics and automated responses - ensuring informed, decisive action is taken promptly.



## Top four ways to simplify security management across your business

- Understanding what is happening and what is needed
- Security solution trials to discover what is possible
- Discussing proof of concepts with your service provider
- Regular cyber security audits

# Respond and recover

The ability to 'rewind and reset' to a point just before an incident is invaluable. No data loss, no public awareness or reaction, and no damage to your reputation.

This can be achieved by:

- **Digital incident response**

Ensures immediate action is taken to protect your systems and data. Immediate handling, containment and mitigation of the event will help prevent a recurrence.

- **Incident management planning**

Develop a strategy and plan to protect and mitigate against an attack - including training, system testing, security exercises, data analysis, compliance and regulation checks.

- **Managed network and security**

A 24/7 cyber Security Operations Centre (SOC) relieves management, providing immediate remedial action in the event of an incident to protect networking, data and systems.

- **Digital incident reporting**

Forensic examination all incident data to understand what happened, with detailed reporting and insight enabling the speedy remediation and prevention of any recurrence.

- **Disaster Recovery as a Service (DRaaS)**

Dynamic real time failover and replication of your virtualised computing environment to a secure, separate disaster recovery platform, ensuring business continuity.

- **Cloud system backup**

A back-up of your systems and data is housed in a highly secure, separate and resilient location, providing point-in-time recovery with simple backup and restoration of systems.

- **Virtual Chief Information Security Office (CISO)**

Regular, flexible and formalised access to a senior security expert to help develop and implement security measures for effective and continuous protection of your organisation.



# VCG offers

**We enable businesses to protect, detect, respond and recover from cyber attacks with minimum disruption and maximum resilience.**

Our security services include accelerated detection, automation and response from the desktop to the cloud, complementing a complex portfolio of end-point protection services for data and applications. We also offer dynamic business continuity planning to keep your business users, data and assets protected.

**We can offer you:**

## One day security review

**We are offering a review of your security profile, to discuss your business objectives and how they drive your security strategy.**

This will provide you with your current position, security weaknesses within the environment based on critical attack vectors and recommendations to improve your overall security position.

**One day assessment / 1 day report on most engagements.**

This can extend to Penetration Testing the environment with vulnerability assessments as an additional extra.

## 20 days proof of concept

**20 days free trial of:** • Umbrella DNS • AMP4E • DUO • CMD

## Free 30 minute security assessment

**30 minutes to identify, assess, review and discover issues with your security set up and discuss solutions for future strategy**

- Identify and assess existing assets and infrastructure – what are the risks you are being exposed to?
- Review technology and existing security infrastructure across the organisation
- Discover what's possible to protect your business, data and reputation

**To request more information, please click here**



# Why VCG?

Our vision is to help organisations thrive by simplifying technology choices, transformation journeys, and digital resilience.

We aim to support you in your next stage of growth, next marketplace, or IT challenge with solutions and services that help optimise your business.

**We create and support a more connected workplace and a seamless interaction with your business-critical applications, on premise or in the Cloud.**

- **Technology transformation partner**
- **Dedicated support and Managed Services**
- **Cost and operational efficiency driver**
- **Trusted advisor and end-to-end partner**

**Get in touch** - find out how our security services could work for you

Call 0161 406 1820 Email [sales@vcg.group](mailto:sales@vcg.group) Visit [vcg.group](http://vcg.group)

