

Technical Solutions



It's been estimated that if an unprotected device is brought online, it will be attacked and infected within just 20 minutes - GCN

Whether you want to update your legacy systems, or are looking to migrate to a public or dedicated cloud, Cyberfort will design, build and deliver an end-to-end solution across whatever technology you require. Our 'secure-by-design' service builds security into the very structure of your architecture. We ensure your data is protected at rest and in transit, always available without disruption.

Cybersecurity is all we do. We understand the network security landscape, giving you advice, guidance and providing 360-degree comprehensive and modular risk mitigation strategies and solutions. Cyberfort's experienced technical architects will design a cost-effective solution to meet your specific needs and technical and security requirements, leaving you free to focus on your own business priorities.

Technical Solutions Services



Network Security

As networks transition from traditional hosted models to the cloud, it's more important than ever to have robust network security. Excellent network security also provides a reliable backbone for your entire IT estate. Getting your network security right will reduce both the likelihood and impact of a cyber breach. Network security covers a broad range of technical and procedural controls. We'll analyse and improve your network security, whatever the scale, complexity or business priority.



Cloud Security and Migration

Whether you're new to the cloud or have already migrated, Cyberfort's experienced teams can help you use the cloud securely. For existing cloud users, Cyberfort will advise you on how to introduce or improve security across your entire platform. We can align this to numerous industry frameworks, offering you a stable, demonstrable cloud security approach and a pragmatic baseline to promote enhanced security postures. All the major cloud service providers can host sensitive data with high levels of assurance. However it is critically important that cloud users do not delegate overall responsibility for security and take the necessary steps to ensure their implementation fully utilises the security controls offered. Cyberfort has extensive experience of securing cloud services to provide independent assurance to client security teams, extending internal capabilities and undertaking knowledge transfer where appropriate.



Architectural Review and Guidance

Cyberfort's experienced security architecture practice is designed to help you produce the most appropriate, effective and repeatable security designs. Based on industry recognised frameworks, including SABSA and TOGAF, Cyberfort's security architects will review, create and enhance your Consulting Services security documentation. Cyberfort is vendor-agnostic, and will only recommend products that meet your specific business requirements and comply with your legal and regulatory obligations.



Security Testing

Testing your technical security controls is vital to your continuous security improvement strategies. It provides evidence that your controls are working as they should to prevent penetration by intruders. Cyberfort's compliance service works in tandem with the cybersecurity suite of services to scope and deliver strategic, targeted and cost-effective security penetration and application testing. We work with you to identify high-value assets and operationally critical targets. We then develop testing methodologies to ensure the controls in place are working effectively. The results from these tests will feed into a continuous vulnerability management (CVM) strategy to routinely test for weaknesses and quickly remediate any issues found.

Your technical security challenges

The technical landscape is constantly changing, presenting challenges in keeping your information secure and your business running smoothly. Cyberfort's Advisory services are designed to provide a versatile and tailored approach to your cybersecurity challenges. These challenges may include:

- Understanding cloud service models, migration strategies and cloud security principles
- Understanding industry best practice (eg. NCSC Cloud Security Principles)
- Lack of in-house technical expertise
- Lack of knowledge of networks and how to keep them secure
- Not knowing how to secure legacy systems and solutions
- The challenge of articulating technical security risks at board-level

How Cyberfort can help you

We're vendor agnostic and will offer a multi-layered approach to understanding your security posture, determining the 'to-be' state, and ensuring your entire business is secure in the following ways:

- Tailored, Scalable and experienced resources
- Testing and improving your entire IT environment's security
- Understanding and advising you on the right path to your organisation's security journeys
- Delivery of certified, industry-recognised methodologies
- Multi-layered approach to organisational security
- We'll review your existing architecture and, if necessary, design and implement an improved framework
- Project management of all resources to orchestrate and integrate activities and deliverables
- Excellent knowledge in technical security frameworks, including:
 - Cyber Essentials/Cyber Essentials Plus
 - CIS Top 20
 - ISO 27000
 - NCSC Guidance
 - NIST CSF
 - AWS Well-Architected Framework
 - CSA CCM