UKFAST®
YOUR FUTURE IS OUR BUSINESS

G-CLOUD SERVICE DEFINITION

LOT: CLOUD SUPPORT

PENETRATION TESTING AND ETHICAL HACKING

0800 923 0601
UKFAST.CO.UK

UKFast®
YOUR FUTURE IS OUR BUSINESS

CONTENTS

Introduction to UKFast 3

Information Assurance 4

Penetration Testing and Ethical Hacking 5

Services 6

Service Features 7

Service Management 11

Buying our Services 15

Pricing 18

UKFAST®
YOUR FUTURE IS OUR BUSINESS

INTRODUCTION TO UKFAST

UKFast is the largest privately-owned hosting provider in the UK, with a comprehensive network of fully owned, high specification data centres, from which cloud services, managed hosting and colocation services are delivered. UKFast has more than 20 years' experience in delivering cloud-based solutions to a range of public sector clients including the NHS, MoD, the Cabinet Office and police forces.

As an exclusively UK-based company, we offer guaranteed data sovereignty. We fully own, manage and operate the UKFast data centre complex including the land it's built on, housing more than 30,000 sq. ft. of enterprise-grade, ISO-certified facilities.

Our PCI compliance and ISO certifications, including ISO 27001, are managed by a dedicated compliance team to ensure our customers have a professional partner in UKFast. Our continued investment, dedication and credentials are further reinforced by high levels of accreditations and qualifications across support personnel, technology and infrastructure. All services, including administration and support and all data including backups and DR capabilities, are entirely hosted within the UK, and all members of the system administration team are vetted by UKVS, holding SC Clearance.

UKFast's dedicated hosting solutions are complemented with award-winning client support, provided by a highly knowledgeable and skilled team, with extensive experience within the sector. Implementing bespoke support structures unique to client requirements, UKFast's 24/7/365 comprehensive support is exclusively UK based. We pride ourselves on our industry-leading Net Promoter Score (NPS), which is consistently in excess of +80 (ten times the industry average).

HIGHLIGHTS

- Accredited as a Secure Data Centre by HMG Departments including Home Office (PASF)
- HSCN, PSN, PSN for Policing, MoD RLI/ALI and Internet Connectivity
- Protective monitoring compliant with NCSC GPG-13
- Separation of personnel administering public-sector operations to those supporting commercial operations with strong two-factor authentication logged profile-based access
- Centralised authentication and authorisation throughout the corporate environment
- Large volume of bespoke proprietary software developed in house to facilitate operational control and reduce supply-chain dependency
- In-house team of experts in penetration testing and ethical hacking, providing additional security service for proactive testing and verification of high security standards
- Support and data centre work all undertaken by UKFast personnel, without reliance on third parties

INFORMATION ASSURANCE

We have an extremely robust and proven security policy and have gained the following accreditations through being independently audited and assessed. We continually improve our processes in information security, quality management and environmental management to facilitate a secure and efficient quality-of-service to our customers.

- ✓ ISO 27001:2013 Information Security Management System
- ✓ ISO 27017:2015 Code of practice for information security for cloud services
- ✓ ISO 27018:2014 Protection of personally identifiable information in public clouds
- ✓ ISO 22301:2012 Business Continuity Management System
- ✓ ISO 9001:2015 Quality Management System
- ✓ ISO 14001:2016 Environmental Management System
- ✓ PCI DSS Level 1 Service Provider
- ✓ Cyber Essentials +

Additionally, our third-party penetration testers hold the following certifications:

- ✓ CREST Certified Tester
- ✓ Cyber Scheme Team Leader
- ✓ Tiger Scheme Senior Security Tester

OFFICIAL / OFFICIAL-SENSITIVE

- For Dedicated Circuit Connectivity you will require one of the following:
  - Site-to-site IPSEC or SSL-based VPN
  - Dedicated fibre direct to our data centre
  - CAS(T) \ Non-CAS(T) compliant connections via MPLS and leased line
  - CPA overlay encryption where required
- For access to the PSN you must be a PSN service provider or hold a PSN certification
- Access to HSCN requires an ODS code and compliance with NHS Digital obligations framework

UKFAST®
YOUR FUTURE IS OUR BUSINESS

PENETRATION TESTING AND ETHICAL HACKING

With cybersecurity firmly on the agenda, public sector businesses are becoming increasingly aware of their organisation's exposure to hackers and the cyber-threats that face their business. Ultimately more has to be done to ensure that customer, employee and third party data remains safe.

Penetration testing has become an essential tool used to expose weaknesses before hackers do. Also known as ethical hacking, it ensures that your public sector business remains safe behind security that works. Security breaches can cost millions, but very few companies are taking the fundamental steps to prevent them from happening. Businesses could save money, and their reputation, by proactively testing for vulnerabilities within their network.

A team of skilled and reliable third-party security professionals simulate a full assault using internal and external attack vectors to test the ability of your systems/environment to withstand a cyber-threat. The goal is to identify vulnerabilities in the network so that they can be secured before a hacker discovers the same holes.

BENEFITS

Taking a proactive approach to online security will ultimately save you time and money. With many public sector organisations already becoming targets, it is important for your business to have identified and eliminated weaknesses to help you avoid a costly outcome. A penetration test will enable your business to:

MINIMISE RISKS	EXPOSE WEAKNESSES	EVALUATE SECURITY
A preventative approach that interrogates your infrastructure for vulnerabilities.	Protect your business, employees, suppliers and customers from holes in your security solutions and avoid data theft.	Regular tests are essential to certify that your infrastructure can protect your business against the latest threats.

SERVICES

IT HEALTH CHECK (ITHC)

An IT Health Check (ITHC) is used to confirm that your information systems and network meet a specified baseline standard. Also known as Codes of Connection (CoCo), these rules are used by organisations like the NHS and the Gambling Commission to ensure only trusted partners are able to exchange data online.

The ITHC provides assurance to your partners that internal and external systems are protected from unauthorised access. This includes wireless access points which connect to the internal network and remote working devices, such as company smartphones. You will need to complete an ITHC once per year – or risk losing access to these trusted resources, such as the NHS Public Service Network (PSN).

MOBILE AND WEB APPLICATION SECURITY

Mobile and web applications are crucial to making data available to employees, customers and partners. But these systems that simplify data availability within the business are attractive targets for cybercriminals. These highly connected applications draw data from numerous internal resources and databases. If hackers can compromise your applications, they can use this foothold to exploit other network resources, or to steal IP and client data. Identifying and addressing vulnerabilities in your web-enabled applications is essential to raising the standard of security within your operations.

INFRASTRUCTURE SECURITY

Weaknesses within your network infrastructure are used by cyber attackers to gain entry to protected resources – like personal data or financial systems. Once inside your network, attackers can exfiltrate data, extort money or cause general disruption and destruction.

An infrastructure assessment probes your network nodes and software, identifying vulnerabilities before they are exploited. Using the same tools and techniques as the criminals, Fidus consultants scan and analyse every aspect of your infrastructure searching for weaknesses that need to be addressed.

SERVICE FEATURES

PHASE ONE: PROJECT SCOPING

Phase one consists of a comprehensive scoping period to ensure all project requirements and deliverables are defined and mutually agreed.

PHASE TWO: RECONNAISSANCE

Reconnaissance is the first step towards building an effective plan of attack, and is split into passive and active. The former involves gathering information on a target without actively engaging with its infrastructure (internet and social media searches); in contrast, the latter involves our pen-testers engaging with the targeted systems. This will help us to identify:

- IP address ranges
- Naming conventions
- Hidden servers or networks
- The times that transactions take place
- Where your traffic is going

PHASE THREE: VULNERABILITY SCAN

This scan initially points out the vulnerabilities in your network which our pen-testers then further exploit during the attack. This scan is in two parts:

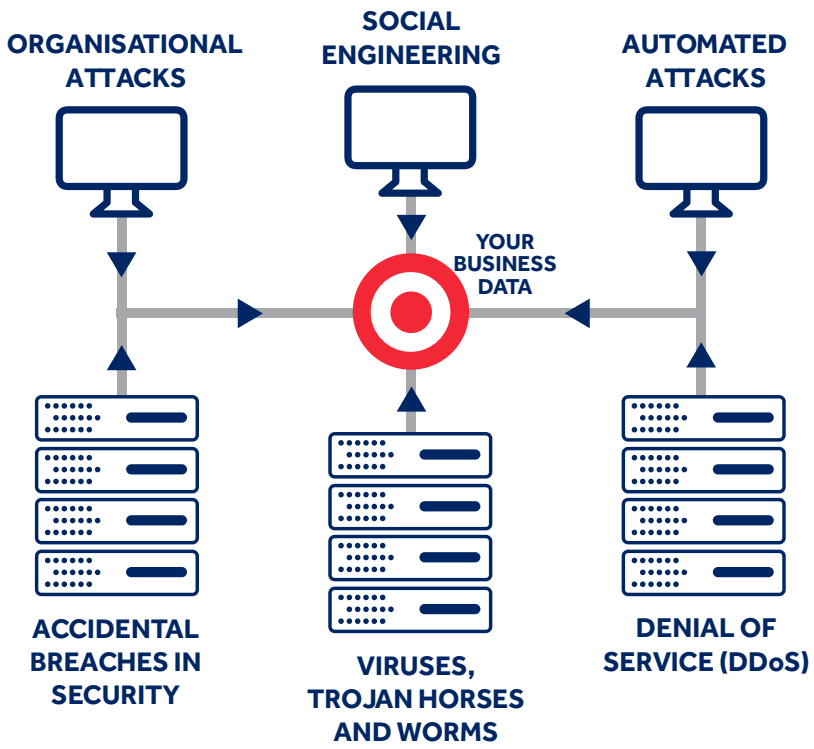
- Server scan – identify open ports, services and known vulnerabilities
- Application scan – hits the website and tests all user inputs for insecurities.
- Network scan – detect all endpoints present on a network

PHASE FOUR: PENETRATION TEST

Our security professionals use the information from the vulnerability scan and the reconnaissance phase to then further profile your systems and launch a full-scale attack to exploit as many vulnerabilities as possible. We typically target:

- Network infrastructure
- Web applications
- Websites and ecommerce systems
- Database servers and storage
- Remote entry points
- Email servers
- Employee workstations

Figure 1:Penetration testing diagram



What do we test for?

- Unpatched vulnerabilities in services, operating systems and applications
- Insecure programming
- Insecure (default) configuration
- Weak passwords
- Weak access control
- Insider attack

We test for vulnerabilities using the following attack methods, all listed in the Open Web Application Security Project (OWASP) top 10:

1. Injection
2. Broken authentication and session management
3. Cross-site scripting (XSS)
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function level access control
8. Cross-site request forgery (CSRF)
9. Using known vulnerable components
10. Unvalidated redirects and forwards.

All of our practices are based on methodology set out by OWASP (a worldwide not-for-profit charitable organisation focused on improving security) so that we can ensure best practice when we are examining how secure your site is.

PHASE FIVE: REPORT

Once we have completed the attack processes we present you with a full report which covers the following:

- Executive summary
- List of vulnerabilities and their severity
- Our technical approach
- Detailed findings and recommendations for remediation.

PHASE SIX: MITIGATION TESTING

Once your business has remedied its vulnerabilities, you have the option to carry out another penetration test focused on the original issues discovered to determine whether the fixes have been successful in stopping our initial attack. This approach not only safeguards your data, but also your customers', employees', suppliers' and that of other third parties associated with your business, easily delivering a respectable return on investment.

SERVICE MANAGEMENT

SERVICE LEVELS

Our network is provided with a 100% network uptime guarantee and 24/7/365 expert technical support as described in table 1. UKFast will reasonably endeavour to meet the following timescales for a support requirement:

AVAILABILITY	
Network	100%
Infrastructure *	99.99%
customer Portal	99.90%

* Monthly
** Based on customer's software architecture following our high availability guidelines.

Availability is based on the total number of operating hours of a given calendar month and excludes planned and emergency maintenance.

Downtime is defined as including issues arising from the UKFast-based network, hardware, virtualisation and base operating system components of the IaaS offering, not at the customer's application layer.

MAINTENANCE NOTIFICATIONS

We custom-built our UK data centres using only enterprise-grade, highly resilient infrastructure, allowing full control and flexibility. UKFast therefore applies the following procedures for the notification of maintenance:

PLANNED MAINTENANCE

Planned maintenance means periods of maintenance of which the customer has been made aware in advance on five (5) days prior notice by UKFast and which may cause disruption of service due to non-availability of the specific service.

Wherever possible, planned maintenance will be carried out without affecting the service. This will generally be achieved by carrying out planned maintenance during periods of anticipated low traffic and on part, not all, of the network at any one time.

EMERGENCY MAINTENANCE

When emergency maintenance is needed, such as a major fault with a power system that is likely to affect the service, UKFast will endeavour to inform the affected parties wherever possible with a minimum of 24- hours' notice. Please note in exceptional circumstances, dependent upon the nature of the emergency, this could be without notice as the scenario dictates.

FINANCIAL RECOMPENSE MODEL

Service Credits

If UKFast does not comply with the Service Levels it shall pay Service Credits to the customer. The customer's right to such Service Credits is in addition to, and not in substitution for, any other rights arising from UKFast's failure to provide Services in accordance with the terms of the Contract.

Availability - In respect of any month when the level of Availability (as defined above under Service Levels), indicative Service Credits below:

% AVAILABILITY ACHIEVED	SERVICE CREDIT DUE (AS A % OF THE STANDARD SUPPORT FEE FOR THE MONTH IN QUESTION)
99.999% or less (but more than 99.50%)	2%
99.99% or less (but more than 99.25%)	5%
99.95% or less	10%

In respect of any month when UKFast fails to comply with the Service Levels (for P1 and P2 severity requests) indicative Service Credits listed below:

PERCENTAGE OF SUPPORT REQUIREMENTS IN RESPECT OF WHICH ONE OR MORE SERVICE LEVEL WAS NOT ACHIEVED	SERVICE CREDIT DUE (AS A % OF THE STANDARD SUPPORT FEE FOR THE MONTH IN QUESTION)
More than 2.5% (but less than 5%)	2%
5% or more (but less than 10%)	5%
10% or more	10%

TECHNICAL BOUNDARIES

RESPONSIBILITIES	UKFAST	CUSTOMER
Purchase of Hardware and infrastructure	✓	
Architecture and build	✓	
Base OS installation and IP configuration	✓	
Management above the VM level (Including OS)	✓	
Citrix environment administration	✓	
Availability and Health monitoring	✓	
Line of business and third party applications		✓
Citrix user management		✓
Third-party applications		✓

* Monitoring available to assist customer

UKFAST RESPONSIBILITIES

Managed and Unmanaged Network Infrastructure Boundaries

In all instances, UKFast takes responsibility for the management of network infrastructure from the point of the external connection terminating with the external interface of a UKFast-operated Layer 3 device (Edge Router, Firewall, VPN Terminator) within our data centres. In the case of the terminating device being customer managed, responsibility is taken from the internal facing interface port. Beyond these interfaces, management of service connectivity is deemed to be the responsibility of the individual connectivity provider (PSN, MPLS, network provider etc.). External Layer 2 termination is not permitted.

Unmanaged Support Boundaries

Unmanaged services are provided with support for the underlying base infrastructure, hardware, core networking and virtualisation. Installation of the Base OS and initial IP configuration will be performed by UKFast, but no OS or application support will be offered beyond this.

Managed Support Boundaries

Managed support provides comprehensive break/fix and health management support across the environment's networking, hardware and virtualisation stacks. It also includes OS support and coverage for applications on our supported software list when running in a supported configuration.

CUSTOMER RESPONSIBILITIES

UKFast is unable to be responsible for:

- Issues with, or which are caused by, third-party software installed by the customer and/or the support of applications that do not feature on either UKFast's supported applications list or as part of the agreed intended functionality of the platform (as agreed in the contract specification documents) and coding and/or development support
- Issues within, or which are caused by, the customer's code
- Administration/management of access and responsibilities for the customer's end-users and for the administration/management of any layers above IaaS. UKFast is not responsible for application security and/or data encryption at the application or OS level
- The suitability of UKFast's services in light of the nature of any data stored on the customer's solution and for determining what steps are appropriate for maintaining security, protection and backup.
- Issues caused by negligence on the part of the customer, its employees, servants or agents.

BUYING OUR SERVICES

ON-BOARDING AND OFF-BOARDING

On-boarding and off-boarding are the processes for beginning to use our services and for when you finish using our services.

ON-BOARDING

We offer services to enable seamless on-boarding and collaborate to design a bespoke solution to meet your requirements. An example phased on-boarding process is demonstrated below:

1. **Discovery**
    - 1.1. Project management teams from both parties meet to identify all moving aspects and understand resource requirements for the project. This will identify any setup fees required
    - 1.2. Initial high-level process agreed and highlighted to all involved
    - 1.3. Owners of key project areas agreed & assigned
2. **Timelines**
    - 2.1. Mutually agreeable timelines are decided
    - 2.2. Milestones are determined
    - 2.3. Project phases defined with resources allocated for each phase
    - 2.4. Deliverables are agreed
3. **Risk**
    - 3.1. Project risk assessments are performed
    - 3.2. RAG reports are agreed
    - 3.3. Escalation chains are defined
4. **Implementation**
    - 4.1. This is when the on-boarding team comes alive and begins the steps from the discovery to the timeline agreed
    - 4.2. User Acceptance Testing (UAT) and initial testing completed for each milestone before sign-off to move to the next phase
5. **Quality Assurance**
    - 5.1. A post implementation clean-up of the old environment
    - 5.2. A debrief and review meeting for the project is held including lessons learned.

SOLUTION ASSESSMENT

We take an ITIL 4 compliant approach to assess your organisation in relation to your readiness for your solution. We assess your current infrastructure and applications and create a service catalogue of applications and services and make recommendations about how best to implement your solution.

OFF-BOARDING

A similar process to on-boarding is provided for customers wishing to leave UKFast. We provide full transitional services at an additional charge (please refer to the pricing document for more details). An example phased off-boarding process is demonstrated below.

1. Discovery: UKFast meets the customer's new provider who will lead the project
2. Timelines: Timelines are agreed where possible and alternatives offered when needed
3. Risk: UKFast identifies any risks that may not be apparent to the new provider or that are inherent to the UKFast solution
4. Implementation: UKFast assists the new provider if needed
5. Quality Assurance: UKFast offers a debrief and review meeting if the new provider requires.

TRAINING

We offer a range of online resources including docs.ukfast.co.uk for detailed technical guidance, UKFastTV for video content, and MyUKFast for basic FAQs and contact with the support team. We offer internally and externally resourced training options, which can be designed around your needs. Our custom-built training centre (see Qualifications section above for further details) is available for customers to host in-house training, run workshops and hold exams on a complimentary basis.

ORDERING AND INVOICING

Orders will be accepted via a signed UKFast or G-Cloud order form. UKFast order forms can be signed digitally online through your MyUKFast portal. Invoices are then raised on a monthly basis with an agreed upfront setup fee chargeable (please refer to the on-boarding process and pricing document for more details).

LEAD TIME

Once an order has been accepted, creation of a new customer within MyUKFast will be completed within 48 hours. The design and deployment of the solution will be assigned resources within five days of order acceptance, dependent on the complexity of the requirements.

CONTRACT TERMINATION

Terms

Please refer to the G-Cloud call-off contract and UKFast's Terms & Conditions for rights to terminate. Agreements shall be entered into for an initial minimum term. An exit fee would be payable if the agreement is terminated before the end of the minimum term.

Domain name transfers will not be made until all outstanding amounts have been paid by the customer, until which time domain names remain the property of UKFast.

Any customer data stored will only be extracted by UKFast with the prior consent of the customer. UKFast shall purge and destroy (as defined in security accreditation for different ILs) customer data from any of its own equipment after the contract ends.

PRICING

For Pricing please refer to the UKFast Pricing Summary and SFIA Rate Card.

UKFAST®

YOUR FUTURE IS OUR BUSINESS

0800 923 0601

UKFAST.CO.UK

MANAGED HOSTING | CLOUD | DATA CENTRES