



# NetFACTS Datasheet

Network Forensics, Audit, and Control Testing Service

## What is NetFACTS?

NetFACTS is a combined network-based assurance and assessment service, designed to measure the collective efficacy of deployed security controls across IT systems, infrastructure or an entire estate. NetFACTS exception reports provide evidence of real events and actual incidents; covering sophisticated attack detection – including infiltration and exfiltration incidents, corporate or third party security policy violations, and specific compliance non-conformities.

Traditional technical assurance services, such as penetration testing and configuration audits, are intended to exhaustively identify all possible vulnerabilities, weaknesses and exposures within an autonomous scope based on perceived and often unquantified threats without consideration of business context and the organisation's risk profile. Whilst penetration testing is an essential part of most technical assurance programmes, a collective measurement from NetFACTS provides a complementary and pragmatic view of security performance in a much wider context, reporting on actual security events and incidents. NetFACTS provides a prioritised approach to risk management and within security maturity models, by assisting with targeted treatment planning, whether through the application of technical changes or updates to policies, procedures and standards.

NetFACTS can measure both the general health and security posture of an organisation at network level as well as the effectiveness of existing security controls, and can be integrated as a security KPI.

## How is NetFACTS facilitated?

At the front end of the service is a proprietary NetFACTS hardware probe which is positioned at the network edge, capturing all packets entering and leaving the perimeter. The probe is initially deployed for a fixed duration performing Deep Packet Capture (DPC) of all traffic traversing the perimeter.

Prior to deployment of the NetFACTS probe, IRM consultants will organise a conference call or workshop to understand the threat landscape & key data assets, review the controls and undertake a short risk profiling exercise. This knowledge enables customised configuration of the probe and targeted analysis of captured data based on the organisation's unique security objectives.

The probe is returned to the IRM Forensics Operations Centre, where an experienced team of technical consultants will analyse the data captured by the probe. Once analysis is complete, a formal report will be produced that includes an executive summary, risks and recommendations table, detailed event descriptions and remediation advice. Forensically sound capture files can be retained by IRM should evidence of incidents be required in any ensuing legal or disciplinary action.

**Information Assurance**  
**Risk Mitigation**  
**Business Resilience**  
**Compliance**



**NetFACTS Service Levels**

There are two NetFACTS service levels:

**Standard Service**

The NetFACTS standard service is a single engagement that provides comprehensive traffic analysis and a full report of security events using a probe deployed for a limited duration.

**Subscription Service**

Following the initial standard service engagement, the probe(s) can be redeployed and captured traffic reviewed periodically as required; this provides ongoing assurance and review as part of a continuous improvement cycle, and can add significant value to compliance programmes that may require monitoring, logging and auditing controls. In addition, the probe can operate in 'flight recorder mode', which can be retrieved for analysis at any point when a serious event is triggered.

**Key Benefits Overview**

Security & Risk Management Benefits	Technical Benefits
✓ Measures enterprise network security as a single entity.	✓ Comprehensive network security monitoring.
✓ Supports a prioritised approach to security management programmes.	✓ Supports a prioritised approach to technical remediation.
✓ Promotes benchmarking and continuous improvement for security maturity models.	Sophisticated intrusion detection using traditional approaches, public and proprietary signatures, heuristic techniques and manual analysis methodologies.
✓ Provides assurance and efficacy measurement of legislative requirements and compliance standards.	✓ Identifies vulnerable software including web browsers, email clients and web servers; and attacks against them.
✓ Identifies policy violations, such as Acceptable Use Policies (AUP) and Data Handling/Classification breaches, and ineffective enforcement controls or ineffective policies.	✓ Identifies intentional unauthorised connectivity and deliberate circumvention of controls over the network perimeter.
✓ Forensically sound full network packet capture - supporting legal or disciplinary actions.	✓ Identifies unintentional network information leakage caused by poor egress filtering or routing.
✓ Assists management of incident response by acting as a 'Flight Recorder' of network events at a forensics level.	✓ The deep packet capture capability of the probe plays a key role in any incident response where events can be fully replayed and analysed.

**Legislative and Compliance Standards Applicability**

- ✓ BS ISO 27002:2005

The NetFACTS service coverage into ISO 27002 is extensive and applicable to many controls within the eleven clauses; in particular - Communications and Operations Management, Compliance, Information Security Incident Management and Asset Management.
- ✓ Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS Requirements 10 and 11 concern regular monitoring and testing of networks; the NetFACTS service provides a framework for measuring the monitoring the effectiveness of controls and methodologies. NetFACTS analysis can be specifically fine tuned to identify elements of cardholder data, such as unencrypted PANs, that may be traversing a network perimeter.
- ✓ HMG Security Policy Framework

The Security Policy Framework dictates universal, mandatory standards across Government. Security Policy No 2 outlines the requirements of the Government Protective Marking System (GPMS). NetFACTS can provide assurance that government assets remain within established network perimeters.
- ✓ Data Handling Procedures in Government (2008)

The 'Data Handling Procedures in Government' publication puts in place new measures to protect information which is applicable across all central Government. NetFACTS can assess many of the core protective measures and those controls stated within the 'Cross Government Actions: Mandatory Minimum Measures' document.
- ✓ UK Data Protection Act (DPA)

Principle 7 of the Data Protection Act states 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.' NetFACTS' deep packet capture can help identify information leakage of this nature.

**About IRM**

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.

