CYBER

Vulnerability Scanning

Minimise overall threat exposure to known vulnerabilities

4D's Vulnerability Scanning provides a detailed snapshot of your IT infrastructure, proactively identifying and classifying your exposure to known vulnerabilities.

Deployed as part of 4D's integrated cyber security offerings, vulnerability scanning is a highly impactful step to minimise your security exposure – at a point in time – to help protect your business from attackers looking to exploit vulnerabilities across your digital assets.

Business Challenges

Scarce resources, limited time and an evolving threat landscape can make it difficult for IT teams on the front lines to keep pace with the latest tools, tactics and techiques of cyber criminals. 4D's Vulnerability Scanning service is a fast and easy way to proactively find and fix vulnerabilities.

4D's Multi-layered Cyber Protection

Maintain business continuity with 4D's Cyber Security solutions

Managed Firewalls
Industry-leading perimeter protection

DDoS Protection
Safeguard your network and data

Threat Monitoring
Proactively minimise overall threat exposure

Managed Backups
Last line defence against system failure

Vulnerability Scanning vs. Penetration Test – are they the same?

A vulnerability scan and penetration testing are often confused, but in fact the two security procedures are quite different:

VULNERABILITY SCAN	PENETRATION TEST
A **Vulnerability Scan** is a technical security assessment using a set of tools to scan your network for known vulnerabilities (e.g. open ports, unpatched security updates, incomplete deployment of security technologies).	A **Penetration Test** (Pen Test) is a manual test and attempts to exploit these vulnerabilities to determine whether unauthorised access or other malicious activity is possible - an ethical hack.

Why scan for vulnerabilities?

- Proactively defend against the constantly evolving and increasingly sophisticated threat landscape
- The nature of today's cloud, on-premise and hybrid network environments requires continuous monitoring to protect your organisation's data and systems 24/7
- Enhanced legal complexity and required regulatory compliance (For example, PCI DSS compliance, Cyber Essentials PLUS, Cisco CIS)

Why 4D?

4D Data Centres is an independently owned UK-based managed infrastructure provider with facilities in Gatwick, Surrey, Kent and London. Since 2007, we've delivered colocation, cloud, cyber and connectivity services to hundreds of small and large-scale organisations.

Vulnerability Scanning Services

4D uses Tenable Nessus – the de facto industry standard for Vulnerability Assessment - along with other tools for scanning and network security auditing.

WHY NESSUS?

- **#1 in Accuracy** - the industry's lowest false positive rate with six-sigma accuracy
- **#1 in Coverage** – more than 130,000 plugins, coverage for more than 50,000 CVE and over 1000 new plugins released weekly within 24 hrs of vulnerability disclosure
- **#1 in Adoption** – trusted by more than 27,000 organisations globally

Service Features

Malware Detection

Uncover and mitigate malware attempting to attack your systems

Advanced Scanning

Broad and deep visibility into vulnerabilities with every assessment

Automated Scheduling

Specify automation at a time that works best for your business

Risk-based Reporting

Risk scored reporting with expert next actions

Visibility into Missing Patches

Don't miss 3rd party security updates across multiple software platforms

What to expect?

4D's Vulnerability Scanning follows a defined methodology to identify possible points of weakness, uncovering system and network flaws to help you implement a proactive threat-prevention strategy.

PREPARATION & SCOPE

Flexible service delivery will allow you to discuss, define and agree the scope of the scanning requirements to meet specific infrastructure requirements.

EXECUTION OF VULNERABILITY SCAN/S

Scans are comprehensively conducted to discover exposure areas across your network to determine, assess and prioritise vulnerabilities based on exploitability.

REPORT & RECOMMENDED NEXT ACTIONS

In-depth report, with risk scored vulnerabilities and an overall risk score based on the volume and severity of vulnerabilities found within your network, applications, devices and IT assets.

Guide Pricing

Our vulnerability scanning can scale to any size organisation, from small businesses to enterprise-level, specifically designed to fit your organisation's requirements.

From £100/month for monthly scanning of 10 IP addesses

Technical Specifications

Our intelligently-designed vulnerability scanning can be deployed for use on any system. It is compatible with Windows, Linux, Apple, and a wide range of other servers, so no matter what your system operates on, we can help keep it safe. Additionally, we can scan any part of your system, including your databases, network devices, firewalls, and web applications. No matter how your system is configured, or how many different elements there are, our vulnerability scanning will keep every aspect of it secure.

Types of scanning and reporting:

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services:

- Amazon AWS
- Office 365
- Salesforce
- Microsoft Azure
- Rackspace

This type of scan may require pre-notification to the third party.

Badlock Detection
Local and remote checks for CVE-2016-2118 / CVE-2016-0128

Bash Shellshock Detection
Local and Remote checks for CVE-2014-6271 / CVE-2014-7169

Basic Network Scan
A full system scan for any host

Patch Audit
An audit that logs into a system to perform a full security patch audit of OS and third party applications

Drown Detection
Remote Checks for CVE-2016-0800

Host Discovery
A simple scan to discover open ports and live hosts on a network subnet

Malware Scan
Scan for malware on Windows or linux Systems (inc. Mac)

Policy Compliance Audit
Audit System Configurations against a known baseline

Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers Leaks

Spectre & Meltdown
Remote & Local checks for CVE-2017-5753 / CVE-2017-5715 / CVE-2017-5754

Wannacry Ransomware
Remote and Local checks for MS17-010 / CVE-2017-0144

Web Application Tests
Scan for published and unknown web application vulnerabilities

The data floor at 4D's Gatwick Data Centre

Take the next step

4D's Cyber Security Solutions supports cloud transformation, infrastructure and data management with an integrated approach to strengthen your overall security posture.

Discover why hundreds of organisations like yours trust us with their data and infrastructure security.