



## Overview

The CNS **COMPLIANCE**Engine **SCAN** Service offers a comprehensive suit of tools that provides:

- ❑ Granular host configuration compliance checking for; service, configuration and patch level compliance on \*nix, Windows, Cisco and more.
- ❑ Configuration change tracking and alerting on network devices, network and host vulnerability scanning, port scan and port diffs reporting on: Compliance failures, Patch exposures & Configuration errors

The CNS **COMPLIANCE**Engine **SCAN** Service offers organisations additional levels of assurance that their corporate hosts, network and IP addresses will continue to be assessed as the new potential vulnerabilities or compliance breaches emerge.

Compliance reports generated by the system are reviewed by a senior member of CNS' Security Assessment Team and published on the secure shareportal. Results of each scan, alert or breach report shall be cross checked against the previous data to track trends.

XML output to SIM/SEM and ad hoc customer report generation is supported (including browse and dashboard reporting). The Service requires the installation of a small device on the customer network which is monitored 365 x 24 hr from the CNS Security Operating Centre. Users of the Service are able to view live data and generate realtime reports via a secure web interface.

The **COMPLIANCE**Engine **SCAN** Service is undertaken using CNS' own, standards based, Scanning & Alerting Engine. This type of configuration reporting allows organisations to specify a technical build template for each host type and to report compliance against this template (i.e. ports, patches, services, configuration settings).

An unlimited selection of secure builds can be used and organisations can specify bespoke settings for CNS' service desk to include in reporting, thereby ensuring that actual compliance is reported upon to the customers specific internal standards.

**COMPLIANCE**Engine  
scan report certify

## SERVICES

### SECURITY ASSESSMENT

Penetration Testing  
Application Testing  
Code Review  
PCI DSS Audit  
ISO27001 Audit  
Risk Assessment  
Security Audit  
Compliance Audit  
Configuration Review  
GAP Analysis  
RMADS

### MANAGED SERVICES

24 x 365  
Threat Alerting  
Threat Management  
Device Management  
Change Management  
Fault Resolution  
Secondments  
Compliance Monitoring  
**SECURITY SOLUTIONS**  
IPS/NAC  
Secure Networking  
Design & Installation  
Firewall & VPN  
Identity & Authorisation

## ACCREDITATION



## COMPLIANCEngine SCAN Standard Features and Functions

Service	Devices	Functionality
Configuration Change Alerting	Network devices	<ul style="list-style-type: none"> <li>• Alert on configuration change, either triggered or on timed check.</li> <li>• Ongoing configuration backup.</li> <li>• Configuration diffs and full history.</li> </ul>
Configuration Audit	Network devices	<ul style="list-style-type: none"> <li>• Automated configuration check on firewall ruleset.</li> <li>• Nipper report output.</li> <li>• Automated audit on configuration change.</li> <li>• Optional alerts</li> </ul>
Vulnerability Scans	Network devices	<ul style="list-style-type: none"> <li>• Nessus vulnerability scan and output</li> </ul>
Patch Checking	Hosts (*nix, Windows)	<ul style="list-style-type: none"> <li>• Patch checking on *nix, Windows host</li> <li>• List of missing patches on per host basis</li> <li>• Timed scan</li> <li>• Optional categorization of patches by criticality</li> <li>• Nagios dashboard integration</li> </ul>
Configuration Checking	Hosts (*nix, Windows)	<ul style="list-style-type: none"> <li>• Configuration checking against defined baselines</li> <li>• List of configuration fails on a per host basis</li> <li>• Nagios dashboard integration</li> </ul>
Vulnerability Scans	Hosts (*nix, Windows)	<ul style="list-style-type: none"> <li>• Nessus vulnerability scan and output</li> </ul>
Configuration Back-up	Network Devices	<ul style="list-style-type: none"> <li>• Ongoing configuration backup.</li> <li>• Audit Log of Last known "good" Configuration</li> <li>• Immediate deployment of clean configs</li> </ul>
Port Scans	All	<ul style="list-style-type: none"> <li>• Regular port scans and diffs as required</li> </ul>

## COMPLIANCEngine SCAN Bespoke Features and Functions

- AV status
- Application (e.g. Oracle, SQL, Apache) configs and changes
- configuration change on AD policies
- file/db column change alerting
- password strength checks

**COMPLIANCEngine**  
scan report certify

## About CNS

Convergent Network Solutions Ltd was established in 1999 in response to market demand for a highly skilled security and networking consultancy in the heart of the city. CNS has grown rapidly since this time, both in company size, the depth and breadth of services offered and reputation for providing exemplary service. The company is majority owned by the principle directors.

**CNS**  
NETWORKS & SECURITY

76 Cannon Street  
London, EC4N 6AE  
www.cnsuk.co.uk  
info@cnsuk.co.uk  
Tel: +44 (0)20 7213 0999  
Fax: +44 (0)20 7213 0990