

# Assuria Auditor

System Security. Assured.



**Configuration Assurance. Vulnerability Assessment. Change Detection. Compliance.**

## Known and Trusted Systems

Maintaining effective levels of information security is impossible without having a clear view of system configurations, current patch states, hardware and software components, user structures, privileges, file permissions and the state of security controls.

Security administrators need configuration assurance – i.e. assurance that systems are in a *known and trusted state*.

## Assuria Auditor

Software solutions such as **Assuria Auditor**, which provide a deep dive internal view of system configurations, are designed to provide this system configuration assurance. Assuria Auditor is deployed in hundreds of government agencies and commercial enterprises in more than 30 countries worldwide.

## Key Features

Assuria Auditor features include; vulnerability assessment, standards compliance assessment, configuration audit, inventory reporting, patch checking and change monitoring. Using an extensible and flexible architecture, Assuria Auditor provides vital protection for business systems and helps maintain systems in a secure and known state.

## Compliance & Vulnerability Assessment

Assuria Auditor is a market leader in assessing and reporting on system vulnerabilities and compliance to regulatory standards (such as ISO27001 and PCI-DSS).

Assuria Auditor measures, manages and reinforces security policy and security good practice, assessing security controls, detecting and reporting security vulnerabilities and security standards non-compliance. Outputs include detailed instructions on how to reconfigure systems to remediate these issues.

## Inventory reporting

Assuria Auditor provides inventory reporting features, listing all hardware components and installed software packages, versions, open ports and much more.

## Change Monitoring

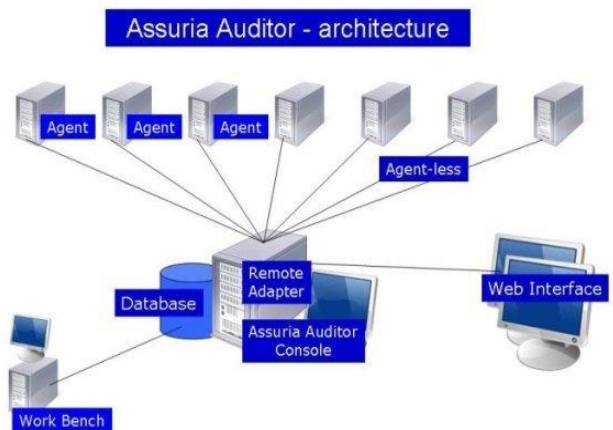
System administrators and security operations centres can be alerted to configuration changes, or changes to system elements and applications. These powerful change detection features allow rapid assessment and reporting of suspicious or unauthorised changes.

## Agent Based and Agentless

Assuria Auditor offers a blend of both agent based and agentless scanning approaches, depending on which approach is most appropriate to meet operational requirements.

For example, where the highest levels of integrity and automation are required, Assuria Auditor uses powerful, self contained and unobtrusive software agents. This is especially important within virtualised environments.

But, where use of software agents is undesirable, Assuria Auditor uses secure, credentialed remote scanning, using the same checks and scan policies as agents. Agent based and agentless operations can be run side by side, in a common environment.



The Assuria Auditor methodology simplifies the creation of system security baselines for users, groups, shares, services and critical system files, and easily fits in with existing business processes. Highly scalable, Assuria Auditor manages large agent populations. For example, our largest user manages more than 1,300 servers nationwide, managed from just 6 control centres.

## Assuria Auditor Features

**Regulatory Standards Compliance.** The comprehensive built-in security database includes mappings of each of Assuria Auditor's 2500+ security configuration checks to appropriate references within a range of standards such as **ISO 27001, BS17799, SOX, PCI-DSS, GCSX CoCo** and others.

With Assuria Auditor it is easy to assess server compliance against almost any standard. Detailed remediation instructions enable even inexperienced system administrators to quickly bring systems up to the level of compliance needed. Powerful reporting also provides verification to satisfy auditors. CVE and BID references are also provided, with CVSS scores where appropriate.

**Internal Policy Compliance.** As well as monitoring compliance with external standards and accepted best practice in security configuration, Assuria Auditor allows users to adjust checks and policies and even write new checks to match the specific requirements of internal security policies.

**Vulnerability Assessment.** Delivered with a comprehensive security knowledge base of more than 2500 configuration checks, patch checks and best practice policies, Assuria Auditor detects potential vulnerabilities, assists with assessment of risk and recommends steps required to mitigate those risks.

**Change Monitoring.** Assuria Auditor enables the creation of system baselines and will monitor those baselines for any changes, including changes to executables, data files, configuration files and registry keys. Change monitoring can be run in automated mode (i.e. scheduled) or in interactive mode.

**Distributed Management Framework.** This framework enables operational role based management of agents and agentless scanning from anywhere on an enterprise network. Large server networks can be managed from a single console and multiple consoles provide almost limitless scalability.

**Virtualisation.** Assuria Auditor is fully compatible with virtual environments, both VMware and Hyper-V. The built-in security knowledge base includes virtualisation checks and VMware ESX and ESXi platforms can be scanned via agents or remotely.

**Comprehensive Reporting** Management and technical reports are provided, identifying security weaknesses, poor configuration, compliance issues and missing patches, with detailed remedies and solutions. Powerful report customisation features allow tailored reporting and report exportation.

**Auto Updates.** Regular monthly security content updates ensure that hosts are protected from even the most recent vulnerabilities and exploits, also allowing rapid distribution of new product features.

**Customisable Checks.** Assuria Auditor is delivered with a huge number of vulnerability, configuration and best practice checks as part of the built-in knowledge base, organised into subject related policies. These checks are written in Tcl, in plain language, so that understanding what each check is doing is easy. Also, the built-in Policy Navigator allows users to easily develop custom policies of their own, to modify built-in checks and even to develop custom checks in order to meet organisation specific needs.

### Supported Platforms:

Assuria Auditor Console Platforms:

- Windows Server 2003, 2008.

Assuria Auditor scanning targets:

- Windows Server 2003
- Windows Server 2008/2008 R2
- Windows 7
- Solaris SPARC 7, 8, 9, 10 and 10 x86
- AIX 5.1+, 6.1
- HP-UX – PA-RISC and ITANIUM 11+
- Red Hat Enterprise Linux
- SUSE Enterprise Linux X86
- SUSE Enterprise Linux 10 IBM Z series
- VMware ESX 3.5
- VMware ESX 4.x

Assuria Limited,  
Reading Enterprise Centre,  
University of Reading, Earley Gate,  
Reading, RG6 6BU, United Kingdom  
W: [www.assuria.com](http://www.assuria.com) E: [info@assuria.com](mailto:info@assuria.com)  
T: +44 118 935 7395 F: +44 118 935 7330

Assuria Partner