vicarius

vRx vRadar

Compliance Scan

The Compliance Scan evaluates systems against recognized security benchmarks, PCI DSS (External ASV & Internal), FISMA, HIPAA, NERC CIP, SOX, IAVA, NESA Benchmarks, DISA STIG, and SCAP profiles, to ensure required controls and configurations are in place. Instead of identifying CVEs, it validates system hardening, policy enforcement, and configuration posture.

How it works

1. **Benchmark selection** - Applies predefined or custom benchmarks such as CIS, DISA STIG, and other SCAP-based standards.
2. **Auth config collection** - Uses credentials or agents to gather system configuration data.
3. **Control evaluation** - Executes XCCDF and OVAL checks to validate each control on the target system.
4. **Pass/fail assessment** - Evaluates each rule independently per control and per asset.
5. **Standards-aligned reporting** - Maps findings to benchmark controls; produces audit-ready reports.

What you get

- **Pass/fail results per compliance control**
- **Compliance scores per asset and benchmark**
- **Evidence for each failed configuration**
- **SCAP-compatible output for auditors**
- **Mapping between controls and remediation**

Why it's important

- **Validates system hardening and security baselines**
- **Supports regulatory requirements (SOC 2, PCI DSS, ISO 27001)**
- **Complements vulnerability scanning with posture validation**

Comparison to Competitors

Capability	vRadar	Nessus	Qualys	Rapid7	OpenVAS
Compliance Scan	**Native – not repurposed audits**	Audit-based	Separate PC module	Partial support	SCAP-dependent
SCAP Native	**Full SCAP (open standards)**	Partial / proprietary	Partial	Limited	SCAP supported
Benchmark Coverage	**CIS, DISA STIG, SCAP built-in**	CIS & STIG files	CIS & STIG (PC mod)	Limited depth	Content-dependent
Pass/Fail	**Explicit per control & asset**	Yes	Yes	Partial	Yes
Audit Output	**SCAP-compliant formats**	Compliance reports	Dashboards / reports	Limited	Limited