vicarius

Discovery Scan

Network Scan

# vRX
# vRadar

vRadar delivers full vulnerability visibility without the heavy appliances, false positives, or deployment headaches of legacy scanners. Inference-driven vulnerability testing, compliance, and CIS hardening – all in a single unified platform.

CIS Scanner

Compliance Scan

Full Vulnerability Scan

# Discovery Scan

A discovery scan identifies which hosts in a network are active before deeper scanning begins. It is the first phase in any vulnerability assessment, used to build an accurate inventory of reachable devices and prevent wasted time scanning inactive IPs.

## How it works

1. **ICMP echo sweep** - Sends ping requests to each target IP.

↓

2. **TCP SYN/ACK probes** - If ICMP fails, sends SYN packets to common ports (22, 80, 443) and interprets replies as “alive”.

↓

3. **ARP requests (local)** - Uses ARP or IPv6 ND to discover devices even when ICMP/TCP is blocked.

↓

4. **Nmap integration** - Runs Nmap discovery with multiple techniques – SYN, ACK, UDP.

↓

5. **Extensive mode** - Scans all IPs without discovery filtering for full coverage, at cost of speed.

## What you get

- **Reachable hosts with IP and optional hostname**
- **No CVE data – forms input list for subsequent scans**
- **Exportable as an asset inventory baseline**

## Why it’s important

- **Ensures resources target only active systems**
- **Reduces false negatives via multiple probe types**
- **Missed hosts here create blind spots in all subsequent scans**

## Comparison to Competitors

| Feature | vRadar | Nessus / Tenable | Qualys | Rapid7 | OpenVAS |
|---|---|---|---|---|---|
| ICMP Ping Sweep | ✓ **Native** | ✓ | ✓ | ✓ | ✓ |
| TCP / UDP Probes | ✓ **Selectable** | ✓ | ✓ | ✓ | ✓ |
| ARP / IPv6 ND | ✓ **Built-in** | ✓ | ✓ | ✓ | Partial |
| Nmap Integration | **Native full flags** | None native – internal engine | None native – internal engine | None native – internal engine | Partial |
| Fine-tuned control | **ICMP, SYN, ACK, UDP** | Limited | Limited | Limited | Moderate |

# Network Scan

The network scan identifies open ports, active services, and operating systems across live hosts, mapping the network-facing characteristics of each device, the foundation for deeper vulnerability and compliance assessments.

## How it works

1. **TCP & UDP port scan** - Checks each host for open ports using SYN scans (TCP) and probe-based discovery (UDP).
2. **Service identification** - Banner grabbing and protocol negotiation to identify software and version.
3. **OS fingerprinting** - TCP/IP stack analysis via integrated Nmap (-O) and Xprobe2 for OS and kernel version.
4. **Network enumeration** - Queries DNS, RPC, SNMP, and shared filesystems for additional context.
5. **Scan policy tuning** - Fully tunable timing, port range, depth, and aggressiveness.

## What you get

- **Open Ports: Full TCP/UDP port list per host**
- **Services: Application and version per port**
- **OS Details: Operating system and kernel version**
- **Network Metadata: DNS, shares, SNMP info**
- **Attack Surface Map: Input for vulnerability scans**

## Why it's important

- **Reveals all externally reachable entry points**
- **Detects rogue or unauthorized services on the network**
- **Validates segmentation and firewall enforcement**

## Comparison to Competitors

| Feature | vRadar | Nessus / Tenable | Qualys | Rapid7 | OpenVAS |
|---|---|---|---|---|---|
| Port Scan Depth | **Full TCP/UDP range** | Fixed templates | Preset cloud range | Fast, less deep | Configurable, slow |
| Service ID | **Deep banner analysis** | Common svc focus | Limited, cloud sync | Basic port mapping | Plugin-dependent |
| OS Fingerprinting | **Dual-engine (Nmap + Xprobe2)** | Single proprietary | Internal logic only | Simplified detect | Outdated fingerprints |
| Network Enum | **DNS, RPC, SNMP, shares** | Common data only | Agent-reported only | Basic data only | Plugin-dependent |
| Scan Policy Ctrl | **Full tuning options** | Fixed templates | Centralized only | Automated presets | Manual, complex |

# Full Vulnerability Scan

A Full Vulnerability Scan is an end-to-end assessment that identifies security weaknesses across all discovered hosts, ports, and services. It combines host discovery, port scanning, and deep vulnerability probing for the most complete coverage possible.

## How it works

1. **Host discovery** - Detects active systems using ICMP, TCP, and ARP probes.
2. **Port scanning** - Identifies open TCP/UDP ports across the full range.
3. **Service detection** - Determines type and version of every running service.
4. **Vulnerability testing** - Inference engine runs targeted checks — each detected service triggers specific modules, results activate deeper checks.
5. **Credentialed scanning** - Optional — with admin credentials, checks missing patches, registry entries, and config issues.

## What you get

- **Vulnerability details: severity, CVE references**
- **Affected host, service, and proof-of-concept evidence**
- **Prioritization by severity and exploitability**
- **Actionable remediation and patching guidance**

## Why it's important

- **Comprehensive risk visibility across network and application layers**
- **Patch validation and compliance reporting in a single pass**
- **Reduces attack surface by identifying exploitable weaknesses early**

## Comparison to Competitors

| Capability | vRadar | Nessus / Tenable | Qualys | Rapid7 InsightVM | OpenVAS |
|---|---|---|---|---|---|
| Core Approach | **Full: discovery → deep vuln testing** | Strong plugin orchestration | Cloud-based detection | Multi-phase + asset context | Basic, limited plugin accuracy |
| Coverage | **Full network, OS, app library** | Broad plugin-based | Cloud-integrated library | Wide + contextual priority | Community-maintained |
| Credentialed | **Windows, SSH, OS-level** | Full coverage | Trusted scanning | Agent-assisted | Limited by plugin scope |
| Customization | **Policy-based: Full, Patch Tue, Net Device...** | Template selection | Prebuilt cloud profiles | Flexible site-based | Manual setup required |
| Exploit Integ. | **SAINTexploit (optional)** | External tools | None | Metasploit integrated | None |

# 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 |

# CIS Scanner

The CIS Scanner evaluates systems specifically against CIS Benchmarks, the industry-standard hardening guidelines for operating systems, cloud platforms, and applications. It provides granular pass/fail results per CIS control mapped to Level 1 and Level 2 benchmark profiles.

## How it works

1. **Benchmark selection** - Selects Level 1 or Level 2 CIS profile for the target OS or application.
2. **Authenticated access** - Uses credentials or agent to collect configuration and registry data.
3. **Control-by-control evaluation** - Runs each CIS check individually against the benchmark.

## What you get

- **Per-control pass/fail mapped to CIS Benchmark IDs**
- **CIS Level 1 and Level 2 scores per asset**
- **Evidence and remediation per failed check**
- **Benchmark-structured reports for audits**
- **Visibility into drift from approved CIS baselines**

## Why it's important

- **CIS Benchmarks are the gold standard for system hardening across industries**
- **Bridges the gap between vulnerability scanning and configuration compliance**

## Comparison to Competitors

| Capability | vRadar | Nessus | Qualys | Rapid7 | OpenVAS |
|---|---|---|---|---|---|
| Native CIS Support | **Built-in – no add-on** | Audit files (manual) | Policy Compliance module | Partial depth | Content-dependent |
| CIS Level 1/2 | **Distinct level scoring** | Partial | Yes | Limited | No |
| Pass/Fail Control | **Explicit per control & asset** | Yes | Yes | Partial | Yes |