COMPARE HACKUITY

Hackuity vs. Tenable

See how Hackuity compares with Tenable for vulnerability operations, risk prioritization, remediation workflows, deployment flexibility, and enterprise control.

Request a demo | Download comparison



Which platform is the better fit?

CHOOSE TENABLE IF

Vulnerability discovery is your priority

Best suited for organizations prioritizing a single-vendor platform consolidating VM, cloud, identity, OT, and AI.

- You need single-vendor platform consolidating VM, cloud, identity, OT, AI
- You prefer native Tenable scanning across your environment
- You prioritize breadth over VM-specific depth
- You have limited EU data residency requirements

VS

CHOOSE HACKUITY IF

Reducing cyber risk is your priority

Optimized for vendor-neutral aggregation, transparent risk prioritization, and European sovereignty requirements.

- **You require vendor-neutral aggregation without scanner lock-in**
- **You need transparent, auditable risk prioritization**
- **You operate in Europe with GDPR, NIS2, data sovereignty requirements**
- **You want a VOC-focused platform built for Vulnerability Operations**
- **You need on-premise or hybrid deployment options**
- **You need a specialist vendor with an agile, EU-based R&D team focused solely on Vulnerability Operations**

COMPARISON TABLE

Capability comparison

Capability	Tenable	Hackuity
Vendor Neutrality	Not core focus Favors Tenable scanners	Strong fit 130+ integrations, no scanner bias
Risk Scoring Transparency	Not core focus Proprietary ExposureAI scoring	Strong fit Transparent TRS, fully auditable
European Data Sovereignty	Not core focus US-headquartered, limited EU data residency options	Strong fit EU SaaS, hybrid, on-prem options
On-Premise Deployment	Not core focus Cloud-first architecture	Strong fit Fully on-prem supported
Platform Breadth (Cloud, OT, Identity)	Strong fit Comprehensive Tenable One	Not core focus VM-focused only
Native Scanning Capabilities	Strong fit Nessus ecosystem + cloud sensors	Not core focus Aggregation only, no scanning
VM-Focused R&D	Partial fit Spread across multiple domains	Strong fit 100% dedicated to VM maturity
Analyst Recognition	Strong fit Gartner Leader, Magic Quadrant for Exposure Assessment Platforms, 2025	Strong fit Forrester UVM Landscape Q1 2025 - Forrester Proactive Security Landscape Q1 2026

DIFFERENCIATORS

Where Hackuity stands apart.

01

Built for your whole security stack

Connect findings from 130+ security tools, including Qualys, Tenable, Rapid7 and CrowdStrike. Hackuity normalizes everything into one place, without favoring one scanner or ecosystem.

02

Know exactly why something is critical

Every True Risk Score is explainable. See the threat signals, asset context and business weight behind it. Your team can understand, defend and tune every priority.

03

Turn priorities into remediation

Finding vulnerabilities isn't the hard part. Fixing them is. Hackuity routes vulnerabilities to the right owners, syncs with ITSM tools, tracks SLAs and proves remediation.

04

Your data. Your deployment.

Choose EU SaaS, hybrid or fully on-premise. Keep vulnerability data where you need it, with deployment options built for European security and regulatory requirements.

05

Deep integrations, not just connectors

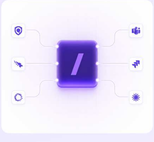
Hackuity doesn't just ingest findings. It connects vulnerability data with assets, threat intelligence and remediation workflows, so teams can act from one place.

130+ INTEGRATIONS

Keep your scanners. Add the operating layer.

Hackuity is designed to work with your existing scanners, cloud tools, asset inventories, threat intelligence feeds, and ITSM workflows. Instead of replacing your stack, Hackuity connects it, normalizes it, and turns fragmented findings into operational action.

Explore Hackuity connectors →



SCENARIOS

When teams choose Hackuity

SCENARIO 01

From Nucleus-centric VM to vendor-neutral CTEM

Nucleus is a capable vulnerability management platform. But if your stack includes tools beyond what Nucleus natively integrates, coverage gaps appear. Hackuity normalizes findings from every tool, 130+ connectors, no scanner bias, into one exposure view, and adds the CTEM operating model Nucleus does not provide.

Explore CTEM →

SCENARIO 02

Building a Vulnerability Operations Center on top of Nucleus

Nucleus tells you what's vulnerable and surfaces risk priorities. It doesn't route ownership, enforce SLAs, or prove remediation progress to your board. Hackuity turns findings into a structured operational program, from triage to closure to reporting.

Explore VOC Coming soon

SCENARIO 03

Delivering managed vulnerability services at scale

Nucleus targets MSSPs but is not purpose-built for multi-tenant service delivery. Hackuity is designed for it from day one: isolated client environments, per-client reporting, and a scalable VOC model that grows with your practice without adding operational overhead.

Explore MSSP →

Still evaluating your options?

Hackuity vs. Qualys → | Hackuity vs. Brinqa → | Hackuity vs. Nucleus →

FAQ

Questions buyers ask when comparing platforms

Does Hackuity replace Tenable? −

No, and that is intentional. Tenable is one of the best discovery engines in the market. Hackuity connects to it, normalizes its findings alongside data from your other tools, and adds the prioritization and orchestration layer Tenable does not provide natively. Your Tenable investment stays intact. Hackuity makes it more actionable.

How is Hackuity's risk prioritization different from Tenable's? −

Tenable scores vulnerabilities based on CVSS and its own ExposureAI model. Hackuity's True Risk Score goes further: it combines threat intelligence, EPSS, CISA KEV, asset criticality, and your business context into one explainable, tunable score. Every decision is auditable. Your team knows exactly why a vulnerability was prioritized, and can challenge or adjust it at any time.

Why would I choose Hackuity over Tenable One? −

Tenable One is designed for organizations standardized on the Tenable ecosystem. Hackuity is a vendor-neutral Vulnerability Operations platform that aggregates findings across your entire security stack, prioritizes risk using transparent scoring, and orchestrates remediation across teams. If you use multiple scanners, cloud security tools, code security tools, or ITSM platforms, Hackuity gives you a unified view without vendor lock-in.

Ready to compare Hackuity with your current setup?

See how Hackuity fits your security program, prioritizes cyber risk, and supports your remediation workflows.

Request a demo | Explore the platform