COMPARE HACKUITY

Hackuity vs. Nucleus Security

See how Hackuity compares with Nucleus Security for vulnerability operations, risk prioritization, remediation orchestration, deployment flexibility, and enterprise control.

Request a demo | Download comparison



Which platform is the better fit?

A pragmatic, buyer-oriented view to help map software capabilities to actual team requirements.

CHOOSE NUCLEUS IF

Federal compliance is your priority

Best suited for organizations prioritizing US Federal compliance, automated POA&M processes, or deep native FedRAMP Moderate requirements.

- You are a federal agency, defense contractor, or SLED requiring FedRAMP Moderate
- You need automated POAM compliance with NIST SP 800-53, FISMA, or CMMC
- You want 200+ integrations with FlexConnect for custom data ingestion
- You prioritize AI-powered CTI via Nucleus Insights for vulnerability enrichment

VS

CHOOSE HACKUITY IF

Reducing cyber risk is your priority

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

- **You need transparent, auditable risk prioritization your team can validate and tune**
- **You want a platform built exclusively for Vulnerability Operations maturity**
- **You want to consolidate findings from any scanner, cloud tool, or ITSM without vendor lock-in**
- **You need a full VOC operating model, from triage to SLA enforcement to verified closure**
- **You operate in Europe with GDPR, NIS2, or data sovereignty requirements**

COMPARISON TABLE

Capability comparison

Capability	Nucleus	Hackuity
European Data Sovereignty	Limited US-headquartered (Florida), AWS infrastructure	Strong fit EU SaaS, on-prem, hybrid: GDPR and NIS2 aligned
Risk Scoring Transparency	Partial fit AI-enriched scoring via Nucleus Insights	Strong fit Transparent TRS, fully auditable and tunable
FedRAMP & US Compliance	Strong fit FedRAMP Moderate, POAM automation, FISMA, CMMC	Limited Not focused on US federal compliance
VM-Focused R&D	Partial fit R&D split with US federal compliance requirements	Strong fit 100% dedicated to VM/VOC maturity
Integration Breadth	Strong fit 200+ connectors + FlexConnect custom framework	Strong fit 130+ native connectors, vendor-neutral by design
Remediation Orchestration	Partial fit Standard ticketing automation	Strong fit Advanced routing, SLAs, feedback loops
Deployment Flexibility	Limited SaaS (AWS/GovCloud) + self-hosted on-prem option	Strong fit SaaS, on-prem: EU-compliant deployment
Analyst Recognition	Strong fit Gartner Challenger EAP MQ 2025 · IDC Major Player 2025	Strong fit Forrester UVM Landscape Q1 2025 · 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 Operating levels

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. Tenable → | Hackuity vs. Brinqa → | Hackuity vs. Qualys →

FAQ

Questions buyers ask when comparing platforms

How is Hackuity's risk scoring different from Nucleus Insights?

Nucleus Insights is an AI-enriched, analyst-curated threat intelligence feed that enriches vulnerability data automatically. Hackuity's True Risk Score goes a step further: it combines threat intelligence, EPSS, CISA KEV, asset criticality, and your business context into one score your team can audit line by line. More importantly, it is tunable by perimeter, asset type, and organizational context. You do not just receive the output, you own and control the methodology.

Nucleus is FedRAMP certified. Does Hackuity have equivalent compliance credentials?

Nucleus has invested heavily in US federal compliance, including FedRAMP Moderate, FISMA, and CMMC. Hackuity is SOC 2 Type II certified and IMDA accredited, and is designed for European regulatory requirements including GDPR and NIS2. If your primary compliance requirement is US federal, Nucleus has a clear advantage. If you operate under European or international frameworks, Hackuity is the stronger fit.

Both platforms target MSSPs. What makes Hackuity different for managed services?

Nucleus supports MSSP use cases as part of a broader enterprise platform. Hackuity is purpose-built for multi-tenant service delivery: isolated client environments, per-client SLA policies, white-label reporting, and a VOC operating model designed to scale across dozens of clients without adding operational overhead. For MSSPs building a structured vulnerability operations practice, that architectural difference matters from day one.

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