COMPARE HACKUITY

Hackuity vs. Brinqa

See how Hackuity compares with Brinqa 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 BRINQA IF

Enterprise exposure management is your priority

Suited for large enterprises seeking to unify exposure data, business context, and remediation across complex environments.

- You need AI-powered exposure management across broad cyber risk domains
- You operate a large enterprise with a heterogeneous security tool stack
- You want AI agents to surface patterns and ownership gaps automatically
- You operate in regulated industries (banking, finance, insurance, utilities) with complex compliance requirements

VS

CHOOSE HACKUITY IF

Reducing cyber risk is your priority

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

- **You need risk prioritization based on a methodology your team can audit and tune, not just trust**
- **You want quantified operational outcomes: 99% noise reduction, 3x MTTR**
- **You operate in Europe with GDPR, NIS2, data sovereignty requirements**
- **You want VM/VOC capabilities from dedicated platform**
- **You prefer vendor-neutral aggregation with transparent scoring**

COMPARISON TABLE

Capability comparison

Capability	Brinqa	Hackuity
Risk Scoring Transparency	Partial fit Proprietary AI scoring via BrinqaIQ, limited tunability	Strong fit Transparent TRS, fully auditable and tunable
Deployment Flexibility	Not core focus Cloud SaaS with agent-based on-prem data collection	Strong fit SaaS, fully on-prem
European Data Sovereignty	Not core focus US-headquartered, limited EU data residency	Strong fit EU SaaS, on-prem options
AI-Powered Insights	Strong fit BrinqaIQ, AI agents, Cyber Risk Graph	Strong fit SmartEx®, MCP Server, Remediation Advisor...
Cyber Risk Breadth	Strong fit Multi-domain: VM, cloud, identity, app security	Not core focus Vulnerability Operations focused
Remediation Orchestration	Partial fit Bidirectional ITSM sync, limited SLA policies and playbooks	Strong fit Full ITSM sync, SLA policies, playbooks, bidirectional workflows
VM-Dedicated R&D	Partial fit Broad cyber risk and exposure management focus	Strong fit 100% dedicated to VM/VOC maturity
Analyst Recognition	Partial fit Gartner Niche Player, Exposure Assessment Platforms, 2025	Strong fit Forrester LVM 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. Tenable → | Hackuity vs. Qualys → | Hackuity vs. Nucleus →

FAQ

Questions buyers ask when comparing platforms

How is Hackuity's risk prioritization different from Brinqa's? –

Brinqa uses AI-powered scoring through BrinqaIQ to surface risk. Hackuity's True Risk Score is built on a transparent, explainable methodology: every decision shows which threat signals, asset criticality, and business context drove the priority. More importantly, your team can tune it by perimeter, by asset type, by organizational context. You don't just trust the score, you understand and own it.

We're a European organization. Does that change the decision? –

Yes, significantly. Brinqa is US-headquartered with limited EU data residency options. Hackuity is built in Europe, offering EU SaaS, hybrid, and fully on-premise deployment. For organizations operating under GDPR, NIS2, or sector-specific regulations, data residency and deployment control are not optional. Hackuity is designed for those requirements from day one.

Brinqa covers a broader range of cyber risk domains. Is Hackuity too narrow? –

That depends on what you need to solve. Brinqa is a broad exposure management platform spanning VM, cloud, identity, and application security. Hackuity is purpose-built for Vulnerability Operations: 100% of R&D is focused on VM and VOC maturity. If your primary challenge is vulnerability management at operational depth, prioritization, orchestration, SLA enforcement, and measurable risk reduction, a dedicated platform will outperform a broad one every time.

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