YOUR UNIFIED VM PLATFORM
AGGREGATE | PRIORITIZE | AUTOMATE

Business Challenge

For 20 years, VM has been limited to inventorying, assessing, and remediating. Except that 80% of cyberattacks leverage a vulnerability known for the past half decade. Fragmented teams, too many tools, and exploding vulnerabilities are a match made in heaven – for attackers.
Case in point: MITRE reports the yearly increase of CVEs is up 476% compared to a mere decade ago. In 2013, your team faced just over 5000 new vulnerabilities and exposures. Today 25,000 new CVEs hit the market every year. That's exponential pain. Despite the average breach costing $4.35 million (source: IBM) and taking nine months to contain last year, cybersecurity teams are experiencing tighter budgets, and three out of four are pursuing vendor consolidation. Meanwhile, Gartner predicts that by 2025, 50% of cybersecurity leaders will have tried and failed to use cyber risk to drive enterprise decision making. Those 50% need a solution.

The Solution

Hackuity integrates your ecosystem to help cybersec teams focus on what's actually vulnerable – not on managing Excel spreadsheets. Our platform breaks security silos and provides a unified view of your cyber exposure specific to your attack surface. Hackuity is your VOC enabler.

Key Benefits

280% reduction of at-risks assets

100% of vulnerabilities centralized & harmonized

96% reduction in CVSS noise

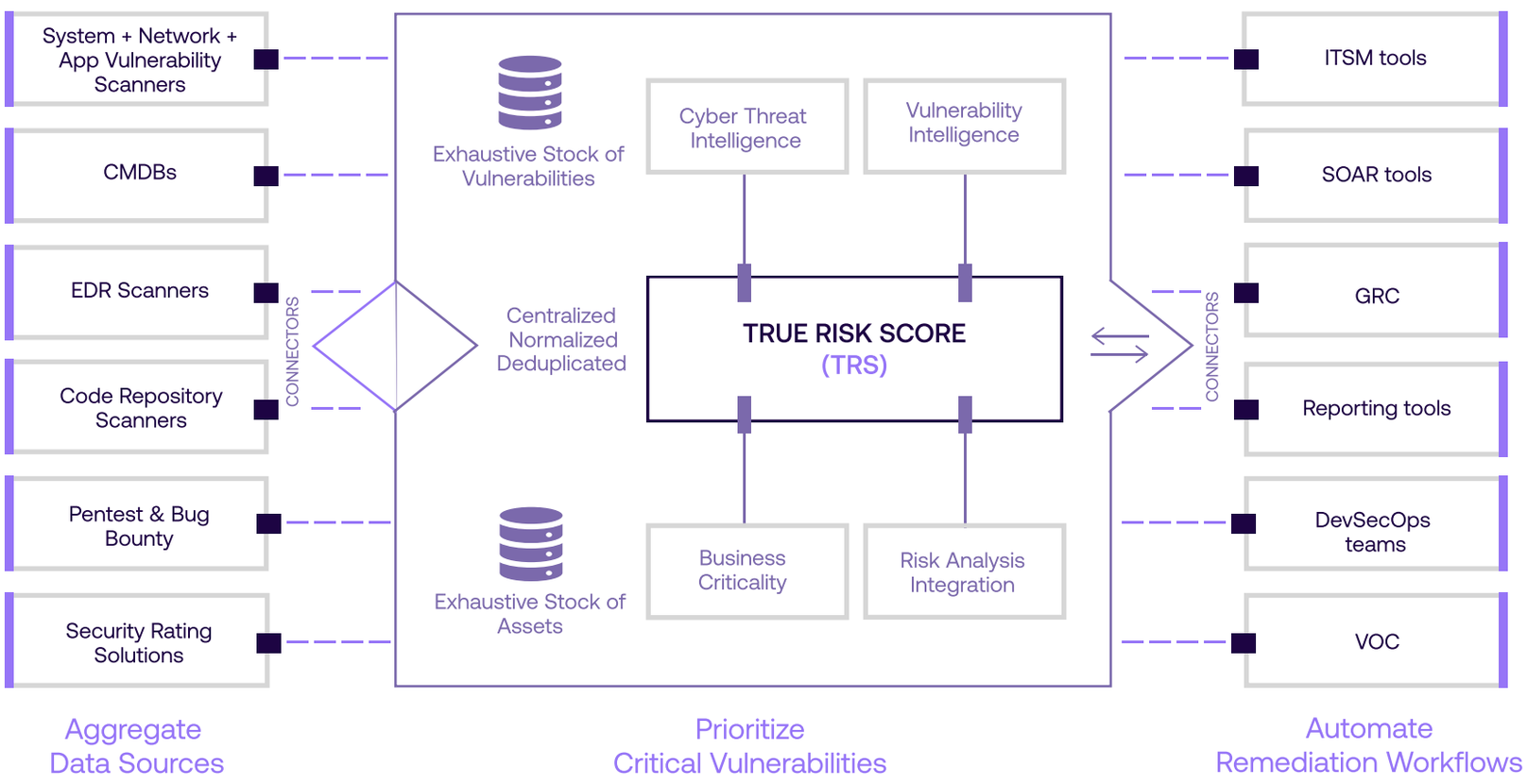
70% end-to-end automation of VM operations

as little as

2

days to deploy

How it works



Certification SOC II

Accreditation IMDA

DEPLOYMENT

Cloud — On Prem — Hybrid

CONNECTORS

70+

SCAN

Aggregate

70+ market-leading tools into one unified platform

Hackuity gives you a unified assessment interface of your entire asset and vulnerability stock from secure API-driven collection and manual file upload. Hackuity is *not* a scanner (but it does make yours more powerful).

+ Unify and normalize varied vulnerability and asset data sourced from different vendor tools, forming a searchable dataset

+ Identify findings based on vulnerability family, attributes, and location

+ Deduplicate vulnerabilities from multiple sources, saving valuable analyst time

+ Collaborate from a dedicated interface that standardizes and digitizes audits executed by internal/ external pentesters in a consistent framework

Prioritize

200,000+ CVEs with our risk-based scoring algorithm

At the core of Hackuity is proprietary risk prioritization technology that combines threat intelligence, vulnerability severity, and your unique business context. Focus remediation efforts on the vulnerabilities that pose the highest risk to *your* attack surface.

+ Proprietary vulnerability prioritization technology (True Risk Score) with direct integration of our CTI data reported by Hackuity Threat Bots

+ Cross-reference of vulnerabilities based on the exploitation of data in CPE (Common Platform Enumeration) format

+ Contextual KPIs (real exploitability, exploit maturity, threat intensity, EPSS) for each CVE providing improved granularity and in-context risk assessment that complies with and goes beyond CVSS

+ Per-asset analysis based on risk exposure, protection measures employed, in-context KPIs, and the full history of the asset security posture

+ Complete Vulnerability Intelligence with Smart Exposure Explorer (SmartEx^2), the deepest encyclopedia of CVEs to date, analyzing open-source and non-public information

+ Hackuity Threat Bots can be leveraged for both your vulnerabilities and your findings

Automate

your cyber team workflows to reduce remediation time

Hackuity's platform streamlines your team operations, reduces remediation time, and breaks silos between analysts, security teams, and production/DevOps teams.

+ Custom dashboards in a single shared repository, unifying all continuous security assessments on your Perimeters

+ Integration with leading ITSM ticketing systems offering bidirectional feedback, automating vulnerability status in an easy-to-understand format

+ Visualization of your Perimeters (group of assets) through an intuitive graphical model to assess and benchmark associated risks

+ RBAC can be applied to Perimeters (allowing delegation of asset ownership) and to remediation-based campaigns

+ Rule-based Playbooks to automate VM operations (ex: ticket creation on Jira, risk scoring of certain assets and vulnerabilities...)

+ Remediation Groups to track progress of the action plans related to findings that share common criteria estate-wide (ex. criticality, remediation...)

What it means for you

CISO / CIO / Head of IT

Get a unified, enhanced view of your entire cybersecurity ecosystem. Maintain visibility across your IT estate and enable your teams to focus on the most pressing cyber risks (instead of drowning in tedious tasks). Delegate risk management to asset/service owners. Improve time to remediation, meet compliance requirements, break team silos, and improve cyber talent retention. Hackuity deploys swiftly with a clear path to ROI.

Security Team Specialist

Whether you're a SOC manager, vulnerability manager, or security analyst, our risk-based scoring technology helps you focus your remediation efforts where they're needed most. Automating your team workflows allows you to reduce time to remediation and better collaborate with other teams. Additionally, with a comprehensive asset inventory, you gain a clear view of your organization's risk exposure.

DevSecOps Specialist

Our platform streamlines vulnerability management programs. With features like Hackuity's standardized vulnerability database and bidirectional synchronization with ticketing systems, you can improve communication with other teams and prioritize work more effectively. The platform provides deeper insights into CVEs and offers proprietary KPIs for improved granularity and in-context risk assessment.

C-level board member

Providing a comprehensive view of the company's security posture, Hackuity enables you to confidently make informed strategic decisions and risk assessments. By reducing the number of at-risk assets, lowering exposure to cyber risks, and offering credible compliance credentials (SOC 2, IMDA), you can reassure stakeholders about the strength of your cybersecurity defenses and the value of their investment.