RHDVM

GET FULL, EXTENSIVE GOVERNANCE OF THE ENTIRE VULNERABILITY LIFECYCLE

Today's organizations rely increasingly on software solutions and applications to improve their operational efficiency: this results **in a much larger attack surface, which includes an ever-growing number of vulnerabilities**. Vulnerability scanners are very effective at detecting vulnerabilities, but for security teams this means having to deal with countless alerts to check and problems to solve.

But **not all vulnerabilities have the same level of criticality**: complex organizations need to focus their limited efforts and resources on remediating the ones that matter most.

RHD VM SUPPORTS ORGANIZATIONS IN VULNERABILITY MANAGEMENT AND CYBER RISK REDUCTION.

By combining a powerful orchestration and case management engine with market-leading Vulnerability Assessment technologies, RHD VM integrates detection, analysis, prioritization, and remediation of vulnerabilities into a single continuous and uninterrupted process, resulting in more efficient, risk-based vulnerability management.

THE VALUE WE BRING

USE A RISK-BASED APPROACH

Define methods for measuring, monitoring, and reporting the risks to which the organization is exposed.

LEVERAGE AUTOMATION

Reduce manual activities, TCO, and Cyber Exposure through a faster response to vulnerabilities.

ENSURE A CONTINUOUS PROCESS

Increase the overall VM process's effectiveness and efficiency through data-driven workflow automation.

DERIVE VALUE FROM ANALYTICS AND ARTIFICIAL INTELLIGENCE

Improve decision-making based on risk with the support of Analytics and Artificial Intelligence technologies for prioritization

* Source: Gartner Market Guide for Vulnerability Assessment Mitchell Schneider, Craig Lawson, Jonathan Nunez, August 7, 2023.

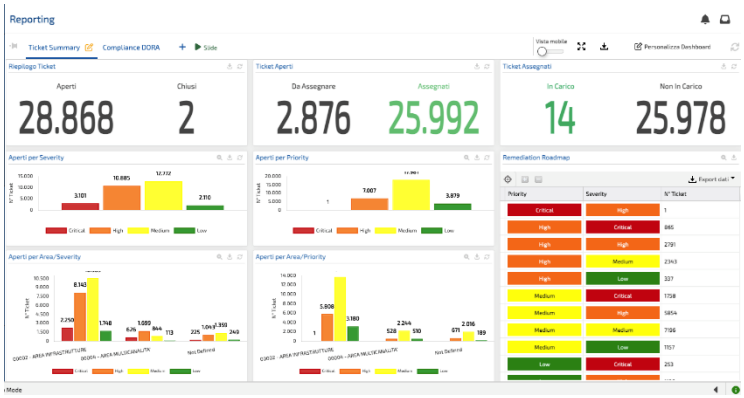
**Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose..

KEY CAPABILITIES

UNIFIED VULNERABILITIES REPOSITORY
Manage all vulnerabilities in a single environment.

RHD VM enables the collection and aggregation of structured and unstructured data from various sources into a unified repository, allowing for:

- analysis, correlation, and aggregation of any type of vulnerability in a single graphical interface.
- sharing information with the right stakeholders and planning remediation.
- defining specific KRIs to determine the company's Security Posture



Native connection to various sources:
VA, DAST, SAST, SCA, manual activities (RED Teaming and PT), market-leading technologies (using off-the-shelf connectors), non-standard tools (using custom connectors).

Advanced data storage and management:
- collection and storage of data from various sources in a single environment.
- structured and NoSQL databases integrated to process Big Data

Data Analysis, Enrichment, and Correlation:
- continuous improvement of KRIs through Business Analytics.
- enrichment, aggregation, and correlation of VA results with non-vulnerability data.
- data-driven workflow management of vulnerabilities.

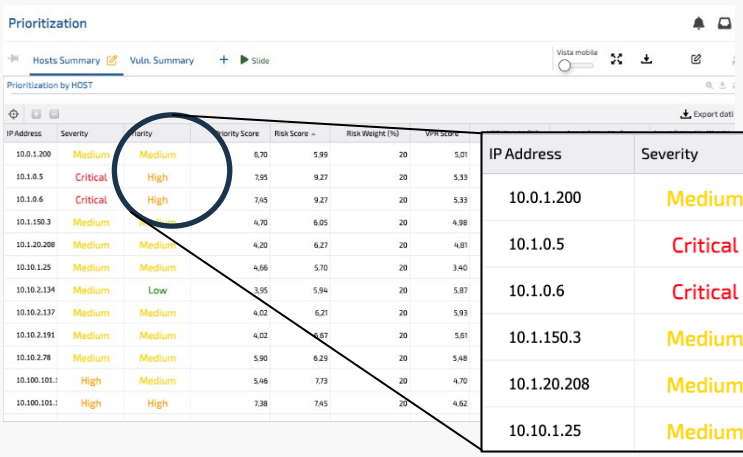
VULNERABILITY PRIORITIZATION
Leverage threat intelligence and business context to define remediation activities

RHD VM provides simple and efficient management of vulnerability prioritization and remediation activities through:

- Enrichment of vulnerability information with Threat Intelligence data.
- Reclassification of vulnerability severity based on their likelihood of exploitation.
- Asset criticality indexes and remediation priority indicators.

Context-based prioritization and remediation:
- Collection of critical asset data.
- Adjustment of the remediation flow based on re-evaluation of priorities.
- KRIs showing security posture and actions to take first.

Vulnerability Intelligence:
- off-the-shelf connectors for multiple Threat Intelligence sources.
- Tenable Lumin connectors for Vulnerability Intelligence provide industry benchmarks and a comparison of KPI effectiveness.
- alerts for matches between an emerging threat model and a known vulnerability.



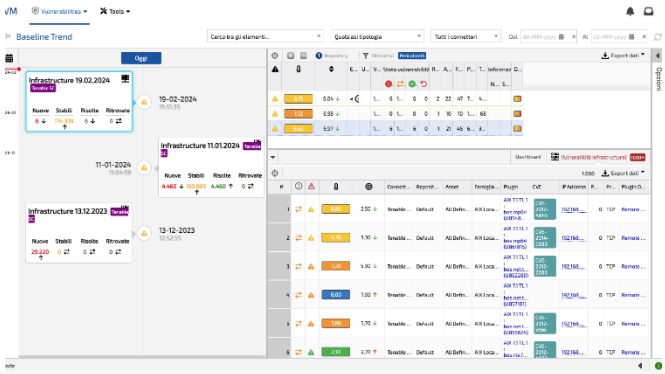
IP Address	Severity	Priority	Priority Score	Risk Score	Risk Weight (%)
10.0.1.200	Medium	Medium	6,70	5,99	20
10.1.0.5	Critical	High	7,95	9,27	20
10.1.0.6	Critical	High	7,45	9,27	20
10.1.150.3	Medium	Medium	4,70	6,05	20
10.1.20.208	Medium	Medium	4,20	6,27	20
10.10.1.25	Medium	Medium	4,66	5,70	20

KEY CAPABILITIES

ASSET CRITICALITY
Identify, manage, and prioritize the most critical assets for your organization.

RHD VM allows for the synchronization and integration of asset management information into the Vulnerability Management process to:

- determine which vulnerabilities should be fixed first.
- know which stakeholders need to act at each stage of the remediation process.
- implement KRIs that correlate vulnerabilities and business information.
- detect malfunctioning hosts and/or unknown assets.
- effectively address multiple compliance requirements (ISO27001, NIST, etc.).



Native connection to asset management tools:

- market-leading technologies (using off-the-shelf connectors) and non-standard tools (using custom connectors).

Enhanced Asset Management Registry:

- setting indicators for the security posture of individual/grouped assets
- identifying any gaps between the known infrastructure and the actual infrastructure;
- tracking the evolution of assets within the organization.

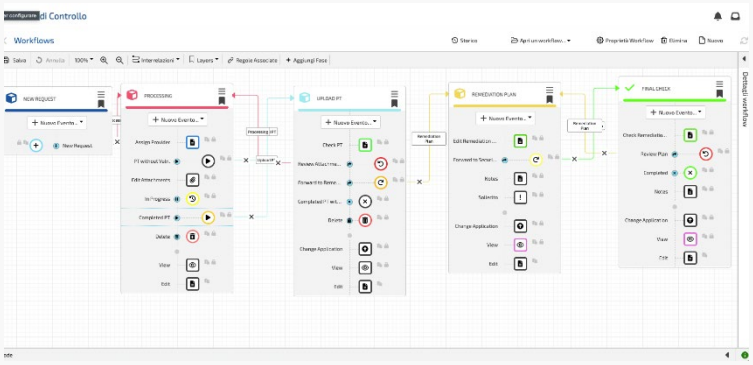
Prioritization of Remediation Activities and Workflow Management:

- defining remediation priorities based on asset criticality;
- involving the appropriate stakeholders for each phase of remediation;
- remediation and/or mitigation of non-functional systems.

VULNERABILITY WORKFLOW GOVERNANCE
Gain full control of the vulnerability management process.

RHD VM provides security teams with the ability to plan and define all stages of the process in line with the organization's needs. This allows:

- stakeholders to manage all vulnerabilities within their scope.
- real-time monitoring of remediation activities and their progress for auditing and performance evaluation purposes.
- the creation of remediation plans that take into account constraints, policies, and exceptions.



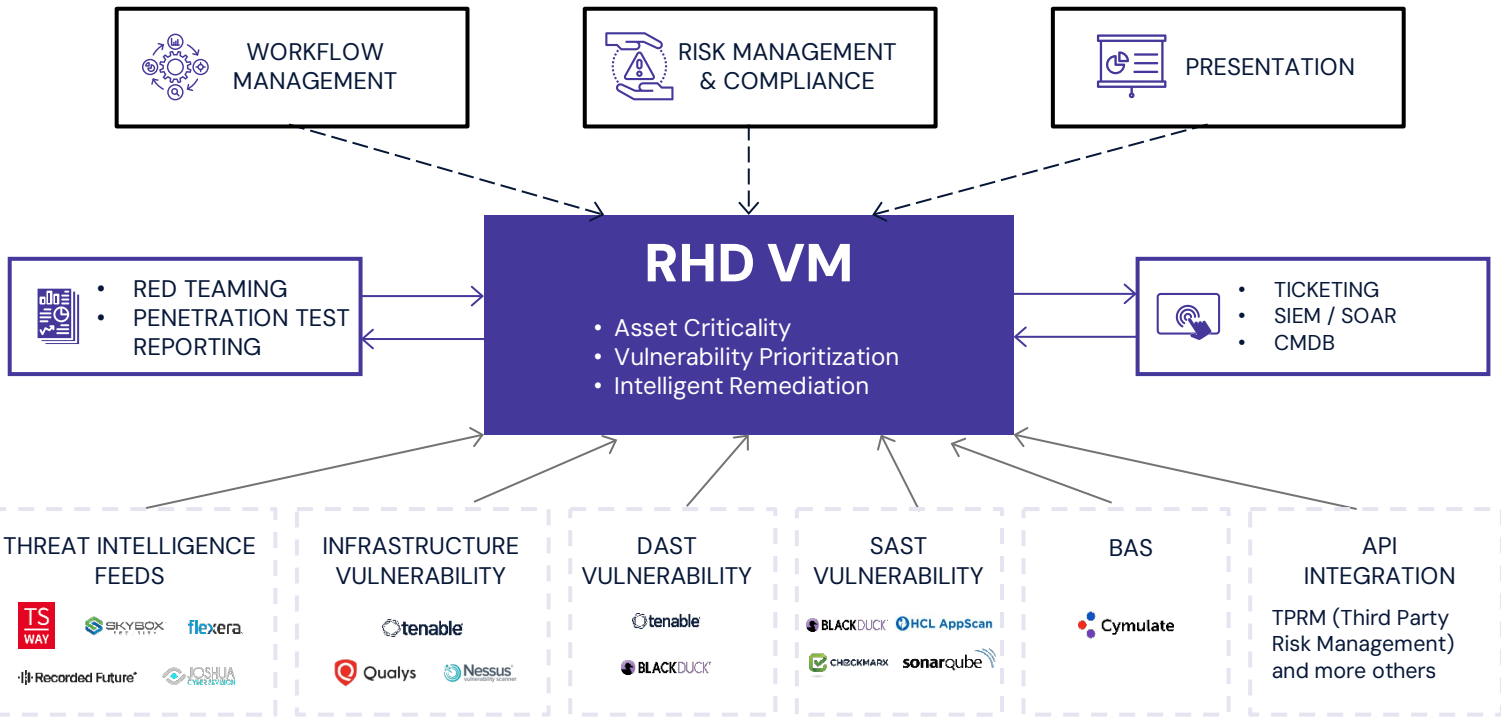
End-to-end governance of continuous threat exposure management:

- 5-phase CTEM (Continuous Threat Exposure Management) process: scoping, discovery, prioritization, validation, mobilization.
- planning, designing, and monitoring the remediation strategy.
- advanced authorization system for team collaboration.
- real-time monitoring of remediation activities for auditing and performance evaluations

Creation and Configuration of Customizable Workflows:

- "low-code" workflow editor for complete customization.
- fully customizable input modules.
- configuration of constraints, policies, and exceptions.
- configuration of authorizations, approvals, escalations, and notifications.
- deployment of single or multiple processes for every type of result

HOW RHD VM WORKS



RHD VM natively integrates with major vulnerability assessment tools, penetration test and red teaming reports, and threat intelligence data.

It uses standard and custom connectors to gather and provide data to other technologies, enriching, correlating, and prioritizing remediation activities for critical assets. Its workflow and risk management engine offers pre-configured processes and a low-code editor to customize them, ensuring full governance of the security posture and risk.

From a single dashboard, you can observe the real-time risk posture. RHD VM can exchange data with external systems like IT Ticketing software, SIEM/SOAR, and CMDB to maximize integration.

RHD VM is the ideal solution for complex organizations and large enterprises that:

- are looking for a collaborative tool for vulnerability management;
- have one or more successfully implemented Vulnerability Scanners and Prioritization Technologies and need to centralize and orchestrate their data;
- need to enrich and correlate asset and vulnerability data from various internal and external sources.
- struggle to prioritize remediation activities based on business risk metrics;
- want to simplify the vulnerability remediation process and reduce manual activities and human intervention;

www.alfagroup.it
info@alfagroup.it
@AlfaGroupIT