SOLUTION COMPARISON BRIEF

Building a More Effective Vulnerability Scanning Program:

Rapid7 InsightVM vs. Tenable.io VM

These days, every vulnerability management tool claims to do a good job of finding vulnerabilities. We believe that's the easy part: It's how you use the data that matters. Rapid7 InsightVM enables customers to scan millions of assets, and makes it easy for organizations of all sizes to take discovered vulnerabilities, prioritize those that need to be fixed first, and assign remediation to the proper parties.

Rapid7 and Tenable both launched cloud platform-powered vulnerability management products in 2017. However, differences in our launch strategies have lead to significant disparities between InsightVM and Tenable.io VM:

- Tenable.io VM was originally the rebrand of Nessus Cloud Manager, and had significant features missing at launch that were standard in Security Center Continuous View.
- In contrast, InsightVM launched with all the capabilities of Nexpose Enterprise, plus additional features like live dashboards and agents. Thus, we have been able to invest in innovative new capabilities, such as remediation workflow, to help customers assess their modern networks instead of just playing catch-up.
- Want to dive deeper into the the various new additions to InsightVM in the first year alone? Read more about InsightVM's Collect, Prioritize, and Remediate capabilities.

Not all "platforms" are created equal. While Tenable's platform launched in 2017, the Insight platform has been live since 2015, and leverages the benefits of the cloud for both advanced analytics and data processing.

Some key examples include:

- The ability to process data into live dashboards
- Deeper analysis of vulnerabilities to find most efficient remediation steps
- A unified, lightweight cloud agent that powers continuous monitoring in InsightVM, InsightIDR, and InsightOps
- Threat feed data from Rapid7's Research and Managed Detection and Response teams that correlates to your assets
- Best-of-breed solutions for vulnerability management, SIEM, incident detection and response, application security, and log monitoring

The breakdown below is intended to help you better understand how Rapid7 InsightVM tackles your vulnerability management challenges as compared to Tenable.io VM.

CHALLENGE	How Tenable.io VM Does It	How InsightVM Does It
UNDERSTANDING YOUR CHANGING NETWORK	Nessus Network Monitor (formerly Passive Vulnerability Scanner) requires additional infrastructure to deploy, may contain more false positives (and can't see encrypted traffic), and duplicates your existing IDS. Agents require heavy resources, and act as a local Nessus scanner.	Adaptive Security detects new devices and vulnerabilities as they join the network *without* requiring additional hardware. Lightweight cloud agents feed live information on known and unknown assets into custom dashboards, giving you intuitive tools to assess your environment with minimal deployment and fewer false positives.
ASSESSING MODERN NETWORK DEVICES	Tenable.io VM possesses the ability to scan cloud services and VMware, but there's no direct integration that enables management of new and deleted assets. The agent is difficult to clone and requires additional scripting to call back to the console.	InsightVM's direct integrations with VMWare, AWS, and Azure allow you to automatically discover and scan new devices as they join the network, import tags, and delete old assets as they're spun down. The lightweight Insight Agent can be embedded in any cloud or virtual image, and automatically clones itself to provide continuous monitoring of new assets.
PRIORITIZING VULNERABILITIES	The CVSS-based scoring gives you a "Critical, High, Medium" rating. You're often left with thousands of "critical" vulnerabilities and little guidance on which ones to start with. The platform includes available exploits, but has no algorithm that factors them into risk scoring.	Our Real Risk score considers CVSS scoring, malware exposure, exploit availability, and age to calculate risk on a granular 1-1000 scale. Some Tenable customers save 40+ man hours per week prioritizing results after switching to InsightVM.
LEVERAGING THREAT INTELLIGENCE AND EXPLOITABILITY INFORMATION	In Tenable.io VM, there's no way of testing which vulnerabilities can be actively exploited nor a way to use the vulnerability data for prioritization and remediation planning. Furthermore, there are no threat feeds showing vulnerabilities being actively exploited in the wild.	In combination with Metasploit, InsightVM lets you validate which vulnerabilities can be exploited live, thus helping you focus on the assets most open to attack and ensure implemented controls are working correctly. Live, integrated threat feeds informed by public and proprietary research are automatically correlated to your assets—all at no additional cost.
PRIORITIZING CRITICAL ASSETS	Prioritization in Tenable.io VM entails manual tagging of assets by filters like "OS," and automatic tagging of assets as they're assessed is highly limited. Additionally, there is no ability to automatically prioritize critical assets by tagging them as such.	Tag assets that are more important than others to amplify their risk score, and they will automatically filter to the top of remediation reporting. You can then create and monitor remediation tasks within InsightVM to gain visibility into what's actually being fixed.
INTEGRATING THE REMEDIATION PROCESS	There is no way to track remediation natively in Tenable.io VM, with the exception of an integration with the ServiceNow Security Operations Vulnerability Management module that comes at an additional cost. Remediation advice is based on fixing individual tickets, not a long-term strategy.	Remediation Workflows let you assign and track remediation from within InsightVM, giving live visibility into progress even across teams. Remediation advice is based on strategic planning of remediation projects. Two-way integrations with Jira, ServiceNow ITSM, and ServiceNow Security Operations are available at no additional cost to easily fold remediation into your IT team's existing workflows.
PLANNING REMEDIATION	Remediation plans are filled with "informational" vulnerabilities and often lack clear, step-by-step instructions or links to patches.	Remediation plans focus on the individual actions that reduce the most risk, such as a single patch that fixes a dozen vulnerabilities. The plans are delivered in simple language with everything you need to apply the fix.

CHALLENGE	How Tenable.io VM Does It	How InsightVM Does It
ASSESSING CONTAINERS	Container assessment comes at an additional cost. You can assess container images for vulnerabilities, but Tenable.io VM can't correlate deployed assets to containers.	Container image assessment is included at no additional cost; deployed containers are automatically correlated to assets to identify container hosts, so you can secure hosts as well as the containers themselves.
MANAGING VULNERABILITY EXCEPTIONS	There is no built-in way to manage exceptions for vulnerabilities that can't be fixed.	InsightVM features a robust vulnerability exceptions manager that allows you to create exceptions across individual assets or groups, provide this reasoning to auditors, and establish expiration dates when remediation can be revisited.

Key InsightVM Strengths	Tenable.io VM	InsightVM
Setup & Management		
Lightweight agent footprint		✓
Agent-based scanning	✓	✓
Agent-less scanning	✓	✓
Scalable to millions of assets	✓	✓
Automated actions/Event-driven scans (Infoblox, Azure, VMware, Sonar, and more)		✓
Vulnerability exception workflow		✓
30+ supported integrations		✓
Container host identification	✓	✓
Container registry integration and image assessment	✓ (Additional cost)	✓
Customizable role-based access control		✓
Risk Prioritization		
Advanced risk scoring and contextualization		✓
Metasploit validation and prioritization		✓
Reporting & Remediation		
In-product integrations with Jira and ServiceNow ITSM		✓
In-product integration with ServiceNow Security Operations	✓ (Additional cost)	✓
Remediation workflow and planning		✓
Compliance		
Templates (CIS, DISA, PCI, Audit, and more)	✓	✓
Customizable role-based access control		✓
Policy editor within UI		✓

READY TO EXPLORE INSIGHTVM FOR YOURSELF? Visit www.rapid7.com/try/insightvm to start your free trial.