RAPID7

SOLUTION COMPARISON BRIEF

Building a More Effective Vulnerability Scanning Program:

Rapid7 InsightVM Enterprise vs. Tenable SecurityCenter Continuous View

These days, every vulnerability management tool does a good job of finding vulnerabilities; it's how you use that data that matters. Rapid7 InsightVM is used by customers to scan millions of assets, and it focuses on making it easy for organizations big and small to take the vulnerability results they find and quickly figure out what needs to be fixed first, and by whom.

The breakdown below is intended to help you better understand how InsightVM tackles your vulnerability management challenges compared to Tenable SCCV. For additional questions, please contact your Rapid7 Account Executive.

CHALLENGE	HOW TENABLE SCCV DOES IT	HOW INSIGHTVM DOES IT
Collecting information and gaining visibility into program success	Many pre-built dashboards that require deployment of additional software (LCE), which are difficult to customize and take ~15 minutes to refresh. A multi-step process to create filters and apply them to dashboards.	Liveboards that update as soon as InsightVM gets new information and are fully customizable, allowing you to create dashboards for any user, as well as easily query your vulnerability and asset data.
	Passive Vulnerability Scanner (PVS), which requires additional infrastructure to deploy, contains many 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 lets you detect 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 few false positives.
	Ability to scan cloud services and VMWare, but no direct integration to manage new and deleted assets. Agent difficult to clone and requires additional scripting to call back to console.	Direct integrations with VMWare, AWS, and Azure enables InsightVM to automatically discover and scan new devices as they join the network, import tags, and delete old assets as they're spun down. Lightweight agent can be embedded in any cloud or virtual image and automatically clones itself to provide continuous monitoring on new assets.

CHALLENGE	HOW TENABLE SCCV DOES IT	HOW INSIGHTVM DOES IT
Prioritizing what's important to your business	CVSS-based scoring gives you a "Critical, High, Medium" rating. Often left with thousands of "Critical" vulnerabilities and no guidance on which ones to start with. Includes available exploits, but no algorithm that factors them into risk score. No threat feeds showing vulnerabilities actively being exploited in the wild.	Risk Score is calculated using malware exposure, exploit availability, and age to give you a granular 1-1000 scale. Some Tenable customers save 40+ man hours per week on prioritizing results after switching to InsightVM. Threat feeds from Rapid7 research and public sources automatically correlate to vulnerabilities found in your environment, letting you easily prioritize your riskiest assets.
	No way of testing which vulnerabilities can be actively exploited, and no way to use the vulnerability data for prioritization and remediation planning.	Integration with Metasploit lets you validate which vulnerabilities can be exploited live, helping you focus on the assets most open to attack and helping you ensure controls you've put in place are working correctly.
	No automated way of testing which vulnerabilities can be actively exploited, and no way to use the exploited vulnerability data for prioritization and remediation planning.	Tag assets that are more important than others to amplify their risk score, and they will automatically filter to the top of remediation reporting. Create and monitor remediation tasks from within InsightVM to gain visibility into what's actually being fixed.
Streamlining remediation	Several integrations with ticketing vendors, but no way to track remediation natively in Security Center. Remediation advice is based on fixing individual tickets, not strategic view.	Remediation Workflows let you assign and track remediation from within InsightVM, ensuring you understand your progress in between scheduled scans. Remediation advice is based on strategic planning of remediation projects. Two-way integration with JIRA and ServiceNow to easily fold remediation into your IT team's existing workflows.
	Remediation plans filled with "informational" vulnerabilities and often lacking clear step-by-step instructions/ links to patches.	Remediation plans focused on which individual actions reduce the most risk, in simple language with everything you need to apply the fix.

InsightVM excels in the areas that are most important to your vulnerability management program:
easy setup and management, risk prioritization, reporting, remediation, and support for your compliance efforts.

KEY INSIGHTVM STRENGTHS	TENABLE SCCV	RAPID7
Setup & Management		
Agent-based and Agent-less Scanning	✓	✓
Scalable to Millions	✓	✓
Automated Actions / Event-driven Scans (Infoblox, AWS, Sonar, and more)		✓
Intuitive Vulnerability Exception Workflow		✓
50+ Supported Integrations		✓
Risk Prioritization		
Advanced Risk Scoring and Contextualization		✓
Metasploit Validation and Prioritization		✓
Reporting & Remediation		
Custom Reporting	✓	✓
Real-time Customizable Dashboards		✓
Continuous Live Monitoring		✓
Remediation Workflow and Planning		✓
Query Vulnerability Data Live		✓
Compliance		
Templates (CIS, DISA, PCI, Audit, and more)	✓	✓
Policy Editor within UI		✓

SEE THE BENEFITS OF INSIGHTVM FOR YOURSELF.
CONTACT US TO REQUEST A DEMO TODAY:

+1–866–7RAPID7 (Toll Free)

+1–617–247–1717

sales@rapid7.com
www.rapid7.com/insightVM