Tenable vs. Qualys vs. Rapid7: The Vulnerability Management Verdict

Unvarnished Reviews Research

This report synthesizes data from 2,500+ verified user reviews and practitioner community posts collected from G2, Capterra, TrustRadius, PeerSpot, Spiceworks, Reddit r/netsec and r/sysadmin, and Stack Overflow. Pricing data reflects vendor pricing pages, CostBench transaction data, Vendr benchmark data, and independent procurement analysis current as of June 2026. Full research methodology at unvarnishedreviews.com/methodology. Research Notes available on request at editorial@unvarnishedreviews.com.

The Verdict Up Front

Tenable is the market leader in vulnerability management, with the largest plugin library available (319,000+ plugins covering 116,000+ CVEs as of March 2026), the deepest OT/ICS coverage in the category, and the most mature ServiceNow integration for enterprise ITSM-driven remediation workflows. It is also the most expensive of the three at enterprise scale and requires the most operational investment to run effectively. Tenable Security Center on-premises requires infrastructure investment and at least 0.5 FTE to operate.

Qualys VMDR is the compliance and cloud-scale platform, built for organizations where audit-ready reporting, continuous cloud scanning, and patch management from a single console are the primary requirements. Its per-asset pricing starts higher than Rapid7's, its modular structure creates licensing complexity, and its 2025 outage history introduces reliability questions not present in the other two platforms.

Rapid7 InsightVM is the most transparent on pricing, the most developer-friendly for Jira-integrated remediation workflows, and the most accessible for organizations without large dedicated security operations teams. It also carries the most documented hidden costs of the three, 10 versus Qualys's 4, despite its reputation for pricing transparency. The headline per-asset price is real; what accumulates around it is not always disclosed upfront.

The vulnerability management market is also being reshaped by a fourth option that belongs in every 2026 evaluation: **Microsoft Defender Vulnerability Management**, included in M365 E5 at zero incremental cost. For organizations already on E5, the burden of proof is on all three independent platforms to justify incremental spend.

Platform Ratings at a Glance

Platform	G2	PeerSpot	Primary Strength
Tenable Vulnerability Management	4.5 / 5	Strong	Coverage depth, OT/ICS, ServiceNow
Qualys VMDR	4.3 / 5	Strong	Compliance reporting, cloud scale
Rapid7 InsightVM	4.3 / 5	Strong	Pricing transparency, Jira integration, usability

All three platforms cluster in the 4.3-4.5 range on G2, reflecting genuine capability from all three vendors. The meaningful differentiation is in use case fit, pricing architecture, and operational requirements, not aggregate satisfaction scores.

The Product Landscape: What You're Actually Evaluating

Each vendor sells multiple vulnerability management products. Choosing the wrong product within a vendor's lineup is as common a mistake as choosing the wrong vendor.

Tenable

- **Tenable Nessus Professional**, standalone scanner, point-in-time results only. No remediation tracking, no continuous monitoring, no asset criticality scoring. Not a vulnerability management program. Commonly purchased by mistake by organizations that need a VM program.
- **Tenable Vulnerability Management (cloud)**, cloud-delivered continuous VM with the full plugin library, risk-based prioritization, and asset management. The standard enterprise choice.
- **Tenable Security Center (on-premises)**, on-premises VM platform for organizations with air-gapped environments or data sovereignty requirements. Requires infrastructure investment and dedicated FTE to operate.
- **Tenable One**, unified exposure management platform aggregating VM, web application scanning, cloud security, identity exposure, and attack path analysis. Tenable's CTEM play. Meaningfully more expensive than standalone VM.

Qualys

- **Qualys VMDR**, flagship VM platform with integrated patch management and threat intelligence. Cloud-delivered, agent-based, covering on-premises, cloud, and virtual assets.
- **Qualys WAS**, web application scanning, separate product and separate license from VMDR.
- **Qualys TotalCloud**, cloud security posture management, separate license.
- **Qualys ETM (Enterprise TruRisk Management)**, unified exposure management, Qualys's CTEM equivalent.

Rapid7

- **Nexpose**, legacy on-premises scanner. Still sold and supported but Rapid7 is actively steering customers toward InsightVM.
- **Rapid7 InsightVM**, cloud-managed VM platform using the Insight Agent (same binary as InsightIDR). Real Risk Score backed by live Metasploit exploit data. The current enterprise standard.
- **Rapid7 Command Platform**, unified exposure management aggregating InsightVM, InsightCloudSec, InsightAppSec, and threat intelligence. Rapid7's CTEM play.

The Critical Differentiator: Plugin Coverage

This is where Tenable has maintained its lead for two decades, and where the gap is most meaningful for complex enterprise environments.

Tenable Research has published 319,000+ plugins covering over 116,000 CVEs as of March 2026. The practical implication: in heterogeneous enterprise environments with legacy systems, uncommon network devices, and OT/ICS assets alongside standard endpoints, coverage gaps are breach risk. Tenable's plugin depth is not marketing, it is the specific reason that organizations running complex infrastructure consistently choose Tenable despite its premium price.

For environments running purely standard IT assets, Windows, Linux, cloud workloads, containers, the practical difference between the three platforms is small. For anything more complex, the coverage gap becomes material.

Qualys and Rapid7 both maintain large plugin libraries, but neither publishes precise numbers the way Tenable does. Independent practitioners specifically note: Tenable's single-sensor installation process on various operating systems is smooth, unlike Rapid7, which requires different versions for separate systems.

What Users Actually Report

Tenable: What Works

PeerSpot and G2 reviewers consistently identify three strengths: coverage depth, reporting quality, and ServiceNow integration. Tenable is user-friendly and excels in reporting, allowing users to easily fetch and schedule reports, with the software's discovery feature aiding in strengthening security posture.

The ServiceNow integration is specifically called out as the most mature bidirectional connector of the three, Tenable's Security Center integration with ServiceNow Vulnerability Response is well-documented, widely deployed, and actively maintained. For enterprises running ITSM-driven remediation workflows, this depth is a genuine differentiator.

Tenable's Vulnerability Priority Rating (VPR) system, using real-world threat data and machine learning for prioritization beyond CVSS scores, is praised for reducing alert fatigue. One PeerSpot reviewer documents approximately 87% reduction in the number of vulnerabilities requiring urgent remediation, specifically in the number of criticals, the clearest quantified ROI finding in this comparison.

Tenable: What Doesn't Work

Implementation complexity for Security Center. On-premises Tenable Security Center requires infrastructure investment and at least 0.5 FTE to operate effectively. PeerSpot reviewers specifically note that "a long implementation" is the primary area for improvement, and that the operational burden is higher than cloud-native alternatives.

Pricing at enterprise scale. Tenable VM runs $26-$38 per asset per year at enterprise scale. For organizations with large asset counts, Tenable One with full module coverage is "paying a materially different number" than standalone VM licensing, a modular pricing pattern that produces renewal surprises.

OT/ICS value only for relevant environments. Tenable's deepest differentiator, OT/ICS coverage through Tenable OT Security, is only relevant for manufacturing, utilities, and industrial environments. Organizations without OT assets are paying for coverage depth they cannot use.

Qualys VMDR: What Works

G2 and PeerSpot reviewers consistently praise three areas: cloud-scale scanning architecture, integrated patch management, and compliance reporting.

Qualys is the only platform of the three with patch management integrated into the base VMDR license, eliminating a separate tool and workflow for organizations where patch execution is the primary remediation mechanism. For compliance-driven organizations (PCI-DSS, HIPAA, FedRAMP), Qualys's audit-ready reporting templates are

specifically called out as the most mature of the three.

The cloud architecture, no on-premises scanner appliances required for standard deployments, reduces infrastructure overhead versus Tenable Security Center. Global Asset View provides a unified asset inventory across cloud, on-premises, and virtual environments that practitioners describe as genuinely comprehensive.

Qualys VMDR: What Doesn't Work

2025 outage history. During 2025, Qualys experienced outages a couple of times, with issues receiving timely root cause analysis deliveries. For a cloud-delivered security platform where continuous scanning is the core value proposition, availability issues are a meaningful concern. Neither Tenable nor Rapid7 has equivalent documented outage patterns in 2025.

Licensing complexity. Qualys is powerful and scalable, but not "set-and-forget." Organizations get deep capabilities, but also more complexity, licensing overhead, and the odd operational surprise. WAS, TotalCloud, and ETM are each separate licenses. The modular structure that makes Qualys flexible also makes its true cost difficult to model at procurement time.

Query building limitations. PeerSpot practitioners specifically document that queries lack grouping operators in Qualys VMDR, a specific operational limitation for security teams that rely on complex asset group queries for prioritization.

MSP pricing structure. Reddit practitioners document that Qualys is not set up for MSPs, expecting payment per client individually, which is a nightmare to manage.

Rapid7 InsightVM: What Works

TrustRadius and G2 reviewers consistently identify three strengths: visual dashboards and reporting, Jira integration for developer-led remediation, and pricing transparency.

InsightVM is rated 4.3/5 on G2 from over 800 reviews. Customers appreciate the visual dashboards and extensive integrations. The live dashboard approach, showing risk in real time as assets change rather than as a point-in-time scan result, is specifically praised for making vulnerability data actionable without requiring security analyst interpretation.

Rapid7's Jira integration is the strongest of the three for engineering-led remediation workflows. Rapid7's heritage in the developer security space gives InsightVM's Jira connector a purpose-built architecture rather than an ITSM-first adapter. For organizations where development teams own remediation, this workflow fit is operationally significant.

Unlike Qualys, which charges per scanner deployment, Rapid7 InsightVM does not charge additional fees for deploying multiple scan engines, a specific cost advantage for distributed environments requiring multiple scanning points.

Rapid7 InsightVM: What Doesn't Work

10 documented hidden costs. Rapid7 InsightVM has 10 documented hidden costs versus Qualys VMDR's 4, a striking finding given Rapid7's reputation for pricing transparency. The headline per-asset price is genuine; what accumulates around it includes professional services, additional modules, and integration costs that are not visible at the list price level.

Learning curve for advanced features. Users highlight challenges such as a steep learning curve, inconsistent scan performance, and limited context-aware remediation guidance for advanced InsightVM configurations. The platform is

more accessible than Tenable for initial deployment but reaches its own complexity ceiling for teams attempting advanced customization.

Scan performance at scale. PeerSpot and G2 practitioners consistently flag scan performance issues in very large-scale setups, specifically, scan times extending significantly beyond expectations for environments with 50,000+ assets.

Pricing Reality (June 2026)

Published Per-Asset Pricing

Platform	Per-Asset/Year	Notes
Tenable VM (cloud)	$26-$38	Enterprise scale; Tenable One significantly higher
Qualys VMDR	$17-$33	Patch management included; WAS/TotalCloud separate
Rapid7 InsightVM	$25-$35	Most transparent published pricing

These ranges obscure more than they reveal. Web application scanning, container scanning, EASM, and CTEM modules each add meaningfully to the base cost.

The Hidden Cost Architecture

Tenable: Nessus Professional ($3,990/year) is not a VM program, organizations that purchase it expecting enterprise VM capabilities are buying the wrong product. Tenable One pricing is materially higher than standalone VM. Security Center on-premises adds infrastructure and FTE costs.

Qualys: VMDR starts at $199-$250 per asset per year, WAS starts at $1,995 per year for 25 applications, and Patch Management adds approximately $30 per asset per year on top of VMDR. Third-party integration fees in ETM run 10%-15% of license costs according to Reddit practitioners.

Rapid7: Standard 3% annual price increases are documented in contract terms. Rapid7's bundled pricing can be more cost-effective than purchasing multiple Qualys modules separately, but the 10 documented hidden costs require explicit line-item verification before signing.

Negotiation Leverage

Vendr transaction data shows buyers who compared multiple vendors and negotiated competitively achieved 20%-35% lower pricing than those who negotiated with a single vendor. The specific lever: Qualys pricing is strict until they're about to lose a deal, getting quotes from Tenable and Rapid7 creates competitive pressure. The same principle applies to all three, a credible competitive evaluation is the most powerful negotiating tool available.

The Microsoft Factor

Microsoft Defender Vulnerability Management, included in M365 E5 at zero incremental cost, is the fourth option every 2026 evaluation must address. For organizations on E5, Defender VM covers endpoints natively with no additional per-asset cost. Its coverage for non-Windows assets, network devices, and OT environments is less mature than Tenable, but for predominantly Windows endpoint environments on E5, the incremental cost justification for any independent VM platform requires explicit documentation.

The Decision Framework

Choose Tenable if:

- Your environment includes OT/ICS assets, legacy systems, or uncommon network devices requiring maximum plugin coverage
- ServiceNow is your ITSM platform and bidirectional vulnerability-to-ticket integration is a core workflow requirement
- You have dedicated security operations staff (0.5+ FTE) to operate the platform effectively
- Compliance frameworks requiring deep vulnerability evidence documentation (NERC CIP, ICS-CERT) are mandatory
- Budget is secondary to coverage depth and you have modeled Tenable One vs. standalone VM costs before signing

Choose Qualys VMDR if:

- Compliance reporting, PCI-DSS, HIPAA, FedRAMP, SOC 2, is your primary vulnerability management driver
- Integrated patch management from a single console is a requirement
- Your environment is heavily cloud-based and agent-based scanning without on-premises infrastructure is preferred
- You have verified the 2025 outage history with Qualys and received documented SLA commitments for your contract
- You are not an MSP, Qualys's per-client pricing structure is documented as problematic for managed service providers

Choose Rapid7 InsightVM if:

- Developer-led remediation through Jira integration is central to your remediation workflow
- Your security team is small and needs the most accessible platform for initial deployment and ongoing operation
- Pricing transparency at the headline level matters, and you have explicitly verified all 10 documented hidden costs before signing
- Your environment is predominantly standard IT assets where Tenable's coverage depth premium is not justified
- You need the strongest integration with the broader Rapid7 platform (InsightIDR, InsightAppSec) for a unified security operations view

The pre-signing checklist for all three:

1. Define your asset scope precisely, per-asset pricing means scope creep is billing creep

2. Map every module you need against the base license, WAS, cloud, container, OT, EASM, and CTEM are separate line items for all three

3. Get a competitive quote from all three before negotiating any single vendor, Vendr data confirms 20%-35% savings for competitive buyers

4. Verify Microsoft Defender VM coverage against your specific environment before assuming independent VM is necessary

5. Request documented SLA commitments and historical uptime data, Qualys's 2025 outage history makes this step non-optional

The Bottom Line

Tenable, Qualys, and Rapid7 are all enterprise-grade vulnerability management platforms. The right choice is not about which is technically superior in the abstract, it is about which fits your environment's complexity, your team's operational capacity, your primary use case, and your honest TCO.

Tenable wins on coverage depth, OT/ICS capability, and ServiceNow integration. It demands the most operational investment and carries the highest per-asset cost. The 87% reduction in critical vulnerabilities documented by PeerSpot practitioners is the clearest ROI signal in the category, for organizations that resource it properly.

Qualys wins on compliance reporting, integrated patch management, and cloud-scale architecture. Its 2025 outage history, licensing complexity, and MSP-unfriendly pricing are documented liabilities that require explicit due diligence before signing.

Rapid7 wins on pricing accessibility, developer workflow integration, and platform usability for smaller security teams. Its 10 documented hidden costs, the most of the three despite its transparency reputation, require explicit line-item verification before the headline per-asset price becomes the actual contract price.

The universal recommendation: run a proof-of-concept against your actual asset inventory before signing any contract. All three vendors offer trial access. The platform that performs against your specific environment, integrates with your existing ITSM and ticketing workflows, and fits your team's operational capacity is the right one, regardless of how it performs in this comparison.

Editorial Correction Policy: If you believe a finding in our research is factually inaccurate, contact editorial@unvarnishedreviews.com with the specific claim and supporting documentation. We review all correction requests and will promptly update any findings that are found to be inaccurate.
