

UNVARNISHED REVIEWS

Veeam vs. Rubrik vs. Commvault: The Ransomware Recovery Reckoning

Unvarnished Reviews Research

Market Position: Backup Stopped Being a Checkbox

Enterprise backup used to be an IT line item, buy a tool, schedule the jobs, confirm the restores work during an annual drill. Ransomware changed that calculus permanently. Cyber-insurance underwriters increasingly require immutable, air-gapped backup as a condition of coverage, and attackers now target backup infrastructure first, encrypting or deleting backups before encrypting production data, so that paying the ransom becomes the only path to recovery. Veeam, Rubrik, and Commvault are the three names most consistently compared in enterprise backup evaluations in 2026, and each has staked out a different position on the ransomware-resilience spectrum: Veeam on breadth and virtualization heritage, Rubrik on security-first, cyber-resilience architecture, and Commvault on the broadest workload coverage in a single platform.

That ransomware-resilience positioning is exactly why the March 2026 Veeam vulnerability disclosure matters as more than routine patch news. Backup servers are a uniquely high-value target: compromise one, and an attacker doesn't just encrypt production data, they can disable or corrupt the recovery path itself. Veeam's advisory acknowledged this risk, warning that once a vulnerability and its patch are disclosed, attackers will likely reverse-engineer the fix to target unpatched deployments. Arctic Wolf's independent threat research adds the sharper point: Veeam Backup & Replication has already been documented as a target in real ransomware campaigns, with Akira and Fog ransomware actors extracting sensitive information from Veeam deployments.

Rubrik and Commvault were not implicated in this specific disclosure. That is a fact about this particular vulnerability cluster, not a permanent security ranking, every vendor in this category has had vulnerabilities disclosed at some point, and the right response for any buyer is a patching and access-control discipline, not vendor loyalty based on one disclosure cycle.

Veeam: The Upside

Veeam's virtualization heritage and broad platform support remain the deepest in this comparison, and its free Community Edition is the only zero-cost entry point among the three. The Veeam Universal License (VUL) covers any combination of VM, physical, cloud, and SaaS workloads under one portable, per-workload license, and the free Community Edition covers up to 10 workloads with no time limit, letting a team pilot the platform without a sales conversation.

Users rate Veeam 4.6/5 across a large, well-populated review base of roughly 700 to nearly 2,000 reviews depending on the listing, consistently the largest review population of the three platforms in this comparison. Reviewers consistently praise reliability and fast recovery, and Veeam's AI-powered malware and anomaly detection, YARA and indicator-of-compromise (IOC) threat scanning, and cleanroom-style recovery validation are documented capabilities.

Veeam: The Downside

The March 2026 vulnerability disclosure is the most serious documented issue in this comparison; see the Red Flags section for the full pattern. Veeam's advisory for version 13 lists six CVEs, three rated critical, two of them at CVSS 9.9: one exploitable by any authenticated domain user and one by an account with the Backup Viewer role. Press coverage of the wider March disclosure counted up to four CVSS 9.9 flaws across the version 12 and version 13 branches. The product's purpose is protecting against the attackers most likely to look for exactly this kind of access.

Immutability is not secure by default the way it is with Rubrik, it requires deliberate configuration. Veeam requires teams to set up hardened repositories, configure object lock, or use external immutable storage; a misconfigured deployment can leave backups exposed to the same encryption risk they're meant to prevent.

Multi-product complexity is a documented, recurring complaint, not an edge case. Veeam's six-product portfolio (Backup & Replication, ONE, Recovery Orchestrator, Kasten, and cloud products) is independently described as overwhelming for some teams, especially during upgrades, and pricing is documented as complex and potentially costly at large-scale implementation despite being nominally flexible.

Rubrik: The Upside

Rubrik's Ransomware Recovery Warranty is a distinctive differentiator among the three, with a limit that depends on the size of the environment. Rubrik states that it covers up to \$10 million in recovery incident expenses at no charge, but only for Enterprise Edition or Enterprise Proactive Edition subscribers with at least 250 terabytes of protected data and a Customer Resilience Manager subscription. The payment cap scales with data volume: \$250,000 for 250-500 terabytes, \$500,000 for 500-750 terabytes, \$1 million for 750 terabytes to 5 petabytes, \$5 million for 5-10 petabytes, and \$10 million at 10 petabytes or more. Coverage requires Retention Lock in compliance mode and monthly health checks. The warranty backs Rubrik's zero-trust, immutable-by-default architecture with a financial commitment, a structurally different promise than a features list.

Users rate Rubrik 4.6/5 across roughly 106-782 reviews depending on the listing, matching Veeam's rating despite a shorter track record and a narrower product portfolio. Reviewers consistently praise the intuitive interface and minimal management overhead, and one reviewer rated the initial setup experience "11 out of 10." Independent benchmarking rates Rubrik's scalability at 9 out of 10. Rubrik reported \$1.66 billion in subscription annual recurring revenue as of July 31, 2026, up 33% year over year, a scale indicator for a platform younger than either competitor.

Rubrik: The Downside

Cost and documentation depth are the two most consistent complaints, and they compound each other for complex deployments. Rubrik's reviews consistently praise usability and security architecture, but independent sources are equally consistent that some users are unhappy with cost and under-documentation for advanced features like analytics and threat hunting, which are described as requiring deeper product knowledge than the core backup workflow.

Rubrik sells by quote, though reseller list rates are reported. A competitor-published analysis of a September 2025 reseller price list reports \$130, \$163, and \$228 per usable back-end terabyte per month for the Foundation, Business, and Enterprise editions, with a three-year minimum on most subscriptions. Vendr's page for Rubrik cites an average contract near \$56,588 a year, with the high end near \$160,000, from a handful of deals. Confirm current rates with Rubrik or a reseller during procurement.

Commvault: The Upside

Commvault's workload coverage is the broadest of the three, supporting over 250 workload types from a single console, a real advantage for organizations with a heterogeneous, hybrid environment. Its ransomware-specific tooling layers three distinct capabilities: ThreatWise seeds decoys and canary files to expose attackers during reconnaissance, Cleanroom Recovery validates clean restore points in an isolated cloud environment before restoring to production, and AirGap Protect maintains immutable copies isolated from production.

Users rate Commvault 4.3-4.4/5 across roughly 164-182 reviews on its core listing, with a broader combined figure of 946 reviews across several review sites averaging 4.5/5. Independent benchmarking ranks Commvault fourth in its backup and recovery category with 3.4% category mindshare, narrowly ahead of Rubrik's 3.2%.

Commvault: The Downside

Deployment complexity and a steep learning curve are the most consistent, specific complaints, independently corroborated across multiple review sources. Reviewers describe SQL and Windows Server configuration complexity, and one reviewer's summary is direct: "Commvault Cloud is powerful, but it's still complex to set up and manage." Independent benchmarking rates Commvault's implementation and recovery-runbook maturity at only 3.7 out of 5 noting that initial implementation is not typically lightweight and that recovery readiness still depends heavily on customer discipline, not just the platform's capabilities.

Commvault pricing depends on the licensing basis. A June 2026 analysis of Commvault's published SaaS rates lists Commvault Cloud virtual machines at \$102.49 per 10-VM pack per month (about \$10.25 per VM), file and object from \$58.50 per terabyte per month, and Microsoft 365 from \$1.70 per user per month. Its 2025 US self-managed price list shows about \$98 per VM per year or about \$150 per front-end terabyte per year, with recovery editions higher at about \$224 and \$265 per front-end terabyte. The same analysis notes that published list prices sit above what most deals close at. Get an itemized quote before assuming Commvault's broader workload coverage costs more or less than Veeam's per-workload model.

Platform Ratings at a Glance

Platform	G2 Rating	G2 Reviews	Trustpilot	Note
Veeam Data Platform	4.6 / 5	~700-1,980	No meaningful Trustpilot presence identified	Largest review base of the three; subject of the March 2026 CVSS 9.9 disclosure
Rubrik Security Cloud	4.6 / 5	~106-782	No meaningful Trustpilot presence identified	Warranty with data-volume thresholds; matches Veeam's rating from a shorter track record
Commvault Cloud	4.3-4.4 / 5	~164-182 (946 combined across platforms)	No meaningful Trustpilot presence identified	Broadest workload coverage (250+ types); lowest numeric rating of the three

All three platforms carry strong G2 ratings clustered in a narrow 4.3-4.6 band, a positive signal across the category. The gap is small enough that it should not decide the purchase by itself; the March 2026 vulnerability disclosure, the warranty's data-volume threshold, and documented implementation differences carry more decision-relevant weight than a few tenths of a point.

Pricing (October 2026)

Platform	Entry Tier	Mid Tier	Top Tier	Pricing Model
Veeam	Free Community Edition, up to 10 workloads	Foundation \$1,550 per 10 workloads a year (about \$155 each); Advanced \$1,890 per 10 (about \$189 each)	Premium \$2,275 per 10 workloads a year (about \$227.50 each), adds disaster recovery orchestration	Veeam Universal License, per workload, portable across VM, physical, cloud, and SaaS; Veeam does not publish list prices for most other products, per Vendr; list prices as reported by a third-party tracker in October 2026
Rubrik	Foundation: \$130 per usable back-end terabyte per month (about \$1,560 a year)	Business: \$163 per terabyte per month (about \$1,956 a year)	Enterprise: \$228 per terabyte per month (about \$2,736 a year); warranty eligibility starts at 250 terabytes	Subscription per usable back-end terabyte, three-year minimum on most subscriptions, sold by quote; reseller list rates from a competitor-published analysis
Commvault	Commvault Cloud: VMs about \$10.25 per VM per month; file and object from \$58.50 per terabyte per month	Self-managed: about \$98 per VM per year or about \$150 per front-end terabyte per year	Autonomous Recovery about \$224 and Cyber Recovery about \$265 per front-end terabyte per year; replication and cleanroom features in higher tiers or add-ons	Published SaaS rates by workload; quote-based self-managed licensing; list prices sit above typical closing prices

Vendr purchase data puts the median Veeam buyer at \$8,352 a year across all Veeam products (range \$4,356-\$27,799) and reports typical discounts of 15%-30% off initial Backup & Replication quotes. Vendr lists no median for Commvault. Veeam raised perpetual socket list prices by up to 9% effective July 2026, and a tracker reports renewal increases of 20%-30% in some user accounts. Rubrik and Commvault figures are reseller or third-party list rates, not quotes.

TCO Comparison: 500-Workload Mid-Enterprise Environment, One Year

Scenario: 500 workloads, assumed to hold 100 usable terabytes, at list prices before discounts.

Line Item	Veeam	Rubrik	Commvault
Platform license at list	Foundation $500 \times \$155 = \$77,500$; Advanced $500 \times \$189 = \$94,500$; Premium $500 \times \$227.50 = \$113,750$	Foundation $100 \times \$1,560 = \$156,000$; Business $100 \times \$1,956 = \$195,600$; Enterprise $100 \times \$2,736 = \$273,600$	Self-managed $500 \times \$98 = \$49,000$; Commvault Cloud VMs $500 \times \$10.25 \times 12 = \$61,500$ (entry tier)
Storage and infrastructure	Add 15%-40% of license cost for repositories, per one tracker: \$11,625-\$45,500	Included in subscription model for usable terabytes; cloud storage costs vary	Not itemized in the sources; confirm before comparing
Operational labor (patching, hardening, repository configuration)	Higher: Immutability requires manual configuration	Lower: Immutable-by-default architecture	Moderate to high: documented learning curve
Ransomware financial backstop	No comparable cash warranty identified	Up to \$10 million, but \$250,000 at 250-500 terabytes and not available below 250 terabytes	Not documented as a comparable guarantee
Year 1 total (license plus Veeam storage)	\$89,125-\$159,250	\$156,000-\$273,600	\$49,000-\$61,500, entry tier only

At the same scenario, Rubrik's list cost runs 2.0x-2.4x Veeam's matching tier, and Commvault's entry tier comes in below both at list, but it excludes the recovery editions that carry the ransomware features, so its figure is a floor, not a comparison to Rubrik Enterprise. Negotiated prices run lower on all three. The comparison that cannot be priced from public data is the labor: Veeam's lower list cost is partly offset by the ongoing work of configuring and maintaining immutability.

Costs the Pricing Table Misses

- **Veeam's list price assumes correctly configured immutability.** A misconfigured hardened repository or object-lock setup defeats the ransomware protection the platform was bought for, so budget security-engineering time for configuration, not just the license fee.
- **Veeam's renewal increases.** Perpetual socket list prices rose up to 9% in July 2026, a tracker reports 20%-30% increases at renewal in some user accounts, and late renewals carry a reported 25% penalty. Confirm the escalation clause in writing before signing.
- **Veeam's storage infrastructure.** A tracker estimates 15%-40% of license cost for repositories and hardware, which the per-workload rate does not include.
- **Rubrik's warranty threshold.** The \$10 million headline applies only from 10 petabytes; a 250-500 terabyte customer is covered up to \$250,000, and an environment under 250 terabytes is not eligible. Read the agreement before pricing the warranty into the decision.
- **Rubrik's three-year minimum.** Most subscriptions run three years, with an option to extend to five, so a first-year price comparison understates the commitment.
- **Commvault's implementation labor.** One independent benchmark rates implementation and recovery-runbook maturity at only 3.7 out of 5, so budget training and onboarding beyond the license line.
- **Patching urgency.** An organization running affected Veeam versions had to patch immediately after the March 2026 disclosure, an irregular but real operational cost for whichever platform discloses the next critical vulnerability.

Complexity Comparison

Dimension	Veeam	Rubrik	Commvault
Implementation	Moderate; initial setup is documented as complex for first-time users, with advanced features requiring additional learning beyond core backup setup	Lowest of the three per independent sources; consistently described as fast and straightforward, with one reviewer rating initial setup "11 out of 10"	Highest of the three; independently rated 3.7/5 on implementation and recovery-runbook maturity with reviewers describing deployment as complex and requiring a steep learning curve
Admin dependency	Moderate to high; immutability is not secure by default and requires deliberate, ongoing configuration of hardened repositories or object lock	Lowest of the three; immutable-by-default architecture is documented as reducing management overhead relative to Veeam's manual configuration model	Moderate to high; SQL and Windows Server configuration complexity is a specific, documented administrative burden beyond the core platform
Learning curve	Moderate; the six-product portfolio is documented as overwhelming some teams during upgrades, a distinct friction from day-to-day single-product use	Gentlest of the three for core backup and recovery workflows; the documented friction is concentrated in advanced features (analytics, threat hunting), described as under-documented rather than difficult by design	Steepest of the three by independent account; one reviewer's summary, "powerful, but it's still complex to set up and manage," is representative of the broader pattern

The pattern across all three tracks closely with each platform's architectural philosophy. Rubrik's security-first, immutable-by-default design pays off in lower implementation and admin burden, the tradeoff is a steeper, less-documented path once a team moves past core backup into advanced threat-hunting features. Veeam's flexibility and broad platform

support come at the cost of manual security configuration that Rubrik handles by default. Commvault's breadth, the widest workload coverage of the three, is the direct cause of its documented complexity; covering 250-plus workload types from one console is not a lightweight engineering problem for the vendor or the buyer.

Red Flags

Every finding below is independently documented and material enough to influence a purchasing decision.

Veeam	Rubrik	Commvault
• Critical vulnerabilities were disclosed March 12, 2026. Veeam's advisory for version 13 lists six CVEs, three critical, two at CVSS 9.9 exploitable by an authenticated domain user or a Backup Viewer. Confirm patch status against build 13.0.1.2067 (or 12.3.2.4465 for version 12) immediately. • Veeam Backup & Replication is a documented ransomware target. Akira and Fog ransomware actors have extracted sensitive information from Veeam deployments. Restrict console access to the minimum accounts and audit who holds any level of access. • Immutability needs manual configuration. A misconfigured hardened repository or object-lock setup leaves backups exposed to the encryption risk the platform is meant to prevent. Audit the configuration rather than assuming it is correct.	• The warranty does not scale down. Eligibility starts at 250 terabytes and the cap is \$250,000 at 250-500 terabytes, against a \$10 million headline. Confirm your data volume against the schedule. • Pricing is quote-only and third-party figures disagree. Reseller list rates and Vendr figures differ. Get line-item pricing in writing, and note the three-year minimum. • Advanced features are under-documented. Analytics and threat hunting are described as requiring deeper product knowledge than core backup. Confirm documentation and training before assuming the ease-of-use reputation extends to them.	• Deployment complexity is the most consistent complaint. Implementation and recovery-runbook maturity is rated 3.7 out of 5. Budget implementation-services time and confirm runbook maturity before assuming production readiness. • List prices overstate and understate in different places. Published rates sit above typical closing prices, and the recovery editions that carry ransomware features cost more than the entry tier. Get an itemized quote and benchmark it against Veeam. • Recovery readiness depends on customer discipline. A broad feature set does not substitute for tested, maintained runbooks. Confirm what ongoing operational discipline the platform assumes.

The Decision Framework

Choose Veeam if:

- Broad virtualization and workload support at the lowest published per-workload price among the platforms with published list rates is the priority, and a free pilot via Community Edition fits the evaluation process.
- You have confirmed current patch status against the March 2026 CVEs and have a documented process for applying future security updates promptly, not at the next scheduled maintenance window.
- Security engineering capacity exists to properly configure hardened repositories and object lock, since immutability is not secure by default on this platform.

Choose Rubrik if:

- A security-first, immutable-by-default architecture that minimizes manual configuration burden is a higher priority than the most transparent pricing.
- The Ransomware Recovery Warranty's schedule has been checked against your data volume, since the \$10 million cap applies only at 10 petabytes and eligibility starts at 250 terabytes.
- You've budgeted for a premium over Veeam's list pricing and have gotten a detailed quote in writing, rather than relying on third-party pricing estimates.

Choose Commvault if:

- Workload diversity is broad, 250-plus supported types, and a single console covering that full breadth outweighs the documented implementation complexity.
- Implementation services budget and timeline account for the platform's independently documented 3.7/5 implementation and recovery-runbook maturity rating, not an optimistic best-case timeline.
- You have pushed for itemized, detailed pricing and benchmarked it against Veeam's list rates before accepting any premium.

Key Decision Factors

Design decides how ransomware resilience is delivered. Veeam is a flexible, broad platform where immutability is a configuration you must get right. Rubrik builds immutability and zero-trust into the architecture. Commvault spreads the widest workload coverage across one console and carries the most implementation complexity.

Audience decides which one fits. Veeam suits virtualization-heavy teams with security engineering capacity. Rubrik suits security-first organizations that want less configuration and can pay a premium. Commvault suits heterogeneous estates that justify a longer implementation.

Price follows the model, and the two big findings change the math. At list for 500 workloads, Veeam runs about \$77,500-\$113,750 a year, Commvault's entry tier about \$49,000-\$61,500, and Rubrik \$156,000-\$273,600 at an assumed 100 terabytes. Veeam's March 2026 vulnerabilities call for immediate patching and access audits, and Rubrik's headline warranty applies in full only at 10 petabytes, so neither finding should be left out of the evaluation.

The bottom line:

- A virtualization-heavy organization with security engineering capacity should choose Veeam, confirm patch status against the March 2026 advisory, and audit its immutability configuration.
- A security-first organization should choose Rubrik, get quote-based pricing in writing, and check its data volume against the warranty schedule.
- A heterogeneous estate should choose Commvault, with an itemized quote and an implementation budget that reflects its documented complexity.