

UNVARNISHED REVIEWS

Arctic Wolf vs. Expel vs. Red Canary: The Managed Detection and Response Verdict

Unvarnished Reviews Research

Market Position: Renting a SOC, and Who Owns the Landlord

Most mid-market security teams cannot staff a SOC that works around the clock, so they rent one. Managed detection and response is the product that does it: a provider watches alerts from your endpoints, identities, cloud accounts, and network, investigates them, and either contains the threat or tells your team what to do. The differences between providers are less about whether they detect threats and more about what they require you to own, how much of the response they perform, and who stands behind the service.

Ownership has become part of that question. Zscaler completed its acquisition of Red Canary on August 1, 2025, a deal reported at about \$675 million, though Zscaler's release did not disclose the price. The release says Red Canary will initially operate as a separate business unit and be branded "Red Canary, a Zscaler company," and that Zscaler plans to combine Red Canary's agentic AI technology with its Data Fabric for Security. Arctic Wolf, for its part, has built out an endpoint offering, Aurora Managed Endpoint Defense, after acquiring Cylance's endpoint business from BlackBerry. Expel is the one of the three that does not sell endpoint protection: it works on top of the tools you already run.

For a buyer, that shapes three things: which of your existing tools the provider supports, what the roadmap prioritizes, and how much leverage you have at renewal. A provider owned by a platform vendor may steer toward its parent's products, and one that sells sensors may support yours less enthusiastically. None of the three has been shown to do either, but each structure carries a different version of the question, and a multi-year contract should answer it in writing.

Arctic Wolf: The Upside

Arctic Wolf is the most complete single-vendor package of the three. The service combines MDR with managed risk, security awareness training, an incident response retainer, and its Aurora platform, delivered through a named Concierge Security Team that holds scheduled reviews with the customer. Users rate Arctic Wolf 4.7/5 across 280 reviews, and customer support is the most-cited strength (58 mentions), followed by threat detection (47). Users score quality of support 9.4 out of 10 and ease of setup 9.0, the highest setup score of the three.

It is the only one of the three with a published warranty. Arctic Wolf's Security Operations Warranty is described as up to \$3 million: \$750,000 on a one-year term and \$1.5 million on a three-year term for the Standard tier, doubling to \$1.5 million and \$3 million at the Max tier, which requires adding Aurora Managed Endpoint Defense. Covered events include ransomware and business email compromise, with legal compliance response included, and coverage for cyber legal liability and business income loss is not part of the Core tier. The warranty can help fund a cyber insurance deductible, and Arctic Wolf states that it is not a licensed insurance producer. Neither Expel nor Red Canary is documented offering a comparable warranty in the sources reviewed.

The bundle suits a small team. A company with a few IT generalists and no security staff gets monitoring, a named point of contact, risk scanning, and training under one contract, instead of assembling an EDR, an MDR provider, and a vulnerability program from different vendors.

Arctic Wolf: The Downside

Cost is the most-cited complaint. Users name "expensive" as the top con (10 mentions) and false positives next (7), and also report that new features arrive as separate paid items and that access to underlying SIEM data is limited. Arctic Wolf publishes no commercial price list, and the one schedule in public circulation is its public-sector list, which carries a \$15,000 platform fee before per-user charges.

Remediation can fall to your team. One reviewer, quoted in a competitor's pricing guide, says Arctic Wolf "overly relies on the client's team for remediation." The quote comes from a vendor with a commercial interest, so treat it as a question to put to Arctic Wolf during evaluation: which response actions will the Concierge Security Team take on your behalf, and which will it hand back to you?

Contract terms deserve a read. One reviewer reports a 60-day renewal notice window instead of the typical 30 days on a partner-sold contract. Vendr reports that Arctic Wolf renewals typically come in 5%-15% above the expiring contract unless negotiated, and 10%-20% higher on last-minute or automatic renewals.

A May 2026 restructuring adds a question about continuity. Arctic Wolf cut about 250 roles, roughly 8.3% of its workforce by one tracker's estimate, with the reductions reported to fall on sales, product, and marketing teams. A company spokesperson called it an "organizational restructuring" to "better align the company's structure and investments with our long-term strategy" while it keeps investing in its Aurora platform and an agentic SOC. The company made no statement about SOC analysts or customer support, and the reporting did not show service effects. Ask which teams support your account and whether your Concierge Security Team is changing.

Expel: The Upside

Expel works with the tools you already own. A profile of the service describes direct API integrations with more than 160 tools across endpoint, identity, cloud, network, and security information and event management (SIEM) platforms, with no new agent or SIEM required, and an Expel Workbench portal that records every analyst and AI action in an audit trail. For a team that has already standardized on CrowdStrike, SentinelOne, or Microsoft, that avoids rip-and-replace.

Transparency is the differentiator. Customers see what analysts did and why, and response actions can run automatically when a detection fires or after an analyst confirms a true positive, which the profile says is the more common setting. Users score Expel highest of the three on quality of support (9.5) and 9.1 on ease of use, and rate it 4.6/5 on 74 reviews, with a matching 4.6 across 146 ratings on Gartner Peer Insights. Per the profile, live monitoring can begin within hours of connecting data sources.

Packaging is flexible. Expel sells three packages, Starter, Select, and Premium, with Premium adding unlimited integrations, API access to Workbench, and a dedicated engagement manager. A May 2024 announcement introduced new offerings aimed at organizations at different stages of MDR maturity, and existing customers move to them at renewal.

Expel: The Downside

Expel is the most expensive of the three in purchase data. Vendr's median buyer pays \$196,629 a year across 51 purchases, in a range of \$60,577-\$302,483, roughly 2.5 times the medians for Arctic Wolf and Red Canary. Vendr's directional bands put spend at \$75,000-\$150,000 under 500 assets, \$150,000-\$400,000 from 500 to 2,000 assets, and above \$400,000 beyond that.

You must already own the tools. Expel does not sell endpoint protection, so the EDR licenses, and any SIEM or cloud log costs, are separate and sit outside the Expel contract. The profile notes that the service works best with a strong existing toolset and suits mid-market and enterprise organizations. A small team without an EDR has more to buy before Expel is useful.

Smaller-sample criticisms point to communication and customization. The top cons among users are communication issues and limited customization (4 mentions each), a thin base given 74 reviews. Vendr reports that standalone onboarding runs \$10,000-\$50,000 or more when it is not bundled, true-up fees apply when asset counts grow mid-term, and custom playbooks or professional services reportedly add 10%-20%.

Repackaging at renewal means repricing at renewal. Because existing customers move to the 2024 offerings at renewal, the renewal quote may not be a continuation of the current price. Vendr reports escalators of about 3%-7% and recommends capping them.

Red Canary: The Upside

Red Canary works across the widest documented set of tools. Its supported-integrations page lists eight EDR integrations (including CrowdStrike Falcon Insight, Microsoft Defender for Endpoint, SentinelOne Singularity, Palo Alto Cortex XDR, Carbon Black, and Trend Micro Vision One), identity sources such as Okta, Microsoft Entra ID, and Cisco Duo, cloud platforms (AWS, Google Cloud, Microsoft Azure, and Wiz), network tools from Cisco, Fortinet, Palo Alto, and Zscaler, and Google Workspace and Microsoft 365 for SaaS and email. It also covers operational technology through Dragos. Vendor neutrality is the core of the pitch.

Users rate it as highly as Arctic Wolf. Red Canary scores 4.7/5 across 131 reviews, and 4.6 across 138 ratings on Gartner Peer Insights. Customer support (40 mentions), threat detection (26), reliability (20), and alert management (16) are the leading strengths, and users score quality of support 9.3 and ease of setup 8.9.

Entry cost is the lowest of the three. Vendr's observed range starts at \$26,980, and its directional per-endpoint benchmarks run about \$50-\$75 for 100-500 endpoints, \$35-\$55 for 500-2,000, and under \$35 above 2,000, all for endpoint coverage before identity, cloud, and network add-ons. The median of \$79,881 sits near Arctic Wolf's.

Zscaler brings scale. The parent's sales reach and engineering resources could extend Red Canary's largely North American footprint, and the release says Red Canary will keep developing its SOC capabilities. Zscaler's stated aim is continuity for customers.

Red Canary: The Downside

The acquisition is the central open question. Forrester's analysts, writing when the deal was announced, called Zero Trust and MDR a weak pairing for bundling, noted that technical integration had no public timeline, and warned about a culture clash between Zscaler's sales-and-marketing orientation and Red Canary's practitioner-driven, expertise-first culture. They also said Red Canary's open community work and its Managed XSIAM partnership with Palo Alto Networks, a Zscaler competitor, were now "a question mark." Zscaler's release does not address those points. It says Red Canary will operate initially as a separate business unit and makes no statement about pricing.

The alert experience draws the most criticism. The top con among users is an inefficient alert system (13 mentions), followed by communication issues (7), and reviewers also cite premium pricing and inflexible dashboard customization.

Price is opaque and add-ons are modular. Red Canary publishes no price list. Cloud, identity, and network coverage are sold as add-ons, which is why the Vendr median (\$79,881) is far above the endpoint-only per-endpoint math. Vendr reports annual escalators of 3%-5% and advises bundling add-ons into the initial contract and setting growth and true-up terms up front.

No warranty is documented. Unlike Arctic Wolf, Red Canary is not documented offering a financial guarantee against a breach.

Platform Ratings at a Glance

Platform	G2 Rating	G2 Reviews	Gartner Peer Insights	Trustpilot	Note
Arctic Wolf MDR	4.7 / 5	280	Not independently confirmed at time of publication	3.1 / 5 on 9 reviews, too few to treat as meaningful	Most reviews of the three; cost is the top con; May 2026 restructuring
Expel MDR	4.6 / 5	74	4.6 / 5 (146 ratings)	No meaningful Trustpilot presence identified	Highest support score (9.5); highest median spend
Red Canary MDR	4.7 / 5	131	4.6 / 5 (138 ratings)	No meaningful Trustpilot presence identified	Now owned by Zscaler; alert system is the top con

All three sit in a narrow 4.6-4.7 band, so the ratings cannot separate them. The decision-relevant differences are what each requires you to own, what each costs for comparable scope, and what the ownership changes at Red Canary and Arctic Wolf mean for continuity. The Arctic Wolf Trustpilot score rests on nine reviews, one of which appears to describe a restaurant, so it is shown for completeness and not as evidence.

Pricing (October 2026)

Platform	Entry Tier	Mid Tier	Top Tier	Pricing Model
Arctic Wolf	MDR Core Silver \$192 per user, plus a \$15,000 Aurora platform fee (public-sector list)	MDR Core Gold \$218 per user; Plus tiers (adds managed risk) \$295 / \$321 / \$360 per user	MDR Core Platinum \$257 per user; Total tiers (adds risk, awareness, and an incident response JumpStart retainer) \$325 / \$351 / \$390 per user	Per user or per server, billing period not stated on the sheet; Aurora Managed Endpoint Defense \$110 per device; quote-based for commercial buyers. Vendr median \$79,740 (range \$24,469-\$315,023)
Expel	Starter package, quote-based	Select package, quote-based	Premium package: unlimited integrations, API access, dedicated engagement manager	Scoped by monitored assets and integrated tools; annual contracts; no list price. Vendr median \$196,629 across 51 purchases (range \$60,577-\$302,483)
Red Canary	About \$50-\$75 per endpoint a year for 100-500 endpoints (Vendr benchmark)	About \$35-\$55 per endpoint for 500-2,000 endpoints	Under \$35 per endpoint above 2,000, plus cloud, identity, and network add-ons	Annual per-endpoint subscription with volume tiers and modular add-ons; no list price. Vendr median \$79,881 (range \$26,980-\$154,687)

The Arctic Wolf figures come from a public-sector price list, which carries a 5% government discount and does not state a minimum or term, so commercial quotes can differ. A third-party guide that cites Vendr transaction data from May 2026 reports a median of \$96,340 across 17 deals, higher than the \$79,740 on Vendr's page, and Vendr's page cites two different ranges, so Arctic Wolf's real price band is wider than any single figure suggests. Vendr reports typical discounts of 20%-35% for multi-year or 500-plus-endpoint Arctic Wolf deals and 15%-30% for multi-year Expel and Red Canary commitments. Expel and Red Canary figures are Vendr benchmarks, not quotes.

TCO Comparison: 500-Endpoint Mid-Market Company, One Year

Scenario: 500 endpoints or users, MDR service only, at list or benchmark prices before negotiation. For Expel and Red Canary, the company is assumed to already license an EDR; for Arctic Wolf, the Core tier is assumed with the customer's existing EDR as well.

Line Item	Arctic Wolf	Expel	Red Canary
Service subscription	Platform fee \$15,000 + 500 × \$218 (Core Gold) = \$124,000; Silver \$111,000, Platinum \$143,500	\$150,000, the bottom of Vendr's 500-2,000 asset band	500 × \$35-\$75 = \$17,500-\$37,500 for endpoint coverage; up to the Vendr median of \$79,881 with identity, cloud, and network add-ons
Onboarding	Not itemized in the sources	\$10,000-\$50,000 if quoted separately	Negotiable; not itemized in the sources
Professional services and custom playbooks	Not itemized in the sources	10%-20% of the subscription: \$15,000-\$30,000	Not itemized in the sources
Remediation labor	\$15,000-\$50,000 reported in a third-party estimate, because response can fall to the customer	Response actions run automatically or after analyst confirmation, configured in Workbench	Not itemized in the sources
Financial backstop	Warranty of \$750,000-\$3 million depending on tier and term	None documented	None documented
Year 1 total, modeled	\$139,000-\$174,000	\$175,000-\$230,000	\$17,500-\$79,881

The ranges overlap less than the medians suggest. Expel's modeled floor of \$175,000 sits above the top of Arctic Wolf's list-based range, and Red Canary's range is wide because the cost of identity, cloud, and network add-ons is the largest swing. Buyers close below list: Vendr's median for Arctic Wolf is \$79,740-\$96,340, about 22%-36% below the \$124,000 list-based subscription. If you also need endpoint protection from Arctic Wolf, Aurora Managed Endpoint Defense lists at \$110 per device, or \$55,000 for 500 devices, which is the cost of the bundle that Expel and Red Canary leave to you.

Costs the Pricing Table Misses

- **EDR licenses sit outside Expel and Red Canary.** Both expect you to run an endpoint product, so its cost belongs on the comparison. Arctic Wolf prices its endpoint offering, \$110 per device on the public-sector list, separately from the MDR tier.
- **Arctic Wolf's platform fee.** The public-sector list carries a \$15,000 Aurora platform fee ahead of per-user charges, which weighs heavily on small deployments.
- **Arctic Wolf's add-on stack.** Managed risk lists at \$100 per user, managed security awareness at \$30-\$42 per user, and an incident response JumpStart retainer at \$5,000 per organization. Users report that new features arrive as extra paid items.
- **Renewal uplifts.** Vendr reports Arctic Wolf renewals typically 5%-15% above the expiring contract and 10%-20% on automatic renewals, with escalators of about 3%-7% at Expel and 3%-5% at Red Canary. Cap them in the contract.
- **Expel's onboarding, true-ups, and services.** Standalone onboarding is reported at \$10,000-\$50,000 or more, true-up fees apply when assets grow, and playbooks and professional services reportedly add 10%-20%.
- **Red Canary's modular add-ons.** Cloud, identity, and network coverage are sold separately, so a quote built on endpoints alone understates the final contract.
- **Notice windows.** One reviewer reports a 60-day non-renewal notice on a partner-sold Arctic Wolf contract. Missing the window renews the term.

Complexity Comparison

Dimension	Arctic Wolf	Expel	Red Canary
Deployment model	Bundled: a proprietary platform and sensors, with an optional Aurora endpoint product	API integrations into the tools you already run; no new agent or SIEM required	Integrations into the major EDR, identity, cloud, and network tools; no sensor
Implementation and onboarding	Users score ease of setup 9.0, the highest of the three	Users score ease of setup 8.8; live monitoring reported within hours of connecting data sources; onboarding fees of \$10,000-\$50,000 are reported when quoted separately	Users score ease of setup 8.9; onboarding terms are negotiable
Admin and staffing dependency	Low for monitoring; some remediation reportedly falls to your team	Higher: assumes an existing, working security toolset and someone who owns it	Moderate: assumes a supported EDR is deployed and healthy
Learning curve for advanced use	Users cite limited access to underlying SIEM data	Workbench exposes analyst actions; users cite limited customization	Users cite inflexible dashboard customization
Integration friction	Highest if you want to keep a non-Aurora EDR: the bundle favors Aurora telemetry	Lowest: more than 160 integrations	Low across a broad documented list, but partner integrations tied to Palo Alto are now uncertain
Alert quality and communication	Users cite false positives (7 mentions)	Users cite communication issues (4)	Users cite an inefficient alert system (13) and communication issues (7)

The pattern follows each design. Arctic Wolf is the easiest to start and asks the most of its customer in lock-in, because the bundle works best when you adopt its tools. Expel asks the most of your existing environment and gives the most visibility in return. Red Canary asks you to have a supported EDR in place and gives broad coverage, with alert handling the area users criticize most.

Red Flags

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

Arctic Wolf	Expel	Red Canary
• A May 2026 restructuring cut about 250 roles. The company calls it an "organizational restructuring" to align investment with long-term strategy and reported no change to SOC analysts or support, and the reporting shows cuts in sales, product, and marketing teams. Ask who supports your account and whether your Concierge Security Team is changing. • Renewal terms favor the vendor. Vendr reports renewals typically 5%-15% above the expiring contract and 10%-20% on automatic renewals, and one reviewer reports a 60-day notice window. Negotiate a cap and a 30-day notice period.	• It is the most expensive of the three in purchase data. Vendr's median is \$196,629, about 2.5 times the other two, and you also pay for an EDR. Test the cost against a scoped quote from the others. • Renewal pricing may be reset. Existing customers move to Expel's 2024 offerings at renewal, so the renewal quote may not continue the current price. Ask for a renewal price commitment in the initial contract.	• Ownership changed on August 1, 2025. Zscaler says Red Canary will operate as a separate business unit to ensure continuity, and Forrester analysts flagged culture, independence, and partnership risk. Get a change-of-control and continuity commitment, and confirm your EDR remains supported. • The Palo Alto Managed XSIAM partnership is uncertain. Forrester called partnerships that depended on MDR independence "a question mark," because Palo Alto competes with Zscaler. If you run Palo Alto, ask how your integration is supported.

- **Cost and false positives lead the criticisms.** Users name "expensive" (10 mentions) and false positives (7) as the top cons, and report extra charges for new features. Get an itemized quote and confirm which features are included.

- **The top warranty tier has conditions.** The \$3 million figure requires the Max tier, with Aurora Managed Endpoint Defense and a three-year term; a one-year Standard term is \$750,000. Read the terms and conditions before pricing it into the decision.

- **Onboarding, true-ups, and services add to the contract.** Standalone onboarding is reported at \$10,000-\$50,000 or more, growth triggers true-up fees, and custom playbooks reportedly add 10%-20%. Put growth pricing in writing.

- **Communication and customization draw criticism.** Users cite both at 4 mentions each, from a small base of 74 reviews. Ask for references that match your size.

- **Alert handling is the top criticism.** Users cite an inefficient alert system (13 mentions) and communication issues (7). Ask to see the alert workflow and a sample escalation.

- **Price is quote-only and add-ons are modular.** Cloud, identity, and network coverage are separate, and escalators run 3%-5%. Bundle coverage into the first contract and cap increases.

The Decision Framework

Choose Arctic Wolf if:

- You are a lean IT team that wants one provider for monitoring, risk, training, and response guidance, with a named contact and a warranty.
- You can accept a bundle that favors its platform and sensors, and you have confirmed in writing which response actions the team performs for you.
- You have weighed the May 2026 restructuring and have a renewal cap and a 30-day notice period in the contract.

Choose Expel if:

- You already own and run a working EDR, identity, and cloud stack, and want transparency into every analyst action for audits or board reporting.
- The budget supports the highest median spend of the three, plus onboarding and your tool licenses.
- You have a renewal price commitment in writing, since the 2024 offerings reset pricing at renewal.

Choose Red Canary if:

- Your estate is built on one of the supported EDR platforms and you want detection expertise on top of it, at the lowest entry cost among the three.
- You are comfortable with Zscaler ownership and have a change-of-control and continuity commitment, particularly if you run Palo Alto tooling.
- You have scoped identity, cloud, and network coverage in the first quote, so add-ons do not surprise you at renewal.

Key Decision Factors

Design decides what you must own. Arctic Wolf is a bundle: you adopt its platform and sensors and get one accountable provider, a Concierge Security Team, and a warranty. Expel is a transparent layer on top of tools you already run, with the most visibility into analyst work. Red Canary is a practitioner-led service across a wide set of EDR, identity, cloud, and network tools, now inside Zscaler.

Audience decides which one fits. Arctic Wolf suits lean teams that want to buy security as a service. Expel suits mature teams with a toolset worth wrapping. Red Canary suits EDR-standardized organizations that want expertise and breadth.

Price depends on scope, and the headline medians mislead. Vendr's medians put Arctic Wolf and Red Canary near \$80,000 and Expel near \$196,600, but Arctic Wolf includes a platform and sensors that the other two do not, and Red Canary's median includes add-ons that its per-endpoint figures do not. On a 500-endpoint scenario the modeled ranges are \$139,000-\$174,000 for Arctic Wolf, \$175,000-\$230,000 for Expel, and \$17,500-\$79,881 for Red Canary before EDR costs.

The Bottom Line

- A lean team without a security staff should shortlist Arctic Wolf, get the response-action split and the warranty tier in writing, and ask how the May 2026 restructuring affects its Concierge Security Team.
- A mature team with an existing toolset should shortlist Expel, compare it with a scoped Red Canary quote, and negotiate onboarding and a renewal price commitment before signing.
- An EDR-standardized team should shortlist Red Canary, obtain written continuity and change-of-control terms, and scope identity and cloud coverage up front.

No MDR provider in this comparison is a clean win. Arctic Wolf's bundle is the easiest to start and the one with a warranty, and its cost, renewal terms, and recent restructuring are real. Expel gives the most visibility and costs the most, with renewal repricing built into its 2024 offerings. Red Canary has the broadest tool coverage and the lowest entry cost, and the Zscaler acquisition is an open question that no review can yet answer. Every provider here carries real pricing friction. The choice is which of those tradeoffs your team can afford and manage.