# CrowdStrike vs. SentinelOne: What Security Teams Actually Experience

*Unvarnished Reviews Research*

*This report synthesizes data from 800+ verified user reviews and practitioner community posts collected from G2, Capterra, TrustRadius, PeerSpot, Spiceworks, Reddit practitioner communities including r/netsec, r/crowdstrike, and r/sysadmin, and IT community practitioner forums. Pricing data reflects published vendor pricing, enterprise procurement benchmarks from Vendr, and independent 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

**CrowdStrike Falcon** is the market-leading enterprise EDR/XDR platform with the deepest threat intelligence ecosystem, the most mature Windows detection capabilities, and the largest managed threat hunting operation in the category. It is also the platform responsible for the largest IT outage in recorded history on July 19, 2024, an event that permanently changed how enterprise security teams assess EDR agent risk.

**SentinelOne Singularity** is the strongest technical alternative, delivering 100% detection rates in independent MITRE ATT&CK; evaluations, autonomous response capabilities that reduce analyst workload, and pricing that runs materially lower than CrowdStrike at comparable tiers. It is also the platform that experienced its own global console outage on May 29, 2025, while actively marketing its architectural superiority over CrowdStrike's cloud-dependent model. That outage does not erase SentinelOne's technical advantages. But it changes the outage risk narrative materially.

Neither platform has a clean architectural record on reliability. The choice between them depends on SOC maturity, budget, threat profile, and an honest assessment of each platform's outage posture, not vendor marketing from either side.

## Platform Ratings at a Glance

| Platform | G2 | Capterra | TrustRadius | Software Advice |
|---|---|---|---|---|
| CrowdStrike Falcon | 4.7 / 5 | 4.7 / 5 | 4.7 / 5 | 4.7 / 5 (55 reviews) |
| SentinelOne Singularity | 4.7 / 5 | 4.8 / 5 | 4.7 / 5 | 4.8 / 5 (109 reviews) |

Both platforms rate identically across all major review platforms. SentinelOne edges CrowdStrike on Capterra and Software Advice by 0.1 points, consistent with practitioner communities rating SentinelOne's management simplicity and cross-platform coverage slightly higher than CrowdStrike's. PeerSpot rates SentinelOne Singularity Complete at 8.8/10 from a large enterprise-weighted review set, reflecting strong satisfaction among organizations that have successfully deployed and configured the platform.

The meaningful differentiation shows up not in aggregate ratings but in specific capability scores and the nature of complaints, and in two documented outage events that belong at the center of any honest 2026 evaluation.

---

## The Two Outages: What Buyers Must Assess

### CrowdStrike: July 19, 2024

On July 19, 2024, CrowdStrike deployed a content configuration update, Channel File 291, to its Falcon Sensor for Windows. The update contained a logic error triggering an out-of-bounds memory read that caused approximately 8.5 million Windows devices worldwide to enter an infinite boot loop. The outage was the largest in recorded IT history.

Recovery was not a software patch. IT teams had to physically access each device, boot into safe mode, and delete specific files. BitLocker-encrypted systems required a unique 48-digit recovery key per device, a multi-day or multi-week remediation effort for organizations with thousands of affected endpoints. Fortune 500 companies incurred an estimated $5.4 billion in direct losses. CrowdStrike's stock fell approximately 40% in the weeks following the incident.

CrowdStrike's CEO issued a public apology, took full responsibility, and implemented additional testing layers and staged rollout procedures. The fundamental cloud-dependent update architecture has not changed.

### SentinelOne: May 29, 2025

On May 29, 2025, less than a year after SentinelOne's CEO publicly stated that the concerns raised by the CrowdStrike outage would "play out for years", SentinelOne experienced its own global platform outage. The outage lasted approximately 7 hours, eliminating security console visibility for all connected commercial customers globally.

The distinction from CrowdStrike's outage is important and must be stated accurately: SentinelOne's May 2025 outage affected console visibility, the management interface, not endpoint protection itself. Customer endpoints remained protected during the outage. Threat data reporting was delayed, not lost. This is meaningfully different from CrowdStrike's July 2024 outage, which took endpoints offline entirely and required manual device-by-device remediation.

SentinelOne's root cause analysis attributed the outage to a control system error triggered by the creation of a new account during a cloud architecture migration. The company was in the process of transitioning its production system to a new cloud-based architecture built on infrastructure-as-code principles.

**What this means for buyers:** Both platforms have now experienced documented global outages. CrowdStrike's was categorically more severe, endpoint protection failed and manual remediation was required at scale. SentinelOne's was serious but fundamentally different, security visibility was lost but endpoints remained protected. Any vendor claiming architectural immunity to outage risk should be evaluated against this documented record from both platforms.

---

## Architecture: The Core Difference

### CrowdStrike: Cloud-Dependent Processing

CrowdStrike's Falcon agent is intentionally lightweight on the endpoint. Detection and analysis happen in CrowdStrike's Security Cloud, processing telemetry streamed from endpoints in real time. This delivers extremely

lightweight endpoint footprint and real-time threat intelligence from across CrowdStrike's 28 trillion+ daily security events. It also creates the update architecture risk that July 2024 demonstrated, where a faulty content update simultaneously affects all endpoints receiving the update.

### SentinelOne: Autonomous On-Endpoint AI

SentinelOne's AI detection and response engine runs directly on the endpoint. The platform can detect, respond to, and remediate threats without cloud connectivity or human authorization. The one-click rollback capability, restoring an endpoint to its pre-attack state, is a meaningful operational advantage in ransomware incidents. The staged update rollout architecture reduces the per-update blast radius compared to CrowdStrike's simultaneous global deployment model.

The May 2025 console outage revealed that SentinelOne's cloud management layer carries its own reliability risk even when the endpoint protection layer functions correctly, a nuance that its marketing around "cloud-dependent architecture creates a single point of failure" (directed at CrowdStrike) did not previously acknowledge.

---

## What Users Actually Report

### CrowdStrike: What Works

TrustRadius, G2, and PeerSpot reviewers consistently praise CrowdStrike's threat intelligence depth, incident response console, and ecosystem breadth. Security practitioners specifically call out the Falcon OverWatch managed threat hunting service, a team of human analysts hunting for threats across CrowdStrike's global installed base, as a capability that SentinelOne's Vigilance MDR competes with but has not matched in scale or tenure.

PeerSpot enterprise practitioners describe CrowdStrike as the default choice when budget is secondary and when the organization has dedicated threat hunters who will use the depth of the Falcon console. The platform's 28% consideration rate among organizations evaluating endpoint security alternatives reflects its position as the enterprise default.

### CrowdStrike: What Doesn't Work

**Licensing complexity** is the most consistent complaint across TrustRadius, G2, and PeerSpot. CrowdStrike sells its platform as a series of separate module subscriptions. A $184.99/device/year Enterprise quote routinely becomes $300-$400+/device when Identity Protection, Spotlight, OverWatch, and Next-Gen SIEM are assembled. Enterprise procurement teams consistently describe discovering add-on costs after contract signature.

**Post-July 2024 trust deficit** persists even among customers who stayed. The architectural risk is now an explicit line item in enterprise security vendor evaluations in ways it was not before.

**Support at standard tiers** is a recurring complaint, practitioners report multiple agents joining a single chat session, templated AI responses, and production changes made without warning. Premier Support, which addresses most of these issues, costs an additional 30% of license fees annually.

### SentinelOne: What Works

TrustRadius, PeerSpot, and Capterra data consistently identify autonomous response, management simplicity for mid-market organizations, and cross-platform coverage as SentinelOne's strongest attributes. The one-click rollback for

ransomware recovery is specifically called out as a differentiator not available in CrowdStrike at the same level of automation.

PeerSpot enterprise practitioners rate SentinelOne's customer-driven support model positively, describing access to product management and ongoing communication as above average compared to similarly-sized security vendors. Software Advice reviewers rate SentinelOne's Behavioral Analytics at 4.89/5 and Endpoint Protection at 5.0/5, the highest scores on the platform.

### SentinelOne: What Doesn't Work

**Dashboard complexity** is the most consistent complaint from Spiceworks community practitioners, specifically that the configuration interface is unclear about whether protection groups are correctly set up, creating uncertainty about actual protection status.

**Resource consumption during scans** is documented across Capterra and TrustRadius, SentinelOne agents can significantly consume endpoint resources during scan operations, which is documented as "unacceptable for older computers still in production."

**Agent removal difficulties** are a documented operational pain point. Practitioners report that SentinelOne does not provide uninstaller tools for endpoints not connected to the portal, meaning disconnected endpoints cannot be uninstalled without manual intervention.

**TrustRadius pricing concerns** for smaller organizations: minimum agent counts and annual billing requirements make SentinelOne expensive for teams below the platform's intended enterprise scale.

**Support quality distinction** documented in IT practitioner communities: "Unlike CrowdStrike where you feel like you have hired a partner, SentinelOne often feels like you have bought a software tool with a help desk attached." This distinction matters most for organizations without strong internal security operations expertise who depend on vendor partnership for threat response guidance.

**The May 2025 outage**, while less severe than CrowdStrike's July 2024 event, undermined SentinelOne's positioning as the architecturally safer alternative. The irony of SentinelOne experiencing a global outage within a year of marketing its cloud-dependency critique of CrowdStrike was not lost on the practitioner community.

---

## MITRE ATT&CK;: The Independent Technical Benchmark

The MITRE ATT&CK; Evaluations are the gold standard for independent endpoint security assessment, third-party simulation of real-world attack techniques with no vendor influence over results.

**2024 MITRE ATT&CK; Enterprise Evaluation:** SentinelOne achieved 100% detection accuracy across all 16 attack steps and 80 substeps, zero detection delays, and 88% fewer alerts than the median across all evaluated vendors, its fifth consecutive year of 100% detection.

**CrowdStrike did not participate** in the 2024 evaluation. In the 2023 evaluation, CrowdStrike's technique detection outperformed SentinelOne's on that year's specific scenarios. The 2024 non-participation means no direct year-over-year comparison is available.

**2025 MITRE evaluation:** Both CrowdStrike and SentinelOne withdrew from the 2025 evaluation. CrowdStrike's own comparison page claims SentinelOne achieved "only 50% protection score with 7 false positives in the most recent

MITRE test in which SentinelOne participated", though this refers to the prevention evaluation, not the detection evaluation, and the framing reflects vendor marketing rather than neutral independent analysis.

**The honest MITRE conclusion:** The most current independent evaluation data available favors SentinelOne on detection completeness and alert efficiency. Both vendors' 2025 withdrawal means 2024 data is the last clean independent benchmark available.

---

# Pricing Reality (June 2026)

## CrowdStrike Falcon

| Tier | Price | EDR Included |
|---|---|---|
| Falcon Go | $59.99/device/year | No |
| Falcon Pro | $99.99/device/year | No |
| Falcon Enterprise | $184.99/device/year | Yes |
| Falcon Complete MDR | $200-$400/device/year (typical) | Yes |

Enterprise procurement data puts the median CrowdStrike annual contract at approximately $53,500, with buyers averaging 22% savings below list price. Post-July 2024, buyers presenting SentinelOne competitive quotes have successfully negotiated 20%-40% discounts on renewals.

## SentinelOne Singularity

| Tier | Price | EDR Included |
|---|---|---|
| Singularity Core | ~$69.99/endpoint/year | No |
| Singularity Control | ~$99.99/endpoint/year | No |
| Singularity Complete | ~$179.99/endpoint/year | Yes |
| Singularity Enterprise | Custom | Yes |

PeerSpot enterprise practitioners report per-device costs typically ranging from $3 to $10 monthly at enterprise volume, reflecting significant discount from list pricing at scale. TrustRadius data positions SentinelOne at approximately one-fifth of CrowdStrike per endpoint at list pricing, though negotiated enterprise rates narrow this gap considerably. For smaller organizations, TrustRadius practitioners note minimum agent counts and annual billing requirements make the platform expensive below enterprise scale.

At the Singularity Complete / Falcon Enterprise tier, the platforms are within approximately $5/device/year of each other at list price. SentinelOne's pricing advantage is most pronounced at lower tiers and in large volume negotiations.

---

# The Decision Framework

## Choose CrowdStrike if:

- Your SOC has dedicated threat hunters who will use the depth of the Falcon console and OverWatch service
- Your environment is heavily Windows-centric and you require the most mature Windows detection

- You rely on a broad MSSP or integration partner ecosystem
- You have assessed the July 2024 architectural risk and have a documented remediation plan for a recurrence
- Budget is secondary to market-leading threat intelligence depth and ecosystem breadth

### Choose SentinelOne if:

- Autonomous response, detecting and remediating without cloud connectivity or human authorization, is operationally important
- You have a multi-OS environment requiring uniform coverage quality across Windows, Linux, and macOS
- File rollback capability for ransomware recovery is a priority
- Budget is a meaningful constraint, SentinelOne delivers comparable detection at materially lower cost, particularly for mid-market organizations
- You have assessed the May 2025 console outage and are satisfied that endpoint protection continuity during a management layer failure is acceptable

### The question both decisions require answering:

What is your organization's documented response plan if your EDR platform experiences a global outage? For CrowdStrike, that scenario means endpoint protection fails and manual device-by-device remediation is required. For SentinelOne, that scenario means console visibility is lost but endpoint protection continues. Both scenarios require planning. Neither vendor's marketing adequately prepares buyers for either.

Run a proof-of-concept against your actual environment, your OS mix, your SOC workflows, your existing integrations, before signing either contract.

---

## The Bottom Line

CrowdStrike and SentinelOne are the two platforms every serious enterprise EDR evaluation comes down to. Both are demonstrably best-in-class. Both have now experienced documented global outages. The nature of those outages differs materially, and that difference is the most important technical distinction in this comparison.

**CrowdStrike** wins on threat intelligence depth, Windows detection maturity, ecosystem breadth, and managed threat hunting scale. The July 2024 outage was categorically more severe than SentinelOne's May 2025 event, endpoints failed and required manual remediation at scale.

**SentinelOne** wins on autonomous response, cross-platform coverage, MITRE ATT&CK; consistency, pricing, and the architectural characteristic that endpoint protection continues even when console visibility fails. Its May 2025 outage revealed that no cloud-connected security platform is immune to management layer failures, a humbling data point given its prior marketing.

The one conclusion not defensible in 2026: evaluating either platform without a documented, tested response plan for what your organization does when your EDR platform experiences a global service interruption.

---