CyberArk vs. BeyondTrust vs. Delinea: The Privileged Access Management Verdict

Unvarnished Reviews Research

This report synthesizes data from 3,500+ verified user reviews and practitioner community posts collected from G2, Capterra, Gartner Peer Insights (1,117 CyberArk reviews, 847 BeyondTrust reviews, 1,550 Delinea reviews), PeerSpot, TrustRadius, Spiceworks, and Reddit r/netsec and r/sysadmin. Pricing data reflects practitioner-reported contract data, independent procurement analysis, and enterprise benchmark data 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

CyberArk is the market-leading privileged access management platform, holding 11.4% PeerSpot mindshare, deployed at over 50% of Fortune 500 companies, and the most comprehensive PAM capability set available. It is also, as of February 2026, an acquisition target completed by Palo Alto Networks for approximately $25 billion. Every organization signing a multi-year CyberArk contract in 2026 is signing with Palo Alto Networks' roadmap, pricing, and support priorities, not CyberArk's independent ones. The Broadcom/VMware parallel is not an overstatement: it is the most important procurement context in this evaluation.

BeyondTrust is the unified platform play, combining privileged password management, privileged remote access, and endpoint privilege management under a single vendor. Its Gartner Peer Insights rating (4.6 stars, 847 reviews) outpaces CyberArk's (4.4 stars, 1,117 reviews) and matches Delinea's. It is particularly strong for organizations where least-privilege enforcement on Windows and Linux endpoints is the primary use case alongside vault and session management.

Delinea (formerly Thycotic + Centrify) is the SaaS-first alternative that wins on usability, deployment speed, and mid-market TCO. Its Gartner Peer Insights score of 4.6 from 1,550 reviews, the largest review set of the three, reflects genuine user satisfaction from a platform that deploys in 6-12 weeks versus CyberArk's 12-20 weeks. For organizations that do not require CyberArk's enterprise complexity depth and are unwilling to accept the Palo Alto acquisition risk, Delinea is the most frequently recommended alternative.

The market context for all three: 74% of data breaches involve the human element (Verizon 2025 DBIR), and compromised privileged credentials remain the most valuable asset an attacker can obtain. PAM has moved from "security best practice" to "cyber insurance requirement", organizations without a deployed PAM solution are now routinely flagged during insurance underwriting.

The Most Important 2026 Development: Palo Alto Networks Acquires CyberArk

No honest 2026 PAM evaluation proceeds without addressing this directly.

Palo Alto Networks completed the acquisition of CyberArk in February 2026 for approximately $25 billion. CyberArk's subscription ARR was $1.08 billion as of Q2 2025, growing 61% year-over-year, with subscription revenues representing 80% of total revenue. This is a strategically significant and highly profitable acquisition for Palo Alto Networks.

What this means for buyers:

The product roadmap under new Palo Alto ownership has not been fully disclosed. Customers evaluating long-term contracts should factor in potential changes to pricing, support, and integrations. The relevant precedent: Broadcom's acquisition of VMware, while in a different software category, demonstrated what can happen to enterprise software pricing and packaging when a financially-oriented acquirer takes control of a market-dominant platform. CyberArk's installed base, over 50% of Fortune 500, more than 35% of Global 2000, gives Palo Alto Networks similar leverage to Broadcom's VMware position.

The machine identity pricing crisis adds urgency. CyberArk's own management acknowledged in Q1 2025 earnings that machine identities now outnumber human identities by more than 80:1, up from 45:1 just a year prior. As AI agents, automated systems, and workload-based architectures multiply, CyberArk acknowledged that traditional per-identity pricing will not scale. Management stated directly that customers will not pay premium prices for each machine or agent. How Palo Alto Networks resolves this pricing challenge, and at what cost to customers, is the most significant open question in the PAM market.

For organizations already on CyberArk: The installed base lock-in is real. CyberArk deployments are deeply integrated into infrastructure, replacing them involves months of migration effort and risk. The practical question is not whether to immediately migrate but whether multi-year renewal commitments are appropriate given roadmap uncertainty.

For organizations evaluating CyberArk new: Request explicit roadmap commitments from Palo Alto Networks, not from CyberArk legacy sales representatives. Get pricing protections in writing for the full contract term.

Platform Ratings at a Glance

Platform	Gartner Peer Insights	Reviews	PeerSpot Mindshare
CyberArk Privileged Access Manager	4.4 / 5	1,117	11.4% (#1)
BeyondTrust	4.6 / 5	847	Strong
Delinea	4.6 / 5	1,550	Strong

CyberArk's lower Gartner Peer Insights rating relative to BeyondTrust and Delinea, despite its market leadership position, reflects its implementation complexity, support quality variability, and pricing premium. BeyondTrust and Delinea tie on Gartner ratings with more satisfied user bases relative to their market segments. Delinea's 1,550 reviews is the largest of the three, reflecting both its installed base breadth and its relatively higher user willingness to review.

What PAM Actually Does: The Category Explained

Privileged access management controls who can access the most sensitive systems in an enterprise, the accounts with administrator, root, or service-level permissions that, if compromised, give attackers complete control. PAM addresses

four core capabilities:

Privileged Account Discovery and Vaulting: Automatically finding all privileged accounts across the environment and storing credentials in a secure vault, eliminating standing credentials and enabling just-in-time access.

Session Management and Recording: Recording every privileged session for audit, forensic, and compliance purposes. If an administrator takes a malicious or mistaken action, the recording provides the evidence trail.

Least-Privilege Enforcement: Reducing endpoint privileges to the minimum required for the task, removing administrator rights from standard users and granting temporary elevation only when needed.

Secrets Management: Managing API keys, tokens, certificates, and service account credentials used by applications and automated systems, the machine identity problem that is growing 80:1 versus human identities.

Architecture and Deployment: The Most Consequential Difference

The deployment complexity difference between the three platforms is the finding that most determines real-world outcomes, and the one most underdisclosed in pre-sale conversations.

CyberArk: Requires a dedicated infrastructure team with Windows Server administration experience. A minimal production setup involves a Digital Vault (isolated Windows Server, often air-gapped), a Central Policy Manager, a Password Vault Web Access server, and typically a Privileged Session Manager. CyberArk's own documentation recommends engaging a certified implementation partner. A typical mid-size enterprise deployment covering 200-500 privileged accounts runs 12-20 weeks and carries ongoing maintenance overhead. Practitioners specifically document that implementation projects stall when organizations underestimate the infrastructure requirements and specialized skills needed to operate the Digital Vault.

Delinea: Moderate complexity. Secret Server can be deployed on a single Windows server for smaller environments, with cloud-native deployment available. Typical enterprise timeline: 6-12 weeks for equivalent scope. The AD bridge component for Linux/Unix adds 2-4 weeks.

BeyondTrust: Varies by product. Password Safe is comparable to Delinea in complexity. Privilege Management for desktops is relatively straightforward (4-8 weeks). Full platform deployment: 8-14 weeks.

The honest implication: CyberArk's deployment complexity is its biggest operational weakness. Organizations that choose CyberArk without a certified implementation partner and without dedicated CyberArk-skilled staff consistently struggle with deployment timelines that extend 2-3x beyond initial estimates. The platform's capabilities are genuine, they require genuine investment to unlock.

What Users Actually Report

CyberArk: What Works

PeerSpot and Gartner reviewers consistently praise CyberArk's breadth, depth, and security architecture. The Digital Vault's tamper-proof credential storage, automatic credential rotation, and session recording capabilities are described as the most mature implementations in the category.

G2 reviewers specifically call out CyberArk's ability to secure connections without revealing credentials and its integrated multi-factor authentication as competitive differentiators. For enterprises with complex hybrid infrastructure spanning on-premises, multi-cloud, and OT/ICS environments, CyberArk's coverage breadth is unmatched.

CyberArk's Secure AI Agent, launched in 2025, addresses the machine identity challenge directly, managing the credentials and permissions of AI agents and automated workloads. With machine identities outnumbering human identities 80:1 in enterprise environments, this capability addresses the PAM market's most pressing emerging challenge.

The Venafi acquisition (machine identity management) and Zilla Security acquisition (identity governance) have extended CyberArk's platform into adjacent identity security categories, making it increasingly a broader Identity Security platform rather than a point PAM solution.

CyberArk: What Doesn't Work

Support quality is the most consistent complaint. PeerSpot documents that CyberArk's support receives mixed reviews, praised for expertise but criticized for delays, especially at Tier One. Practitioners describe initial support contacts as slow to escalate, with resolution timelines extending beyond acceptable windows for security incidents.

Implementation complexity and cost. CyberArk deployments require certified implementation partners, a cost that is not on the license page and is not optional for complex environments. Post-Palo Alto acquisition, the availability and cost of certified CyberArk implementation partners is an open question.

Palo Alto acquisition uncertainty. This is the most significant documented complaint in 2026 practitioner communities: organizations that signed multi-year CyberArk contracts before February 2026 are now evaluating whether renewal terms will change under Palo Alto ownership. The product roadmap under new ownership has not been fully disclosed.

BeyondTrust: What Works

G2 reviewers consistently praise BeyondTrust's session recording and approval processes, centralized management of user roles and permissions, and the quality of its unified platform. The centralized management features are specifically described as more robust than CyberArk's for administration and oversight, a finding consistent with BeyondTrust's higher Gartner Peer Insights rating.

BeyondTrust Password Safe is praised for quick setup, strong compliance features, and favorable executive-level reviews. The platform's Privileged Remote Access capability, purpose-built for vendor and contractor access management, is the strongest in this category of the three platforms.

Practitioners specifically document strong global support availability and efficiency for BeyondTrust Password Safe, a direct contrast to CyberArk's support quality complaints.

BeyondTrust: What Doesn't Work

Documentation gaps are the most consistent complaint, specifically around User Verification and UVM configuration. PeerSpot practitioners document that documentation quality does not match the platform's complexity for advanced configurations.

Product breadth creates integration complexity. BeyondTrust's unified platform, spanning Password Safe, Privileged Remote Access, and Endpoint Privilege Management, is a strength for organizations that buy the full suite.

For organizations that want point solutions, the integration between modules requires planning and expertise.

Delinea: What Works

Gartner Peer Insights reviewers, 1,550 reviews, the largest of the three, consistently praise usability, deployment speed, and support quality. Delinea's Secret Server is described as deployable on a single Windows server for smaller environments and available in cloud-native configuration for larger ones, the most accessible deployment of the three.

Delinea's support is specifically documented as responsive and expert, with minor issues resolved efficiently. This is the sharpest contrast to CyberArk's Tier One support complaints, Delinea's support quality is its most consistent competitive advantage in practitioner reviews.

For mid-market organizations, typically 500-5,000 employees without dedicated PAM engineering teams, Delinea's balance of capability and operational simplicity is specifically validated in practitioner communities as the right TCO choice.

Delinea: What Doesn't Work

Advanced analytics and threat detection are specifically called out as less extensive compared to CyberArk. For organizations where behavioral analytics, threat detection, and deep session intelligence are security requirements, Delinea's capabilities trail CyberArk.

Integration complexity with some services is noted by PeerSpot reviewers, specifically that professional services costs are higher than expected and that integration projects carry more friction than initial sales conversations suggest.

Pricing. PeerSpot reviewers describe Delinea Secret Server as enhancing security and efficiency but "pricier" than expected for what it delivers, with mixed financial benefits reported across different deployment sizes.

Pricing Reality (June 2026)

All three platforms use custom enterprise pricing, no published list prices. The following reflects practitioner-reported and independently researched estimates.

CyberArk

CyberArk does not publish pricing. Enterprise deployments are typically priced per account/identity managed, with platform modules (Vault, Session Manager, Endpoint Privilege Management, Secrets Manager) each carrying separate licensing.

Practitioner-reported ranges:

- Mid-market (200-500 accounts): $50,000-$150,000/year
- Enterprise (1,000-5,000 accounts): $150,000-$500,000+/year
- Implementation partner cost: $50,000-$200,000+ (not included in license)
- Ongoing CyberArk-skilled staff: $100,000-$150,000+/year salary equivalent

The machine identity pricing uncertainty: CyberArk's acknowledgment that per-identity pricing will not scale for machine identities at 80:1 ratios means current pricing models for AI-heavy environments are in flux. Organizations deploying significant AI agent infrastructure should explicitly negotiate machine identity pricing terms before signing.

Post-acquisition note: Under Palo Alto Networks ownership, pricing authority and renewal terms are controlled by Palo Alto's enterprise sales structure. Request explicit price protection for the full contract term in writing.

BeyondTrust

BeyondTrust uses modular pricing across its product lines. Practitioner-reported estimates:

- Password Safe: $30,000-$100,000+/year depending on account count
- Privileged Remote Access: $10,000-$50,000+/year depending on user count
- Full platform: $80,000-$250,000+/year for enterprise deployments
- Implementation: 8-14 weeks; professional services $20,000-$80,000

Delinea

Delinea Secret Server pricing is the most accessible entry point of the three:

- Cloud edition: from approximately $15,000-$30,000/year for smaller deployments
- Enterprise: $50,000-$200,000+/year depending on scope
- Implementation: 6-12 weeks; typically lower professional services cost than CyberArk

The negotiating principle for all three: Run a competitive evaluation involving all three before signing any single vendor. Competitive quotes from BeyondTrust and Delinea have historically produced 20%-35% CyberArk discounts. Under Palo Alto ownership, test whether this leverage still applies, and document the answer before removing competing bids from the negotiation.

The Decision Framework

Choose CyberArk if:

- Your organization is large enterprise (5,000+ employees) with complex hybrid infrastructure spanning on-premises, multi-cloud, and OT/ICS
- Comprehensive PAM coverage depth, vaulting, session management, endpoint privilege, secrets management, machine identity, from a single vendor is the requirement
- You have or are hiring dedicated CyberArk-certified staff, and have budgeted for a certified implementation partner
- You are already deployed on CyberArk and migration cost avoidance justifies renewal
- You have requested explicit roadmap commitments and pricing protection from Palo Alto Networks for the full contract term
- Your organization already runs Palo Alto Networks security products and the acquisition creates genuine platform integration value

Choose BeyondTrust if:

- Least-privilege enforcement on Windows and Linux endpoints is a primary use case alongside vaulting
- Vendor and contractor privileged remote access management is a significant requirement
- You want a unified platform covering password management, remote access, and endpoint privilege under one vendor without CyberArk's implementation complexity

- Support quality at Tier One is operationally important, BeyondTrust's global support availability is documented as superior to CyberArk's

Choose Delinea if:

- Your organization is mid-market (500-5,000 employees) without a dedicated PAM engineering team
- Deployment speed matters, 6-12 weeks to production versus CyberArk's 12-20 weeks
- You want the lowest enterprise TCO of the three for comparable core PAM capabilities
- Support quality is a priority, Delinea's practitioner-documented support is the strongest of the three
- You are evaluating CyberArk alternatives specifically due to the Palo Alto acquisition uncertainty

The Palo Alto test before signing CyberArk:

Before signing or renewing any CyberArk contract, get written answers to four questions from Palo Alto Networks (not from CyberArk sales):

1. Will pricing terms change at renewal?

2. Which CyberArk product roadmap commitments does Palo Alto Networks guarantee for the contract term?

3. How will CyberArk-certified implementation partner availability and pricing be maintained?

4. What is the machine identity pricing model for AI agent deployments at scale?

The Bottom Line

CyberArk, BeyondTrust, and Delinea are all credible enterprise PAM platforms. The right choice is not about which has the most features, it is about deployment complexity, support quality, total cost of ownership, and the unprecedented acquisition context that makes 2026 CyberArk evaluations fundamentally different from any previous year.

CyberArk remains the most capable and most widely deployed PAM platform. The Palo Alto Networks acquisition is the single most important procurement context for any 2026 evaluation, not the product's features. Request roadmap and pricing commitments in writing from Palo Alto Networks before signing. The parallel to Broadcom/VMware is the right frame of reference.

BeyondTrust wins on unified endpoint and remote access privilege management, Tier One support quality, and the ability to consolidate multiple PAM use cases under one vendor without CyberArk's implementation overhead.

Delinea wins for mid-market organizations that need production-ready PAM in weeks rather than months, lower TCO than CyberArk, and the highest practitioner-documented support quality of the three. As CyberArk evaluation uncertainty grows post-acquisition, Delinea is the most consistently recommended enterprise alternative in practitioner communities.

The universal starting point for any PAM evaluation in 2026: define whether your primary use case is human privileged accounts, machine/service account secrets management, endpoint privilege enforcement, or vendor remote access, because the platform that leads in each category is not always the same one. Map your use cases before evaluating vendors.

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.
