Okta vs. Microsoft Entra ID: The Identity Platform Verdict

Unvarnished Reviews Research

This report synthesizes data from 1,500+ verified user reviews and practitioner community posts collected from G2, Capterra, TrustRadius, PeerSpot, Spiceworks, and Reddit practitioner communities. Pricing data reflects vendor pricing pages, verified purchase 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

Microsoft Entra ID is the most appropriate choice for the majority of enterprise organizations, specifically any organization running Microsoft 365. For M365 E5 customers, Entra ID P2 is included at effectively zero incremental cost, delivering SSO, MFA, identity governance, and privileged identity management. TrustRadius data confirms that 26% of Entra ID reviewers specifically cite cost savings from licensing consolidation within existing Microsoft subscriptions as a primary benefit. The capability gap versus Okta has narrowed substantially in 2024-2026. Its primary limitation, hybrid environment complexity, affects 44% of deployments and is specifically documented in TrustRadius reviews.

Okta is the most appropriate choice for organizations with complex, multi-vendor environments where identity must bridge hundreds of applications across many different vendors, where Okta's 7,000+ pre-built integrations, superior workflow automation, and platform-neutral architecture deliver value that Entra ID cannot match for non-Microsoft workloads. Okta is also the platform with a documented security breach cascade between 2022 and 2024 whose trust recovery the company's own leadership describes as incomplete. The SSO tax, where SaaS vendors charge 15% to over 100% more per user when connected via third-party SSO, can multiply the sticker price by 10x or more and is the most undisclosed cost in identity platform procurement.

A notable market signal: both platforms are losing PeerSpot mindshare as of April 2026, Entra ID from 28.6% to 16.8% and Okta from 14.0% to 8.9% in the IAMaaS category. JumpCloud and other challengers are gaining ground in the mid-market. Neither incumbent should be evaluated without assessing the emerging alternatives.

Platform Ratings at a Glance

Platform	G2	TrustRadius	PeerSpot (CIAM)
Microsoft Entra ID	4.5 / 5	4.5 / 5	8.3 / 10
Okta Workforce Identity	4.5 / 5	4.5 / 5	8.6 / 10

Both platforms rate identically at 4.5/5 on G2 and TrustRadius, reflecting genuine market-leading capability from both. In the Customer Identity and Access Management category specifically, Okta holds the #1 PeerSpot ranking with 13.3% mindshare versus Microsoft's 3.4%, a category where Okta's CIC/Auth0 platform genuinely leads. For

workforce identity, the ratings converge, and the decision comes down to ecosystem fit, budget, and documented security history.

The Okta Security Incident Record: Mandatory Context

No honest 2026 review of Okta proceeds without addressing its security history directly. Between 2022 and 2024, Okta experienced a cascade of serious security incidents.

January 2022, Lapsus$ Breach: Hacker group Lapsus$ compromised Okta's systems through a third-party support provider (Sitel). Okta did not disclose the breach until months after it occurred, only after Lapsus$ shared screenshots of Okta's internal systems publicly. The delayed disclosure damaged enterprise customer trust significantly. 366 customers were affected.

December 2022, Source Code Theft: Attackers stole Okta's source code, exposing the authentication platform's blueprint.

September/October 2023, MGM and Caesars via Okta: High-profile attacks on MGM Resorts and Caesars Entertainment exploited Okta super-administrator accounts through social engineering. MGM's recovery costs exceeded $100 million.

October/November 2023, Customer Support System Breach: Attackers accessed Okta's customer support management system and downloaded a report containing the names and email addresses of all Okta customer support system users, affecting 100% of the customer base. Okta's own SEC filing from November 2023 confirmed this scope. Okta initially downplayed the incident before the full scope was disclosed.

October 2024, Authentication Bypass: A security flaw allowed unauthorized access by bypassing username-based authentication.

Financial consequence: Okta agreed to pay $60 million to settle a shareholder lawsuit over its handling and disclosure of the 2022 breaches.

Trust recovery status: Okta's own CISO acknowledged in early 2024 that the brand "built up over a decade" had been "tarnished" and that the company had not yet "bounced back." Okta's FY2026 10-Q filed with the SEC explicitly lists "cybersecurity incidents" as an ongoing risk factor, standard legal disclosure, but notable in the context of recent history.

Okta has implemented architectural changes post-2024 and has not experienced a major breach since October 2024. For enterprise security teams, the due diligence question is not whether Okta is appropriate, it may well be, but whether the specific architectural changes implemented post-2024 have been independently verified for the use case under evaluation.

Architecture: The Fundamental Difference

Okta: Platform-Neutral Identity

Okta was built as an independent identity layer that sits between users and applications, not privileging any particular vendor's ecosystem. Its 7,000+ pre-built application integrations cover the full spectrum of enterprise SaaS,

on-premises, and custom applications. Okta Workflows provides no-code identity workflow automation for complex provisioning and lifecycle management across heterogeneous environments.

In environments where identity must bridge Salesforce, Workday, AWS, Google Workspace, hundreds of SaaS tools, and custom applications simultaneously, Okta's platform-neutral architecture delivers consistency that Microsoft's ecosystem-centric approach cannot match for non-Microsoft workloads. PeerSpot reviewers specifically cite Okta's flexibility and comprehensive feature set as superior in environments requiring diverse application integration.

Microsoft Entra ID: Ecosystem-Integrated Identity

Entra ID was built as the identity foundation of the Microsoft ecosystem. It integrates at the deepest level with Azure, Microsoft 365, Dynamics 365, Power Platform, Intune, and the full Microsoft security suite. TrustRadius data shows Entra ID functioning as the identity provider for 72% of non-Microsoft applications in reviewed deployments, demonstrating that its reach extends meaningfully beyond the Microsoft stack, though with less pre-built integration depth than Okta for non-Microsoft environments.

The Conditional Access integration with Intune, Defender, and Microsoft Purview, enforcing device compliance and risk signals in real time across the full security stack, is a genuine architectural advantage for Microsoft-first organizations that Okta cannot replicate natively.

What Users Actually Report

Microsoft Entra ID: What Works

TrustRadius reviewers identify three consistent areas of strength: Conditional Access policies (cited by 21% of reviewers), MFA implementation (18%), and broad integration capabilities with both Microsoft and third-party services (18%). The security outcomes, reduced unauthorized access, enhanced compliance posture, and streamlined user provisioning, are well-documented across both TrustRadius and G2.

Cost savings are the most cited business impact: 26% of TrustRadius reviewers specifically reference licensing consolidation within existing Microsoft subscriptions as a primary benefit. PeerSpot enterprise practitioners document approximately 30% efficiency savings in some deployments by eliminating VPN channels and enabling direct Azure server access through Entra's Zero Trust model.

Microsoft Entra ID: What Doesn't Work

Hybrid environment complexity is the primary documented limitation. TrustRadius review data shows 44% of Entra ID deployments are hybrid, synchronizing identities between on-premises Active Directory and cloud, and reviewers specifically flag "configuration complexity when integrating with older on-premises Active Directory systems" as the most common friction point. Practitioners in Spiceworks and TrustRadius communities recommend bypassing hybrid join in favor of full Entra ID join where possible, but note that legacy systems frequently make this impractical.

Non-Microsoft application integration depth trails Okta for organizations with large non-Microsoft SaaS portfolios. While Entra ID supports 72% of non-Microsoft applications as an identity provider in reviewed deployments, the pre-built connector quality and automation depth for non-Microsoft apps is consistently described as less mature than Okta's.

Admin portal navigation complexity is a secondary complaint, the breadth of Microsoft's product surface creates navigation complexity for identity administrators who are not deep Microsoft specialists.

Okta: What Works

PeerSpot and TrustRadius reviewers consistently praise Okta's application catalog depth, workflow automation flexibility, and platform neutrality. In Customer Identity specifically, Auth0/CIC, Okta holds the #1 PeerSpot ranking with 95% of users willing to recommend the platform, versus 87% for Microsoft. For customer-facing application authentication, Okta's CIC platform genuinely leads the category.

Okta's efficiency gains are documented in TrustRadius: centralized security, automated lifecycle features, and accessibility improvements despite customization limits. Organizations that successfully implement Okta for complex, multi-vendor environments report meaningful productivity gains from eliminating per-application credential management.

Okta: What Doesn't Work

The SSO tax is the most significant and least disclosed cost in Okta procurement. Independent pricing analysis documents that SaaS vendors charge 15% to over 100% more per user when connected via third-party SSO. For a 100-person company using 80 SaaS tools, the true annual Okta cost reaches $220,400 compared to the $20,400 sticker price, a 10x multiplier driven by SaaS subscription upgrades across the portfolio. HubSpot is a specific documented example: the standard plan at $9,600/year jumps to $43,200/year when SSO integration is required. This is not Okta's fault, it is the SaaS vendor ecosystem's pricing structure, but it is a cost that flows directly from the decision to implement Okta, and it is almost never modeled in procurement business cases.

Complex pricing structure. Okta's a la carte module pricing, SSO, Adaptive SSO, MFA, Adaptive MFA, Universal Directory, Lifecycle Management, API Access Management, Workflows, and Identity Governance each priced separately, creates a total cost that consistently surprises buyers at renewal. Verified purchase data puts the median Okta customer cost at approximately $43,840/year with only 14% average discount from list, meaningfully less negotiating leverage than CrowdStrike or Zscaler.

Post-breach trust deficit. Even with no major breach since October 2024, regulated industries, financial services, healthcare, government, are now requiring documented architectural change verification in Okta contract negotiations that were not standard before 2022.

Mindshare declining. Okta's PeerSpot IAMaaS mindshare fell from 14.0% to 8.9% year-over-year as of April 2026. In a growing market, this decline indicates competitive displacement, primarily by JumpCloud in the mid-market and by Entra ID in Microsoft-stack enterprise environments.

Pricing Reality (June 2026)

Microsoft Entra ID

Plan	Price	Included In
Free	$0	All M365 plans
P1	$6/user/month	M365 E3, Business Premium

P2	$9/user/month	M365 E5 (zero incremental)
Entra Suite	$12/user/month	P2 + Governance + Private Access

The near-zero cost reality for E5 organizations: For organizations already on M365 E5, Entra ID P2 carries zero incremental licensing cost. Switching to Okta means paying $17/user/month for Essentials, approximately $1M+ annually for a 5,000-user organization, on top of existing E5 spend, not instead of it.

For E3 organizations: Entra P2 available as add-on at $9/user/month vs. Okta Essentials at $17/user/month, a 47% licensing cost advantage before SSO tax and implementation are factored.

Okta Workforce Identity

Plan	Price	Key Capabilities
Starter	$6/user/month	SSO, MFA, Universal Directory, 5 workflows
Core Essentials	$14/user/month	Adds Adaptive MFA, basic lifecycle
Essentials	$17/user/month	Full lifecycle, 50 workflows, privileged access
Professional/Enterprise	Custom	Advanced governance, dedicated support

The true cost calculation:

- Okta Essentials at $17/user/month: $204,000/year for 1,000 users at list
- Median verified customer cost: approximately $43,840/year (reflects typical mid-size deployment)
- Implementation and professional services: $30,000-$100,000
- SSO tax across SaaS portfolio: 10x sticker price possible at scale
- Annual contract minimum: $1,500, no month-to-month option
- Average negotiated discount: 14% off list (less leverage than most enterprise security vendors)

Negotiating principle: Running a credible Entra ID evaluation against Okta, even when Okta is the preferred outcome, remains the most effective lever for improving Okta commercial terms. The 14% average discount can expand meaningfully with a documented competitive alternative.

TCO Comparison: 1,000-User Enterprise

Component	Okta Essentials	Entra ID P2 (E5 org)	Entra ID P2 (E3 + add-on)
Identity license	$204,000/yr	$0 incremental	$108,000/yr
Implementation	$30,000-$100,000	$10,000-$40,000	$15,000-$50,000
SSO tax (SaaS portfolio)	Significant, model explicitly	Minimal	Minimal
Admin overhead	Moderate	Low for M365 admins	Low for M365 admins
Year 1 Total	**$264,000-$354,000+**	**$10,000-$40,000**	**$123,000-$158,000**

The TCO gap for E5 organizations is among the largest in any enterprise software category. For E3 organizations, Entra P2 at $9/user/month produces a 47% licensing cost advantage over Okta Essentials before SSO tax, implementation, and ongoing operational costs are considered.

The Decision Framework

Choose Microsoft Entra ID if:

- Your organization runs Microsoft 365, particularly E3 or E5
- 70%+ of your applications are Microsoft (M365, Azure, Dynamics, Power Platform)
- Cost savings from licensing consolidation are a business priority
- Your IT team already manages Microsoft environments and can extend expertise to Entra
- Your environment is cloud-native or willing to bypass hybrid join for new deployments
- Conditional Access integrated with Defender, Intune, and Purview is a security priority
- You are in a regulated industry where a unified Microsoft compliance stack simplifies audit

Choose Okta if:

- Your environment is genuinely multi-vendor, significant non-Microsoft SaaS, AWS, Google Workspace, and custom applications requiring deep integration
- Workflow automation for complex identity lifecycle across heterogeneous systems is a core requirement
- You need Customer Identity Cloud (Auth0) for customer-facing applications, Okta's CIC leads this category
- Your Microsoft 365 footprint is minimal and Entra ID ecosystem value does not apply
- You have conducted documented post-breach architectural due diligence and are satisfied with remediation
- You have explicitly modeled the SSO tax across your full SaaS portfolio before signing

Consider JumpCloud if:

- You are a mid-market organization under 2,500 users without significant Microsoft or Okta investment
- You want directory-as-a-service, SSO, MDM, and MFA in a single platform at lower cost than either market leader
- PeerSpot and practitioner communities consistently identify JumpCloud as the most cited challenger gaining ground at the expense of both Okta and Entra ID

The Bottom Line

In 2026, identity is the control plane through which enterprise software, security, and compliance converge. The Okta vs. Entra ID decision shapes vendor lock-in, security posture, and software economics for years.

Microsoft Entra ID wins on TCO for any Microsoft 365 organization, particularly E5, on Microsoft ecosystem integration depth, and on the simplicity of a single-vendor security stack. Its hybrid environment complexity is real and documented. Its capability gap versus Okta has narrowed to the point where the TCO advantage alone justifies it for most Microsoft-stack organizations.

Okta wins on application catalog breadth for non-Microsoft environments, workflow automation flexibility, and Customer Identity. It carries a meaningful price premium, a post-breach trust deficit that its own leadership acknowledges, and a hidden SSO tax that most procurement analyses fail to model accurately.

The single most important action before signing either platform: calculate the SSO tax explicitly across your actual SaaS portfolio. The Okta license cost is the entry price. The SSO tax is where the real financial exposure lives, and it is almost never in the business case.

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.