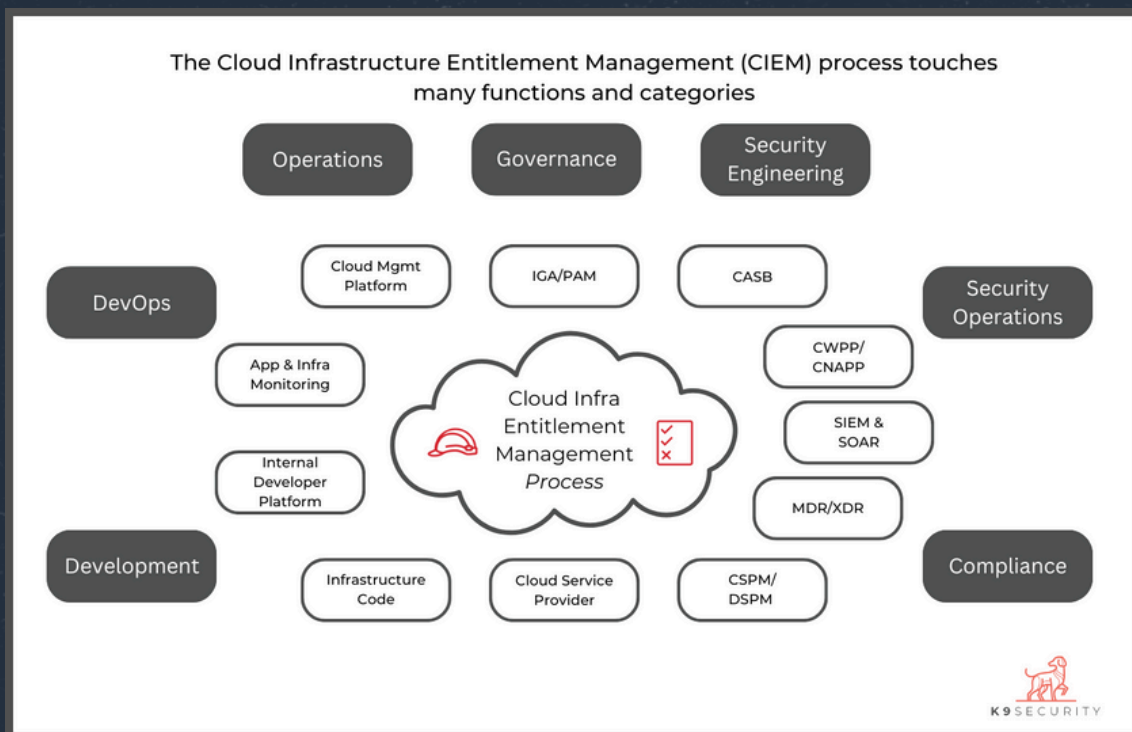


k9 Security CIEM Adoption Market Research Brief November 2024

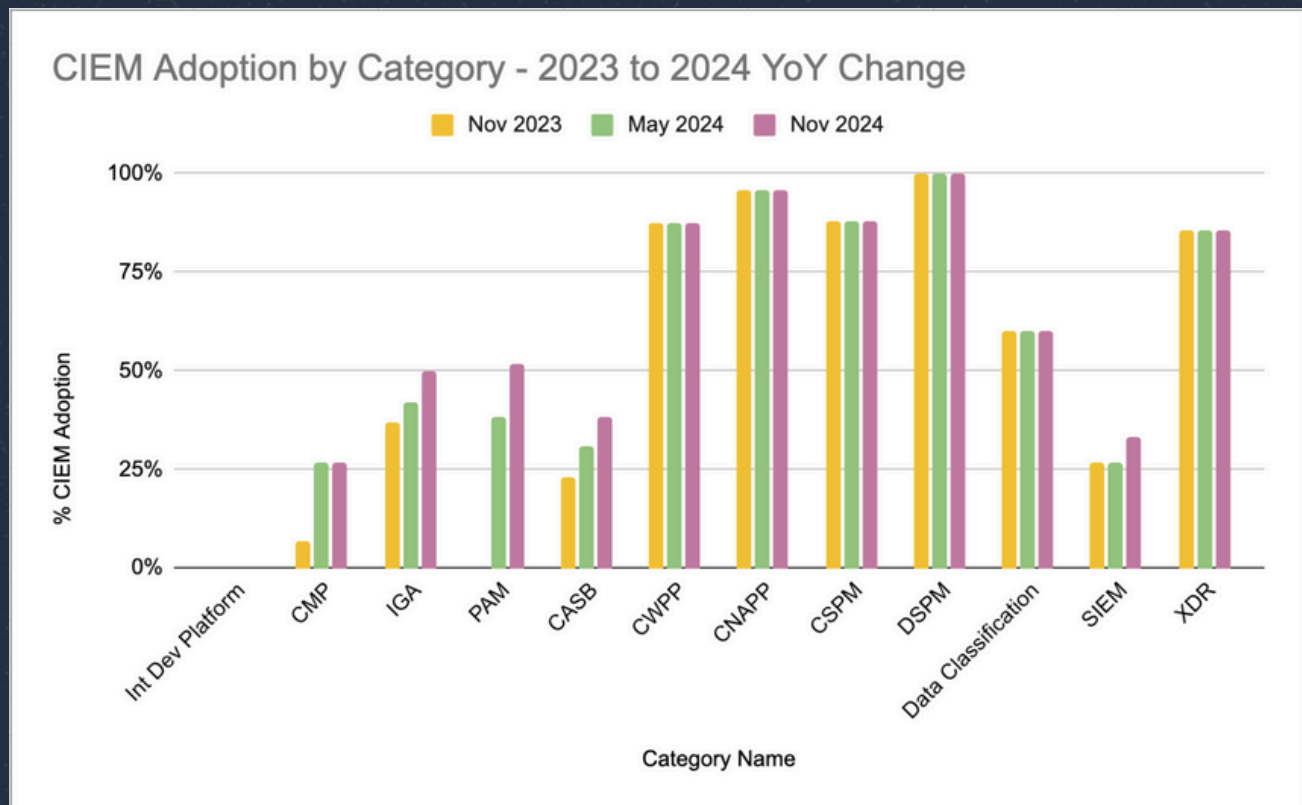


Cloud Infrastructure Entitlement Management (CIEM) continues to see increasing adoption across the cloud security market, reflecting its essential role in securing modern cloud environments. This market analysis shows how CIEM is expanding- from supporting security operations use cases into security engineering, access governance, and cloud management. CIEM has evolved from a specialized capability to a foundational element of cloud security products.



Market Adoption by Category

Here's how CIEM has propagated through the cloud security market over the past year:



Key Insights

Most notably, year-over-year trends show CIEM integrating into long-established categories:

- Cloud Management Platforms: 27% (4/15 vendors), +20pp YoY
- Cloud Access Security Brokers (CASB): 38% (5/13 vendors), +15pp YoY
- Privileged Access Management (PAM): 52% (14/27 vendors), +14pp YoY
- Identity Governance & Administration (IGA): 50% (10/20 vendors), +13pp YoY



Meanwhile, categories like DSPM, CSPM, and CWPP are all stable at high levels of adoption. This reflects CIEM being included into DSPM & CNAPP by definition. Furthermore, most CSPM and CWPP products are part of a CNAPP suite.

However, Internal Developer Platform (IDP) remains at 0/14 vendors—a seemingly untapped opportunity to shift security left and empower developers with access controls earlier in the development lifecycle.

CIEM-enabled Use Cases by Category

We found that CIEM capabilities are enabling multiple critical use cases for multiple technology roles. The key use cases are: resource discovery, access provisioning, risk assessment, security monitoring, and compliance reporting.

Use case	Cloud Management	Governance & Security Engineering	Security Operations & Compliance
Resource Discovery	✓	✓	✓
Access Provisioning & Review	✓	✓	✓
Risk Assessment		✓	✓
Security Monitoring			✓
Compliance Reporting			✓

Resource Discovery: Map entitlements across identities, resources, and roles, providing clear visibility into "who has access to what" while uncovering hidden permissions and misconfigurations.

Access Provisioning and Review: Integrate entitlement context to automate least privilege enforcement, role adjustments, and Just-in-Time access - ensuring all permissions align with organizational policies.



Risk Assessment: Correlate entitlements with user behavior, resource sensitivity, and operational needs to flag high-risk permissions, identify attack paths, and prioritize remediations.

Security Monitoring: Provide identity-aware context to enhance security alerts and detect anomalous access patterns - including privilege escalations and cross-cloud access attempts.

Compliance Reporting: Automate access reviews and tracks entitlement changes, generating audit-ready reports to ensure compliance with frameworks (ISO 27001, SOC 2, GDPR, Well-Architected)

What we think this means for Product Leaders

At k9 Security, we see these CIEM adoption trends highlighting both an opportunity and an imperative: the majority adoption in PAM (52%) and IGA (50%) signals that traditional identity security products must integrate CIEM quickly or risk falling behind.

For Product Leaders, especially in PAM and IGA companies, this isn't just about feature parity - it's about recognizing that cloud access entitlements are essential for making intelligent access decisions in cloud environments.

Clarence Hinton, Chief Strategy Officer at CyberArk, was quoted in their recent partnership announcement as saying:

"Cloud development is a primary driver of vast numbers of new human and machine identities that are being created every day, by different siloes within the organization and with differing – often unmanaged – permissions and access levels. For security teams to keep up, there is a need to rethink our approach to how these identities are discovered and secured so that this significant attack surface is understood and can be acted on."

Building CIEM capabilities requires significant investment in time and engineering resources. We've observed a significant portion of companies choosing to integrate CIEM capabilities from a partner to accelerate time to market and focus on core value.



What we think this means for MSPs

For Managed Service Providers, CIEM offers a strategic path to expand professional services revenue while solving critical client challenges. As organizations grapple with complex cloud permissions and scarce security expertise, MSPs can use CIEM capabilities to deliver high-value assessment, remediation, and governance services.

By leveraging CIEM data to identify risks and prioritize improvements, MSPs can create compelling professional service engagements that increase revenue and deliver promised security outcomes for customers. MSPs are well-positioned to offer specialized expertise in optimizing and managing identity and data security, turning technical complexity into service opportunities.

Looking Forward: AI-Enhanced CIEM Products and Services

We expect the integration of AI with CIEM capabilities to drive a critical evolution in cloud security. For Product Companies, especially PAM and IGA vendors, AI will transform existing entitlement data into a strategic asset. Through integration partnerships, vendors will be able to automatically detect excess or unintended permissions, map complex relationships between traditional and cloud-native access models, and provide context-aware recommendations for right-sizing permissions - all without the costly effort of building from scratch. This will allow them to extend their existing frameworks while helping customers manage the growing complexity of cloud permissions.

For Managed Service Providers, AI-enhanced CIEM capabilities will revolutionize service delivery. By automatically contextualizing and prioritizing findings based on risk and business impact, AI will help MSPs generate actionable client recommendations and vastly improve security service economics. We anticipate AI-assisted remediation workflows will help MSPs meet SLA commitments while scaling their expertise across more clients. This combination of intelligent automation and predictive analysis will enable MSPs to shift from reactive troubleshooting to proactive risk management and governance, maintaining consistent service delivery even as cloud environments grow more complex.



We believe the convergence of AI and CIEM will address a fundamental industry challenge: delivering better cloud security with constrained resources. And major players in the industry seem to agree; when the Identity at the Center podcast spoke to Andrew Moore, VP Product at SailPoint, regarding what's on the horizon in the world of identity security, he said:

"I think what [AI is] going to enable us to do more than anything else is be less fearful about the proliferation of accounts and access and to really find needles in a haystack fast."

Product companies will be able to quickly expand their capabilities through strategic integration rather than costly development, while service providers can focus on strategic guidance by leveraging AI for routine analysis and remediation. This powerful combination should help organizations improve their security posture despite the industry-wide shortage of security expertise, making robust cloud security more accessible for enterprises of all sizes.

Conclusion

The integration of CIEM capabilities into established categories like Privileged Access Management (PAM) and Identity Governance & Administration (IGA) demonstrates its growing importance in modern cloud security strategies by enhancing workflows such as access provisioning, risk assessment, and compliance reporting.

CIEM is transforming these domains into more proactive and dynamic security frameworks and are being enhanced by AI-driven advancements such as automated policy enforcement and entitlement graph analysis.

These improvements enable organizations to better align with Zero Trust principles, while also increasing efficiency and scalability. CIEM's integration into PAM and IGA will also set enterprise user's expectations that access entitlements should be available when making access decisions and shape the next generation of identity-aware, cloud-native security solutions.

