


# Jumping into the Cloud for AI

**David Norfolk** ©Bloor Research November 2026

ARTICLE REPRINT

***JumpCloud* is transforming from a useful cloud-based directory platform for identity management. into what it sees as a unified access control plane. Its key drivers for growth appear to be Active Directory displacement, sport for strategic partner ecosystems, and expanding AI governance capabilities.**

I was talking to JumpCloud because I think that what it offers is, or could be, important at the business outcome level, in a world where AI agents are first-class players on the team with humans but laws mandating human accountability still apply. What JumpCloud potentially offers is a must-have for the business, not just another toy for the IT group.

**My takeaways from meeting them are that:**

- JumpCloud has a reasonably global scale and market reach, making it a significant player, although its current success comes largely from smaller customers, I think, and it is just starting to expand into bigger enterprises. It does have some large customer successes, however.
- Its enterprise expansion is significantly powered by replacing legacy Microsoft Active Directory (AD) infrastructure, offering a modern, cloud-native identity and access solution. That is probably a good idea as, although AD has improved over time, it was never my favourite directory service.
- Most important is its strategic partnership with Google and support for Google's ***Workplace Transformation***. JumpCloud serves as the identity and device management engine that helps enterprise clients transition from Microsoft 365 to Google Workspace. That is a very political relationship: some people like Microsoft 365 (I don't), some people like Google Workspace (I do). Neither are perfect – but JumpCloud might have difficulty selling into companies where the CEO has drunk deeply of the Microsoft Kool-Aid.
- The JumpCloud platform unifies identity, access, endpoint device management, and SaaS/AI management into a single control plane, enabling businesses to replace several stand-alone vendors. That is, on the face of it, a good idea but there are a couple of provisos: **1)** Are the JumpCloud products good enough compared to the stand-alone competition; **2)** Can it integrate effectively with the products from stand-alone vendors, so as to support an incremental upgrade journey for large customers? Bearing in mind that in very large multinational customers it may never entirely replace the existing stand-alone products.
- Recent JumpCloud product additions focus on Shadow AI discovery, MCP management, token usage tracking, and provisioning distinct identities for AI agents alongside human users. This, I think, ties in with Bloor's views, that AI agents and human users are equivalent and a particular task may be given to an AI agent and then transition back to a human and vice versa. Bloor thinks that the attributes of AI agents largely overlap with human agents but do include specific attributes – especially around accountability (humans can be accountable, AI agents can't be, yet anyway, except through a relationship to the person "sponsoring" an AI agent). AI agents will have relationships to tech support, warranties, suppliers etc. whereas a human has analogous relationships to training, HR etc.
- I think that perhaps one key issue for what is essentially a value-added directory service such as JumpCloud is the maintenance of relationships. So, if JumpCloud manages identity, access, endpoint device management, and SaaS/AI management, it needs to manage relationships between these things, ideally up to the business outcome level. If the organisation is involved in Widget Production, say, which identities are accountable for widget quality, which AIs are essential for widget production and which just provide the icing on the cake, which human identities interact with which AI agents, which endpoint devices can be used by which human identities – or AI agents? And so on, and all these relationships may change with time. JumpCloud, I think, needs to assist with providing answers to questions like ***"Agentic AI ### has "gone rogue", which parts of widget production could be affected, which employees are accountable, who is responsible for building and training Agentic AI ###, where is Agentic AI ### deployed, if our customer sues us over the behaviour of Agentic AI ###, will our public liability insurance cover us"*** and so on. As an aside, the deployment of something like JumpCloud might well impact (reduce) the cost of liability insurance and the like, although this is probably in the future.




More generally JumpCloud seems to have a strong channel partner strategy, especially with Google, although I haven't room to go into details here. It is worth noting that roughly one-third of JumpCloud's overall business flows through channel partners, with a heavy concentration in the smaller business tier (10–50 users). JumpCloud embeds its core device management and SSO engines directly into broader HR and global workforce platforms (e.g., Deel global payments, compliance and HR; Electric AI for HR workflows). I like the integration into what is effectively an ecosystem for the organisation.

The implication of all this is JumpCloud provides business-level benefits (not necessarily by itself, but perhaps by using key partners) and should be sold primarily to the top management/compliance team, not just to the IT group – although the active buy-in of IT will be important, of course.

What is particularly new, and largely why I am writing this blog, is its AI gateway and agentic lifecycle management. It elevates AI agents from simple API keys or shared secrets to formal entities within JumpCloud's identity management framework – which is good. There are group-based access policies (admins can place AI agents into specific groups, assigning explicit permissions, app integrations, and target roles) and a designated human responsible individual is required for every created agent identity, in order to to maintain paper trails and legal accountability – this is very important, in my opinion.

More governance is provided by JumpCloud's lightweight OS Query device agent, used to scan endpoints for local AI applications and Model Context Protocol (MCP) connections. Nevertheless, note that AI Governance (which only has real meaning in the context of organisational governance generally, is an evolving thing. It may be dependent on the current legal frameworks, which may not be AI aware in every case – what makes logical sense is sometimes overwritten by what the law actually says. And, of course, once Artificial General Intelligence arrives (if it ever does), AI agents might have their own accountability.

I am not going to go into the details of JumpCloud governance enablement here, but I will note that it can surface real-time metrics on token consumption across models and platforms (e.g., AWS Bedrock, Gemini Enterprise), in order to mitigate the possibility of unanticipated usage costs appearing. I think that this could be a major initial "low hanging fruit" benefit from deploying JumpCloud, helping to justify the introduction of the product generally.

ARTICLE REPRINT

BLOOR RESEARCH

+44 (0)1494 311 460
info@Bloorresearch.com
www.Bloorresearch.com