FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

Reimagining Identity Security: How JumpCloud Is Building the Control Plane for the AI Era

An Interview with

Greg Keller

Co-founder and

Chief Technology Officer

JumpCloud

in conversation with

Adrian Drozd

Associate Partner & Global Practice

Area Leader, Frost & Sullivan

For more than a decade, JumpCloud has been challenging long-standing assumptions about how identity, access, and device management should function in modern enterprises. Long before identity became widely recognized as the central pillar of cybersecurity, JumpCloud was already building a unified, cloud-native platform designed for distributed workforces, heterogeneous devices, and Software as a Service (SaaS)-driven environments.

In this Transformational Growth Leadership (TGL) conversation, Adrian Drozd of Frost & Sullivan speaks with Greg Keller, Co-Founder and CTO of JumpCloud, about the company's origins, its platform-first philosophy, and how identity security is evolving in response to non-human identities, AI-driven automation, and global digital transformation. The discussion also explores JumpCloud's partnership strategy, recent acquisitions, geographic growth, and the leadership values that underpin Keller's approach.

Building a Unified Platform in a Fragmented World

Adrian Drozd: *Let's start with some background. JumpCloud pioneered the unified directory platform more than a decade ago. What motivated that vision, and how did it shape the early direction of the company?*

Greg Keller: When we founded JumpCloud in 2013–2014, the market was fundamentally structured around the assumption that identity management and device management were separate domains, each supported by different products, vendors, and operational philosophies. We believed that separation no longer reflected how modern companies actually worked.

Employees were already using cloud services, working across platforms, and operating in distributed environments. Binding identity to a single on-premise system felt outdated and restrictive. From the beginning, we were clear that JumpCloud would not be a tool or a standalone product. We wanted to build a platform, a unified control plane that treated identity and device as two sides of the same coin.

At the time, Microsoft Active Directory (AD) functioned as the gravitational center of enterprise IT. Entire ecosystems were built with the assumption that AD would always be the authoritative source of truth. But the companies I was building and working with didn't look like that. They were cloud-born, browser-native, globally distributed, and operating across Mac, Linux, and Windows environments. What was missing was a cloud-first identity backbone that didn't depend on Windows infrastructure. That gap became the foundation of JumpCloud.

Building that unified vision required solving extremely complex technical challenges, but having philosophical clarity from day one made the effort worthwhile. Looking back, committing to a platform-first approach rather than assembling disconnected tools is what positioned JumpCloud for long-term relevance as the identity landscape evolved.

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

> "Identity has always been the most powerful control plane, but for many years it didn't receive the attention it deserved because legacy architectures kept it fragmented."
>
> —Greg Keller, Co-Founder & Chief Technology Officer, JumpCloud

The Shift Toward Identity-centric Security

Adrian Drozd: *Over the 10+ years since JumpCloud launched, what major shifts have you observed in the market around identity, security, and customer expectations?*

Greg Keller: The most significant shift has been the global recognition that identity is the foundation of modern security. Cybersecurity evolved in phases. Initially, the focus was on protecting the device. Then it shifted toward securing the network. Only more recently has the industry truly centered its strategies around identity.

Identity has always been the most powerful control plane, but legacy architectures kept it fragmented for years. Today, attackers overwhelmingly target identity because it offers the most efficient path to privilege escalation and lateral movement. The threat landscape has made this reality impossible to ignore.

Another major shift is the rise of non-human identities. AI agents, automation bots, service accounts, machine-to-machine workflows, and MCP (Model Context Protocol) servers now perform tasks that were once handled by humans. However, most organizations still rely on trust frameworks designed exclusively for people. Non-human actors behave differently and can carry enormous risk if they are not governed properly. This is a frontier many organizations underestimate, and the rapid acceleration of AI has only intensified the challenge.

Customer expectations have also changed dramatically. Modern IT teams want consolidation, automation, and simplicity. They don't want to manage a patchwork of standalone identity, MDM (Mobile Device Management), SSO (Single Sign-on), PAM (Privileged Access Management), and MFA (Multi-factor Authentication) tools. They want a single platform that delivers visibility and control without increasing operational complexity. JumpCloud's original thesis aligns closely with what the market is now demanding at scale.

AI, Automation, and Human Oversight

Adrian Drozd: ***AI is clearly a defining theme right now. Where do generative and agentic AI fit into JumpCloud's solutions, and how do you balance automation with human control?***

Greg Keller: We think about AI through a dual model: JumpCloud for AI and AI for JumpCloud. This framing helps us stay grounded in both governance and productivity.

On the JumpCloud for AI side, our responsibility is to help organizations discover, manage, and govern all AI systems in use, whether they are human-facing or autonomous. That includes controlling entitlements, mapping graph relationships, monitoring access behavior, and enforcing least privilege for non-human identities. AI systems are powerful, but without proper governance they can quickly become vectors for misuse or unintended damage.

On the AI for JumpCloud side, we use AI internally to drive major gains in administrator productivity. We evaluated multiple large language models and selected Google Gemini because of its strength in reasoning, security posture, and enterprise readiness. Gemini powers capabilities such as automated script generation, identity analytics, workflow creation, and admin assistance.

For example, an administrator can ask JumpCloud to generate a script to check whether CrowdStrike is installed on a Windows machine and deploy it if it's missing. The AI produces accurate code instantly, significantly reducing the time required for tasks that previously demanded manual effort.

At the same time, humans remain firmly in the loop. AI within JumpCloud does not make autonomous final decisions. It drafts, analyzes, and proposes, but a human must approve before any sensitive action occurs. Preserving human oversight is essential for trust, accuracy, and alignment with security expectations.

Partnerships and the Changing Enterprise Stack

Adrian Drozd: ***Partnerships have become central to JumpCloud's growth strategy. Can you talk about your partnership with Google and how it strengthens your position?***

Greg Keller: The partnership with Google is one of our most strategically important relationships, and it's built on a shared understanding of how modern enterprises want to operate. Many organizations are reevaluating their reliance on Microsoft E3 and E5 ecosystems. They want flexibility, cost efficiency, simpler licensing, and stronger assurances around security.

Google brings best-in-class collaboration tools and rapidly advancing AI capabilities, including Gemini. JumpCloud brings identity, access control, device management, and zero-trust enforcement. Together, we form an end-to-end, cloud-native stack capable of replacing traditional on-premise and Microsoft-centric models.

Since our OEM partnership announcement, we have seen significant interest from enterprises seeking integrated ecosystems that don't lock them into restrictive licensing or legacy assumptions. The partnership also reinforces our AI strategy, ensuring that our embedded LLM (Large Language Model) benefits from strong reasoning and security-first design. Ultimately, it's not just a technology alignment, but a philosophical one around openness, flexibility, and cloud-native simplicity.

Acquisitions, Talent, and Global Reach

Adrian Drozd: ***JumpCloud has made several acquisitions in the past 18 months. How have these strengthened the platform and supported long-term growth?***

Greg Keller: We evaluate acquisitions through what I call the three T's: Technology, Talent, and Territory. Each acquisition must bring meaningful strength in at least one of these areas, though ideally it contributes to all three.

From a technology perspective, we've expanded significantly into privileged access management, identity threat detection and response, and SaaS discovery. Acquisitions such as VaultOne, Stack Identity, and Breez allow us to analyze billions of monthly transactions and detect anomalies, risks, and privilege escalation more effectively.

From a talent perspective, our philosophy is unusual. Founders of acquired companies become co-founders within JumpCloud. We want to preserve their entrepreneurial energy and sense of ownership. These individuals have built companies from the ground up, and by giving them real agency, we maintain a founder-driven pace of innovation.

The third dimension is territory. Innovation is global, not confined to Silicon Valley. We have strong engineering teams in Brazil, Turkey, Southeast Asia, and beyond. These acquisitions diversify our footprint, deepen our engineering capabilities, and broaden our understanding of identity challenges across regions.

Growth Opportunities and Emerging Markets

Adrian Drozd: ***Looking ahead, what are JumpCloud's aspirational growth goals over the next few years?***

Greg Keller: The biggest opportunity is the rapid expansion of AI adoption and the corresponding need for governance. AI is being integrated across every function, and each system requires identity, access, and entitlement controls. We're positioning JumpCloud as the backbone that enables intelligent, secure IT and responsible AI usage at scale.

Another opportunity lies in HRIS integrations. Many HR platforms are expanding into IT management, including onboarding, offboarding, and access provisioning. Because JumpCloud is API-first and modular, it serves as a natural embedded identity layer for these providers.

MSP (Managed Service Provider) ecosystems are also evolving. Historically aligned with Microsoft-only stacks, MSPs increasingly want cross-platform capabilities, support for cloud-native businesses, and new revenue streams around identity and zero trust. JumpCloud is well positioned to meet those needs.

Regional Momentum and Market Focus

Adrian Drozd: ***Which regions or customer segments are most exciting right now?***

Greg Keller: India and Southeast Asia stand out as particularly exciting. In markets such as India, Malaysia, and Indonesia, digital transformation is accelerating across fintech, e-commerce, logistics, and SaaS. These organizations are cloud-first and unburdened by legacy infrastructure, allowing them to adopt modern identity paradigms from day one.

In India specifically, a profound shift is underway. India is no longer perceived as the "back office of the world." It is now a thriving innovation hub, with founders returning from global experience and building sophisticated technology companies at impressive scale. Venture capital is flowing, talent density is rising, and modern IT needs are exploding. These companies need identity platforms that support rapid growth, heterogeneous devices, AI adoption, and a distributed global presence. JumpCloud is already deeply engaged in these markets and sees enormous long-term potential.

A Personal Closing Message

Adrian Drozd: ***To close, what message would you like to share?***

Greg Keller: On a personal level, my message is simple: be kind. The world has become more distributed and demanding, and it's harder than ever to read emotional cues. Leading with empathy costs nothing, but it matters.

From a security standpoint, help the people around you enable MFA on their financial accounts, especially older relatives. They are disproportionately targeted by sophisticated threats, and small actions can dramatically reduce risk. If everyone did this for one or two people, we would make a meaningful impact on global digital safety.

Greg Keller| co-founder and the Chief Technology Officer (CTO) of JumpCloud

Greg Keller is a **co-founder and the Chief Technology Officer (CTO)** of **JumpCloud,** a company providing a cloud-based directory platform for identity, access, and device management. He has been instrumental in the company's product vision, R&D, and global growth since its inception.

Adrian Drozd | Associate Partner & Global Practice Area Leader at Frost & Sullivan

Drozd is an **Associate Partner & Global Practice Area Leader** at **Frost & Sullivan,** guiding global strategy and research initiatives across the security and ICT landscape. With more than two decades of experience in market intelligence and strategic consulting, he supports leading technology providers in defining growth pathways, refining market positioning, and navigating emerging trends. Adrian is known for his analytical depth, commitment to evidence based insight, and ability to translate complex technology developments into clear strategic direction. He collaborates closely with senior executives to shape forward looking decisions and drive measurable business impact.

Ready to Lead the Transformation?

- **Book a Growth Strategy Session**: Align your growth roadmap with Frost & Sullivan's visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts**: Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Share Your Transformation Story:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council** Collaborate with industry leaders shaping the future of your ecosystem.
- **Nominate for the Best Practices Recognition**: Be recognized for excellence in growth strategy, execution, and customer impact.
- **Demonstrate Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Activate Brand & Demand Growth:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Appendix: Enabling Secure Growth in the AI-Driven Identity Era

For readers who want to explore further, **Frost & Sullivan** recommends:.

- Data Security Posture Management Market
- External Attack Surface Management Sector
- Global Surveillance Solutions Growth Opportunities
- Extended Detection and Response (XDR) Industry
- Cloud-native Application Protection Platform (CNAPP) Market

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. ➜

FROST & SULLIVAN