GIGAOM

GIGAOM CxO BRIEF

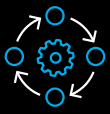
COMMISSIONED BY:
CLOUDBRINK

Rethinking Secure Access Around the User Experience

SECURITY & RISK


GIGA
OM

GigaOm CxO Decision Brief: Rethinking Secure Access Around the User Experience



Solution Overview

Cloudbrink delivers a user-centric, software-only secure access platform that replaces legacy VPN, SD-WAN, and ZTNA stacks. Its ephemeral “FAST Edges” and endpoint-aware architecture prioritize performance, posture, and simplicity – without appliances or tunnels.

Benefits

Cloudbrink enables:

- Typical 20%–400% performance improvement under degraded network conditions, according to Cloudbrink’s published test results.
- Fewer IT tickets and faster user onboarding – 300+ users in a day
- Continuous posture enforcement with eight-hour MTLS 1.3 cert rotation
- Unified policy and visibility across SaaS, hybrid cloud, and private apps
- Predictable licensing with no hidden infrastructure costs

Urgency

Worth immediate consideration if your organization is:

- Dealing with VPN exploits or increased zero-day exposure
- Supporting remote or hybrid workers struggling with latency and app instability
- Integrating new business units or M&A targets
- Trying to collapse fragmented ZTNA, SWG, and SD-WAN tools
- Preparing for continuous trust or compliance audit requirements

Impact

Shifts secure access from a perimeter function to a user-driven model.

- IT teams gain operational simplicity and global agility
- Security posture aligns with real-world user behavior and device state
- Users experience faster access, fewer prompts, and higher productivity
- Governance becomes centralized and policy enforcement unified
- Culture shift: secure access becomes an enabler, not a bottleneck

Risk

Potential challenges include:

- Alignment required across security, IT, and identity teams
- Endpoint visibility and posture baselines must be enforced
- Organizations still tied to fixed POPs, GRE tunnels, or appliance-based models may face inertia
- Success depends on policy clarity and operational maturity, not just tool deployment

01 Solution Value

This GigaOm CxO Decision Brief was commissioned by Cloudbrink.

SECURE ACCESS HAS LONG BEEN FRAMED as a problem of location, infrastructure, and control. Traditional ZTNA and SASE solutions have responded with platform models built around static points of presence, virtual appliances, and policy enforcement planes anchored in centralized infrastructure. Yet for most enterprises, the reality is now far more fluid: applications are scattered across hybrid environments, users move constantly between networks, and the attack surface expands every time the experience degrades.

Cloudbrink offers an alternative approach, reframing secure access around the experience of the user, not the architecture of the system. Instead of relying on hardware-based POPs or site-to-site tunnels, Cloudbrink's architecture deploys as a 100% software-only solution that dynamically provisions edge resources ("FAST Edges") near users on demand. These ephemeral edges are paired with a lightweight client (Brink App) that handles secure access, posture assessment, and performance acceleration in real time.

Cloudbrink claims that this model can yield performance improvements of up to 30x under challenging network conditions, particularly where packet loss, latency, or mid-mile congestion would traditionally impair productivity. While this figure reflects specific scenarios (such as packet loss and latency when transferring large files), the architecture is clearly optimized to deliver measurable gains for hybrid workers, field teams, and latency-sensitive applications. Less than 0.5% packet loss has been found to lead to a significant reduction in available capacity. Most customers can expect to see an aggregate of 20%-400% improvement in application responsiveness after deploying the solution.

Critically, Cloudbrink's stack eliminates many of the operational compromises found in traditional ZTNA deployments:

- No GRE tunnels or static service edges to manage
- No SD-WAN or uCPE hardware at the user level
- No need to trade performance for posture

Instead, session security and policy enforcement are handled via Mutual TLS 1.3, with Cloudbrink rotating certificates every eight hours, which is a practice far beyond the norm (many vendors continue to rely on TLS 1.2 and multiyear certificates). This

rotational approach increases security fidelity while minimizing the attack surface associated with long-lived credentials and predictable infrastructure.

Cloudbrink positions this model as “Personal SASE,” which is a user-following stack that adapts to device posture, network behavior, and role-based access policies without requiring user intervention or location-based exceptions. Rather than forcing remote employees to route through centralized gateways or configure context-specific tunnels, access is granted (or denied) based on the combination of verified identity, device compliance, and active session telemetry.

From an operational perspective, the platform offers centralized visibility across all user activity, with a unified policy engine covering internet, SaaS, and private application access. Customers report rapid onboarding, including one enterprise that successfully enrolled the first 300 users on day one, and cite reduced IT overhead due to simplified deployment, license transparency, and the elimination of appliance supply-chain challenges.

For CIOs and CISOs, the appeal is clear: a secure access model that doesn’t sacrifice performance, a user experience that doesn’t create friction, and an architecture that doesn’t replicate the complexity of the systems it was meant to replace.

Cloudbrink’s approach will be especially relevant for organizations:

- Supporting highly distributed or mobile teams
- Facing performance complaints from remote workers
- Trying to consolidate disjointed VPN, ZTNA, and SWG components
- Seeking greater control over user-to-application access paths without adding infrastructure drag

While results will vary based on network conditions, deployment model, and operational readiness, Cloudbrink’s design aligns with the evolving needs of modern enterprises, where productivity, security, and experience are no longer separate concerns.

02 Urgency and Risk

Urgency

The shift to hybrid work is no longer a temporary disruption. It is the new baseline. Yet most secure access architectures still reflect a centralized mindset that is built for data centers, fixed endpoints, and controllable networks. As the locus of work continues to drift toward distributed environments, the gaps between users and applications have widened. So have seams between performance, security, and usability.

CIOs and CISOs are increasingly accountable for these gaps. Remote productivity complaints, unresolvable latency issues, and access delays are no longer viewed as IT nuisances but are interpreted as leadership failures. End users expect secure access to "just work," regardless of location. Boards and audit teams expect the same consistency from the security stack. And infrastructure teams are caught in the middle, trying to reconcile brittle VPNs, underperforming ZTNA, and a wave of user experience incidents they are not equipped to resolve.

This pressure is compounded by the nature of today's security threats. As adversaries shift their focus to user endpoints, identity compromise, and misconfigured access layers, the traditional perimeter is largely irrelevant. But so too are architectures that replicate perimeter logic through static tunnels, fixed gateways, or visibility silos.

Cloudbrink's model, which is centered around dynamic access, rotating trust certificates, and ephemeral edge presence, is designed to counteract both threat evolution and workforce dispersion. It aligns trust evaluation with the user's real-world context: identity, device posture, behavioral signals, and network state.

The longer enterprises delay a rethink of secure access, the more compounded their risk becomes.

02 Urgency and Risk

Risk

Failure to modernize secure access strategies introduces exposure across multiple dimensions:

Operational risk – Static, appliance-heavy solutions increase downtime and support burdens. Users encountering degraded app performance in the field or during high-latency sessions (e.g., large file uploads, real-time editing, DaaS input lag) often bypass official channels, introduce shadow IT, or disengage, all of which degrade security posture and create negative productivity spirals.

Security risk – Continued reliance on legacy TLS versions, long-lived certificates, and predictable edge infrastructure creates blind spots and persistent targets. Vendors that still operate via fixed POPs or GRE/IPSec tunnels offer attackers known vectors for interception or enumeration.

Organizational risk – Fragmented management consoles, policy mismatches across components (e.g., SWG vs. ZTNA vs. VPN), and inconsistent enforcement undermine the credibility of security and infrastructure leadership. The inability to articulate or measure user-level security posture in real time becomes a governance issue, not just a technical one.

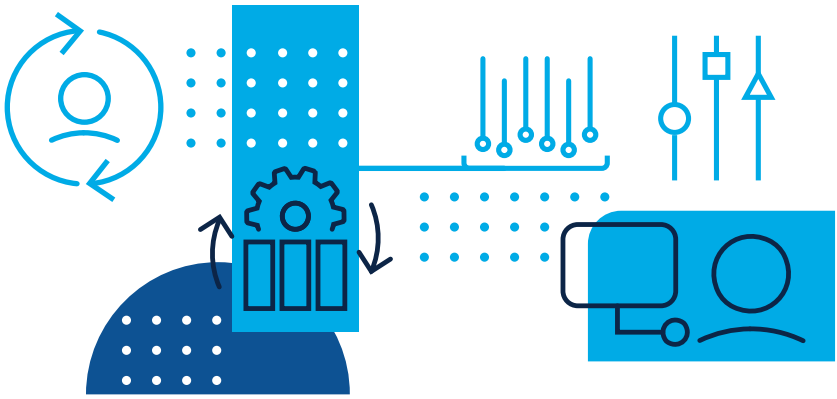
Scalability risk – As business demands grow, especially across geographies or contractor ecosystems, legacy models struggle to scale. Each new region, partner, or access scenario often requires manual provisioning, hardware expansion, or policy workarounds. This slows down the business and creates integration drag.

Reputational risk – For regulated industries, remote access failures can impact audits, delay compliance attestations, or result in public disruptions that affect trust and brand equity.

In many enterprises, these risks accumulate slowly, masked by the inertia of existing tools and the false comfort of “it’s working well enough.” But user experience is often the first system to fail, and the hardest one to measure until it’s too late.

03 Benefits

MODERNIZING SECURE ACCESS AROUND THE USER, rather than the network, offers meaningful benefits that extend well beyond traditional security posture. Cloudbrink's architecture prioritizes experience, speed, and simplicity without weakening control, and in doing so, unlocks value across IT, security, and business leadership.



Key benefits include:

- **Elimination of the performance-security trade-off**
  Many ZTNA deployments force a compromise: tighten access, degrade experience; loosen controls, improve usability. Cloudbrink's model removes this dilemma by collapsing security enforcement and performance optimization into a single endpoint-aware agent. Sessions are protected via rotational MTLS 1.3, while traffic is accelerated based on real-time network telemetry and congestion awareness (there is technically no acceleration, but Cloudbrink stops the "matias equation backoff," resulting in a perceived acceleration).

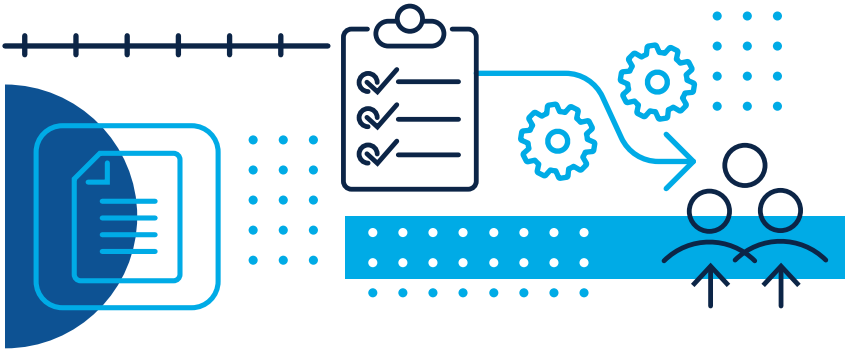
03 Benefits

- **Improved workforce productivity**
  Users working on constrained or unstable connections (e.g., home Wi-Fi, mobile networks, low-quality ISP paths) often experience significant latency and failure rates. Cloudbrink's FAST Edge architecture and QOE optimization target these mid-mile and last-mile limitations directly, improving responsiveness for bandwidth-sensitive apps like DaaS, collaboration tools, and large file transfers.
- **Fewer support tickets and lower IT burden**
  Enterprises cite measurable reductions in access-related support incidents after deploying Cloudbrink, particularly during VPN sunset or SD-WAN migration phases. Because all features are software-based and centrally managed, there is no supply-chain friction, no hardware lifecycle to maintain, and no fragmented control plane to troubleshoot.
- **Unified policy and visibility across environments**
  Cloudbrink enables a single console to enforce access controls across SaaS, web, hybrid cloud, and internal applications. This reduces administrative complexity, eliminates misaligned rules between components, and ensures consistent posture across distributed endpoints. Visibility includes both security state (via continuous posture checks) and performance telemetry (via the Brink Quality Index).

"Enterprises cite measurable reductions in access-related support incidents after deploying Cloudbrink, particularly during VPN sunset or SD-WAN migration phases. Because all features are software-based and centrally managed, there is no supply-chain friction, no hardware lifecycle to maintain, and no fragmented control plane to troubleshoot."

03 Benefits

- **Transparent and predictable licensing**
  Cloudbrink offers a named-user licensing model that includes all features, edges, and bandwidth, removing the variable-cost exposure found in many bundled or usage-metered platforms. This simplifies budgeting and allows teams to scale without procurement friction or surprise costs during expansion.
- **Faster time to deploy, validate, and scale**
  With no hardware dependencies and no appliance staging, Cloudbrink customers can onboard users rapidly, in some cases adding hundreds of endpoints within a day. Integration with existing IdPs accelerates policy enforcement, while SaaS-native infrastructure supports global rollout with minimal configuration overhead.



While Cloudbrink's benefits will vary based on the network environment, identity integration maturity, and workforce distribution, the overall impact is consistent: a more agile, user-aligned access model that elevates experience while strengthening posture.

For CIOs and CISOs, these benefits represent a new lens on secure access, where productivity, risk, and simplicity are measured together, not in opposition.

04 Best Practices

IMPROVING SECURE ACCESS OUTCOMES isn't just a product decision; rather, it's a leadership posture. Most of the friction organizations face today comes not from the wrong tools, but from outdated assumptions about what "remote access" and "security perimeter" actually mean.

Enterprises that successfully adopt a user-centric access model typically rethink not just architecture, but also roles, metrics, and expectations across the organization. Based on GigaOm's research and Cloudbrink's architectural principles, the following best practices can help guide a smoother and more impactful transition.

1. Reframe user experience as a risk metric

Poor experience isn't just a UX problem, but a security gap. Laggy connections, unpredictable access, and unstable tunnels lead to workarounds, shadow IT, and user disengagement. Security and infrastructure leaders should incorporate performance indicators (e.g., time to first byte, app responsiveness, Brink Quality Index) into operational dashboards and treat performance degradation as a trigger for investigation.

2. Shift enforcement to the endpoint, not the edge

Legacy models rely on static POPs or VPN concentrators as the enforcement point for policy and inspection. Cloudbrink's model pushes that enforcement closer to the user via device posture checks, continuous certificate validation, and dynamic policy at the application layer. This reduces attack surface and improves agility. Even if not adopting Cloudbrink, enterprises should evaluate how much logic still resides in fixed infrastructure.

3. Consolidate policy across public and private app environments

Many ZTNA solutions treat internet-bound traffic differently from private app access, leading to multiple consoles, misaligned policy engines, and conflicting enforcement logic. Cloudbrink's unified policy layer covers SaaS, web, and hybrid-cloud access from a single point of control. This simplifies policy hygiene and reduces audit complexity. CIOs should push for tools that allow unified context across application types, and not separate silos.

4. Automate trust but verify continuously

Instead of one-time MFA followed by static session trust, best-in-class platforms now support continuous device posture checks and dynamic session validation. Cloudbrink, for example, runs device compliance checks every 30 minutes by default and can revoke access if conditions change. This reduces dwell time for compromised endpoints. Enterprises should aim for zero trust implementations that evolve throughout a session, not just at login.

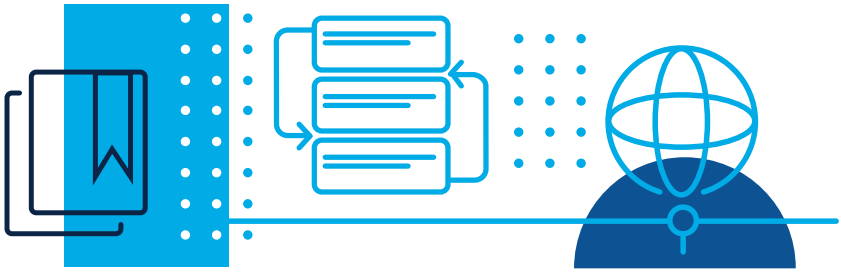
5. Design for agility, not just compliance

The most effective access strategies are those that scale quickly with organizational change, such as M&A, remote onboarding, and new cloud regions. Cloudbrink's software-only approach and dynamic FAST Edges reduce infrastructure friction and accelerate rollout. CIOs should consider the deployment velocity and operational adaptability of their current stack, particularly when expanding to new markets or user populations.

6. Make policy and performance visible to the board

Board-level conversations around secure access typically focus on compliance and risk. But in distributed environments, user experience is risk. By tying performance data to access telemetry and incident trends, CIOs and CISOs can elevate secure access from a background utility to a strategic enabler. Platforms like Cloudbrink, which expose both posture and performance metrics in a unified console, can help teams close that reporting gap.

These practices don't require a full rip-and-replace strategy, but they do require a new baseline: one where the user, not the network, defines how access should work.



05 Organizational Impact

MODERNIZING SECURE ACCESS AROUND user experience and endpoint trust is not just a technical migration. Instead, it reshapes how security, infrastructure, and IT operations engage with each other and the business. While platforms like Cloudbrink can be deployed rapidly and without hardware friction, the real impact plays out across people, processes, and planning.

People Impact

Shifting the trust model from the perimeter to the endpoint demands new collaboration patterns.

- **Security and networking teams** must align on posture policies, identity integration, and acceptable risk thresholds, particularly around mobile and BYOD endpoints.
- **IT operations** gains new visibility into user-level experience metrics, but may also be asked to support escalations tied to perceived latency, access failure, or application behavior, even when the infrastructure is healthy.
- **End users** experience fewer prompts, less friction, and faster access, but may be subject to session revocation or conditional access if posture degrades. This requires clear internal communication and training.

Importantly, organizations adopting a user-following ZTNA model often report a cultural shift: from viewing secure access as a compliance constraint to treating it as a **productivity platform**. That shift can only succeed if it's championed cross-functionally.

Process Considerations

Legacy access processes are often optimized for static infrastructure: centralized gateways, long-lived certs, fixed tunnel paths. These assumptions break down under dynamic, distributed, or ephemeral architectures.

Enterprises adopting Cloudbrink's approach should revisit:

- **Access provisioning workflows**, especially around device onboarding, MFA timing, and IdP role mapping.
- **Policy deployment** and testing, ensuring consistency across hybrid-cloud apps and SaaS platforms.

- **Runbooks for performance or posture degradation**, with escalation paths defined across IT, security, and end-user support.
- **Incident response frameworks**, incorporating posture telemetry, session logs, and QOE metrics as inputs for root cause analysis.

Investment Outlook

While Cloudbrink eliminates the need for appliance purchases, SD-WAN endpoints, and VPN concentrator capacity planning, it still represents a platform decision that has both strategic and operational implications.

Key shifts in investment thinking include:

- **Licensing simplicity** – Cloudbrink uses named-user licensing with no bandwidth or feature-based upcharges, improving forecast accuracy and reducing procurement overhead.
- **Operational savings** – Customers report reduced ticket volumes, faster onboarding, and lower maintenance burdens, particularly in distributed environments.
- **Infrastructure avoidance** – By removing the need for physical or virtual appliances, Cloudbrink sidesteps common bottlenecks tied to supply chain, lifecycle refresh, and site provisioning.
- **Future-proofing** – Dynamic edge provisioning, MTLS 1.3 rotation, and continuous posture checking align well with emerging regulatory expectations and zero trust maturity models.

Over time, organizations may find that these investments allow them to collapse multiple tools (VPN, SWG, ZTNA) into a unified experience, not just to save cost, but to reduce complexity and risk.

“While Cloudbrink eliminates the need for appliance purchases, SD-WAN endpoints, and VPN concentrator capacity planning, it still represents a platform decision that has both strategic and operational implications.”

06 Solution Timeline

IMPLEMENTING A USER-CENTRIC SECURE ACCESS model like Cloudbrink's is less about infrastructure lift and more about policy alignment and integration discipline. Because the platform is fully software-based and cloud-native, deployment can begin quickly, but long-term value depends on how well organizations coordinate security, identity, and endpoint management practices.

Implementation Considerations

Organizations with fragmented policy ownership, legacy IdPs, or unmanaged devices may need to address foundational issues before realizing full value. That said, Cloudbrink's architecture is designed for agility:

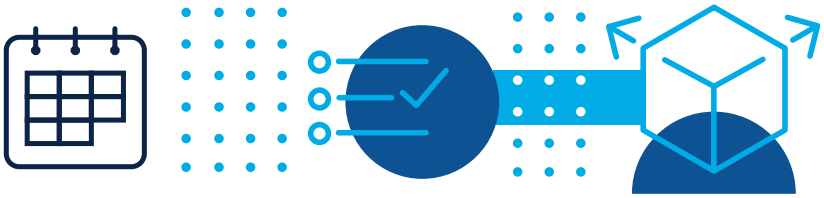
- Endpoint agents are lightweight and deployable via standard MDM tooling or direct installation.
- FAST Edges are instantiated automatically based on user location and traffic needs, with no infrastructure staging or capacity planning required.
- Policy enforcement integrates with existing identity providers, allowing role-based access to be inherited rather than rebuilt.

Key dependencies include:

- IdP integration and RBAC design
- Endpoint management (visibility, posture assessment tools)
- Cross-team coordination between IT, security, and networking

Typical Timeline Elements

While specific timelines vary, the general adoption pattern follows four key phases:



06 Solution Timeline

1. Discovery and Assessment

Understand the current-state architecture:

- Where performance complaints and support tickets originate
- How current VPN, ZTNA, or SWG tools are distributed
- Which endpoints are managed or unmanaged
- What policies exist for app segmentation, SaaS access, and BYOD control

This phase also identifies pilot users and candidate applications (e.g., DaaS, large-file transfers, sensitive SaaS).

2. Design and Integration

- Integrate Cloudbrink with existing IdP (e.g., Okta, Entra, Ping)
- Define role-based access policies
- Establish baseline posture expectations (disk encryption, AV status, etc.)
- Configure user groups and pilot cohorts

3. Deployment and Validation

- Distribute the Brink App to pilot users
- Validate posture enforcement, access success, and performance gains
- Monitor the Brink Quality Index to identify improvement zones
- Begin phasing out legacy VPN or SD-WAN agents in controlled groups

Enterprises report successful onboarding of hundreds of users in less than a day, but best practice is to pair speed with observability. Success metrics should include user satisfaction, ticket reduction, and posture enforcement rates.

06 Solution Timeline

4. Operationalization

- Expand to additional user groups, regions, and application segments
- Formalize performance thresholds and posture alerting
- Integrate Cloudbrink logs into SIEM/XDR systems
- Establish reporting cadence for executive KPIs (uptime, trust posture, performance quality)

Future Considerations

As regulatory pressure grows around continuous trust, just-in-time access, and secure-by-design principles, architectures like Cloudbrink's will align more directly with compliance and audit demands.

The platform's built-in capabilities, such as rotational MTLS 1.3, dynamic edge activation, and posture-triggered session revocation, position it well for future mandates that require evidence of active session management, not just perimeter hardening.

Organizations that invest early in dynamic, user-following models may find themselves better prepared for the next wave of zero trust expectations, not just in terms of control, but in terms of **agility, transparency, and measurable outcomes.**

"As regulatory pressure grows around continuous trust, just-in-time access, and secure-by-design principles, architectures like Cloudbrink's will align more directly with compliance and audit demands."

07 Analyst's Take

SECURE ACCESS USED TO BE A BOUNDARY PROBLEM. Then it became a segmentation problem. Now it's an experience problem, and that's exactly where most zero trust architectures fall short.

Despite two decades of progress, most enterprise access strategies still assume that the user must adapt to the system. That performance degradation is inevitable. That security and usability are opposing forces. That friction is just the price of safety.

Cloudbrink flips that equation. It treats the user, rather than the network, the perimeter, or the appliance, as the primary unit of design. By collapsing enforcement, acceleration, and visibility into a software-only, endpoint-aware service, Cloudbrink doesn't just connect users to applications. Instead, it optimizes and secures the experience every step of the way.

GigaOm does not take vendor claims at face value. Not every user will see 30x improvements. Not every deployment will be seamless. But the architectural design choices, such as ephemeral edges, rotational MTLS, continuous posture validation, no GRE tunnels or virtual appliances, speak to a different set of priorities: **user performance as a security control, not a trade-off.**

07 Analyst's Take

For CIOs and CISOs, that shift matters. It reframes secure access not as a compliance check or a cost center, but as an enabler of productivity, scale, and agility. It gives security leaders a new narrative that is grounded in real outcomes:

- Reduced support load
- Faster onboarding
- Consistent UX across regions
- Fewer attack surfaces
- Simpler licensing and rollout

Perhaps most importantly, it gives organizations a path forward that doesn't replicate the complexity of the systems they're trying to replace.

If you're still treating VPNs as a stopgap, SD-WAN as a user access solution, or ZTNA as an overlay, you're solving yesterday's problems with yesterday's tools. It's time to ask:

What if secure access actually made work easier, not just safer?

Cloudbrink isn't the only path forward. But it's a credible and sharply differentiated one. And for leaders ready to rethink access as a strategic asset, it's a conversation worth having.

Report Methodology

THIS GIGAOM CXO DECISION BRIEF ANALYZES a specific technology and related solution to provide executive decision-makers with the information they need to drive successful IT strategies that align with the business. The report is focused on large impact zones that are often overlooked in technical research, yielding enhanced insight and mitigating risk. We work closely with vendors to identify the value and benefits of specific solutions, and to lay out best practices that enable organizations to drive a successful decision process.

About Howard Holton

HOWARD HOLTON IS AN ANALYST AT GIGAOM. He has worked in IT for three decades, the last half in executive leadership, as a CIO and CTO. He has been an engineer, an architect, and a leader in telecom, health care, automotive, retail, legal, and technology.

In the last decade, Howard focused on cloud technology and economics, data analytics, and digital transformation. As CTO of Hitachi Vantara, he spent his time developing digital transformation, IT, and data strategies for Fortune 1000 companies and global governments.

His years at Rheem Manufacturing, Hitachi Vantara, and others provided the experience that helped him develop a mind for leadership—the successful execution of vision and culture to inspire. Successful leadership is all about maximizing your team's potential, as Howard has demonstrated over the course of his career.

Howard is also a technologist at heart; passionate about how data science and new technologies can be used to accelerate time-to-market and better serve the customer, now and in the future. Howard has been a trusted advisor and agent of change to a number of organizations, bringing vision and successful execution to internal and external customers alike.

GIGAOM

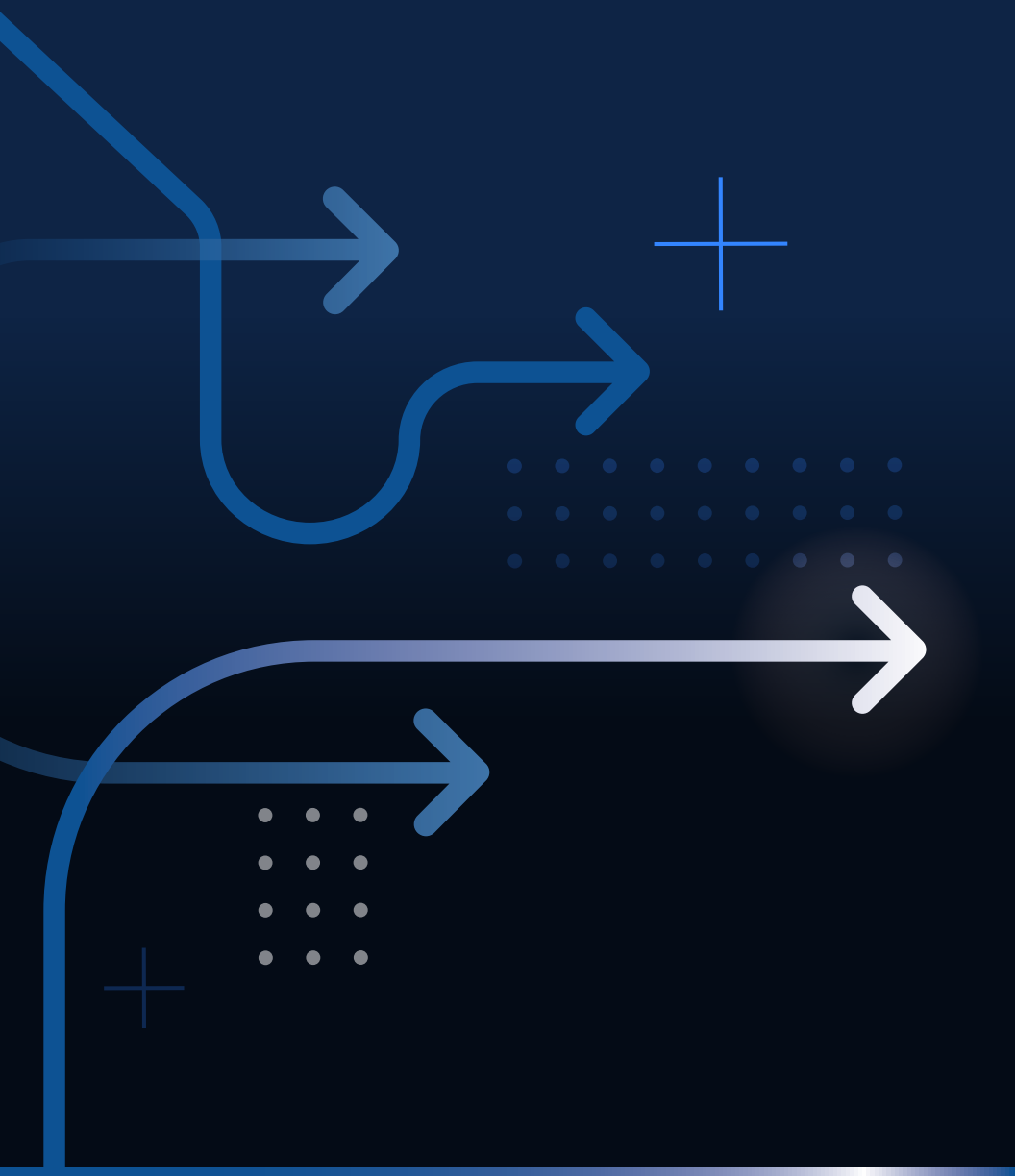
About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.


GIGA
OM



GIGAOM

GigaOm democratizes access to strategic, engineering-led technology research. We enable businesses to innovate at the speed of the market by helping them to grasp new technologies, upskill teams, and anticipate opportunities and challenges. The GigaOm platform changes the game, by unlocking deep technical insight and making it accessible to all.